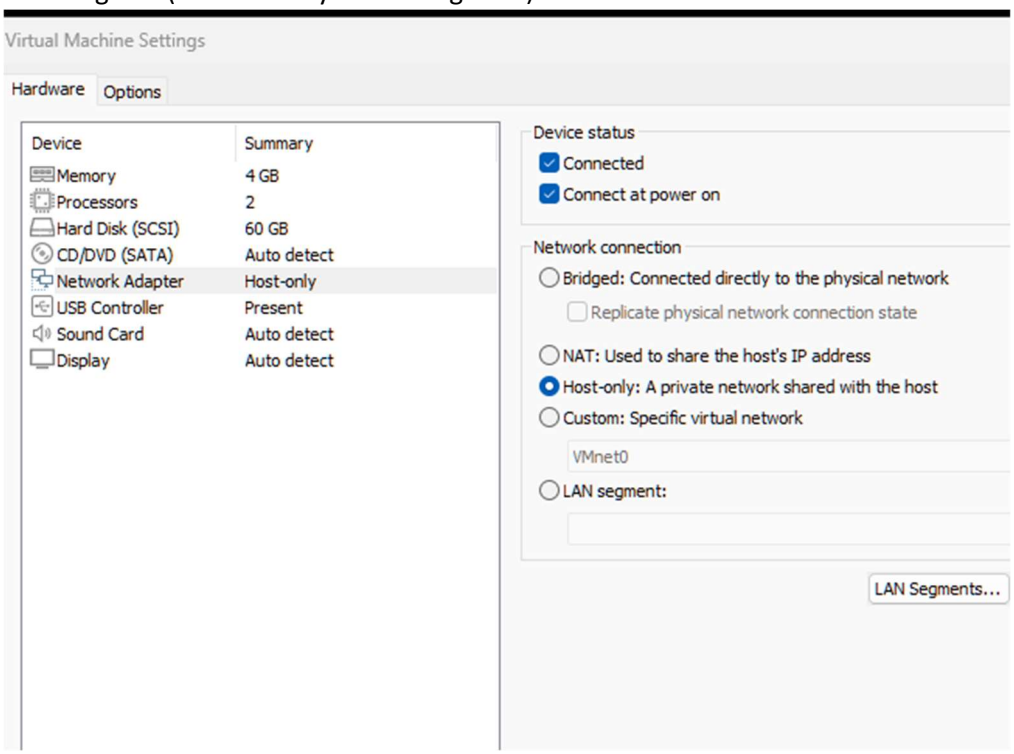
TP1 - Installation d'un serveur Windows

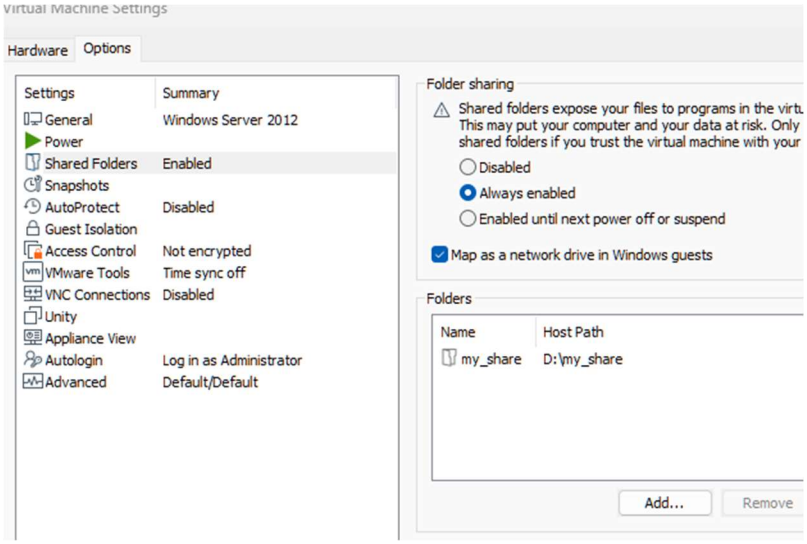
Ifrim Vasile-Alexandru M2SSI

1. Installez Virtualbox et ses extensions. Téléchargez Windows Server 2012 R2 (version d'essai - langue anglaise).
   For the following TP I chose to use VMWare. I downloaded a Windows Server 2012 R2 from https://www.microsoft.com/en-us/evalcenter/download-windows-server-2012-r2.
2. Créez un environnement virtuel pour Windows sur Virtualbox. Documentez vos choix concernant les ressources attribuées à la machine virtuelle en vous appuyant sur des ressources officielles. Expliquez votre choix de configuration Réseau.
   According to https://www.techtarget.com/searchwindowsserver/tip/Be-aware-of-essential-Windows-Server-2012-hardware-requirements, Windows Server 2012 R2 has the following minimum requirements: single 1.4GHz 64-bit processor, 512 MB RAM, 32 GB storage and 10/100 Mbps Ethernet network connection. For more performance, I can spare more than this even if a bit redundant. More importantly is the network configuration: I had issues with the adapter in bridged mode on the eduroam network – no internet access, default Windows automatic ip address. So, whenever internet access was needed by the guest machine, i switched to NAT. For anything else, a Host-only network was used for the ability to access from host to guest (and visibility between guests).

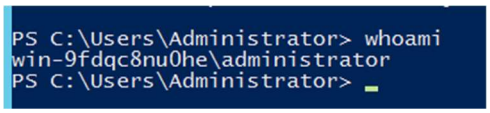


3. Montez le disque téléchargé sur la VM et lancez la machine virtuelle. Installez le serveur Windows Server 2012 R2 avec Interface Graphique
4. Créez un compte administrateur. Justifiez votre choix de nommage. A la fin de l'installation, effectuez une snapshot de la machine.
   I chose to just name it Administrator, but for a secure name common and descriptive names should be avoided (Admin, Administrator, root, srvAdmin, srv_mng) to obscure the fact that that account has any privileges more than your next user, making it hard for attackers to target it. Also, for any server management consistent naming conventions should be used.

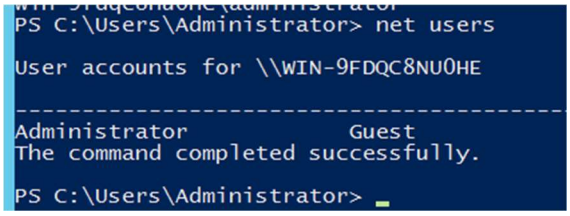
5. Créez un répertoire d'échange (shared folder) entre votre machine hôte et votre machine virtuelle. Assurez-vous que vous êtes bien en mesure d'échanger des données entre votre hôte et la VM.



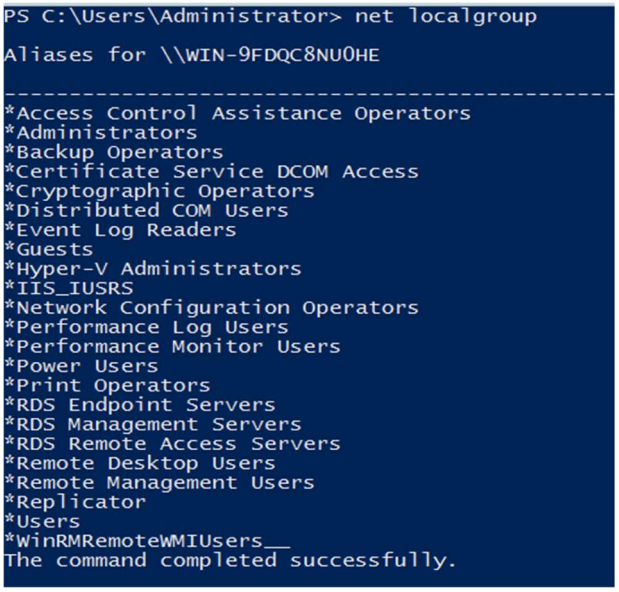
6. Ouvrez l'intepréteur de commande par défaut de Windows. Identifiez les commandes adaptées qui permettent d'afficher les informations suivantes :
   - l'utilisateur courant
     >whoami



   - la liste des utilisateurs locaux
     >net users



   - la liste des groupes locaux
     >net localgroup



- la version du système
  >systeminfo

```
Host Name:                 WIN-9FDQC8NU0HE
OS Name:                   Microsoft Windows Server 2012 R2 Standard Evaluation
OS Version:                6.3.9600 N/A Build 9600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00252-10000-00000-AA228
Original Install Date:     9/20/2024, 2:46:27 PM
System Boot Time:          9/20/2024, 2:55:21 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 158 Stepping 10 GenuineIntel ~2400 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 11/12/2020
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-08:00) Pacific Time (US & Canada)
Total Physical Memory:     4,095 MB
Available Physical Memory: 3,408 MB
Virtual Memory: Max Size:  5,503 MB
Virtual Memory: Available: 4,575 MB
Virtual Memory: In Use:    928 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\WIN-9FDQC8NU0HE
Hotfix(s):                 7 Hotfix(s) Installed.
                           [01]: KB2919355
                           [02]: KB2919442
                           [03]: KB2937220
                           [04]: KB2938772
                           [05]: KB2939471
                           [06]: KB2949621
                           [07]: KB2999226
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) 82574L Gigabit Network Connection
                                 Connection Name: Ethernet0
                                 DHCP Enabled:    Yes
                                 DHCP Server:     255.255.255.255
                                 IP address(es)
                                 [01]: 169.254.76.253
                                 [02]: fe80::cdd2:b3ad:7e64:4cfd
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will n
```

- informations détaillées sur les interfaces réseau configurées
  >ipconfig /all

```
PS C:\Users\Administrator> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : WIN-9FDQC8NU0HE
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-A3-63-71
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::cdd2:b3ad:7e64:4cfd%12(Preferred)
   Autoconfiguration IPv4 Address. . : 169.254.76.253(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 301993001
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2E-7F-A4-AA-00-0C-29-A3-63-71
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{0BE31B70-195A-4A36-9F4C-BE5E90AB2A01}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter #2
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

- la liste des processus en cours d'exécution
  >tasklist

```
PS C:\Users\Administrator> tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          4 K
System                           4 Services                   0        256 K
smss.exe                       216 Services                   0      1,028 K
csrss.exe                      336 Services                   0      3,472 K
wininit.exe                    416 Services                   0      3,432 K
services.exe                   508 Services                   0      5,000 K
lsass.exe                      516 Services                   0      8,580 K
svchost.exe                    576 Services                   0      9,648 K
svchost.exe                    608 Services                   0      6,848 K
svchost.exe                    772 Services                   0     14,044 K
svchost.exe                    824 Services                   0     27,020 K
svchost.exe                    864 Services                   0      9,612 K
svchost.exe                    932 Services                   0     13,676 K
svchost.exe                    304 Services                   0     10,524 K
spoolsv.exe                   1052 Services                   0      8,620 K
svchost.exe                   1120 Services                   0     10,020 K
VGAuthService.exe             1140 Services                   0      9,036 K
vm3dservice.exe               1196 Services                   0      3,836 K
vmtoolsd.exe                  1216 Services                   0     16,708 K
wlms.exe                      1280 Services                   0      2,608 K
dllhost.exe                   1748 Services                   0     10,076 K
msdtc.exe                     1804 Services                   0      6,708 K
WmiPrvSE.exe                  1932 Services                   0     15,800 K
WmiPrvSE.exe                  2768 Services                   0     11,168 K
csrss.exe                     2108 Console                    2     19,760 K
winlogon.exe                  3048 Console                    2      5,048 K
dwm.exe                       2968 Console                    2     53,448 K
vm3dservice.exe               2972 Console                    2      4,248 K
taskhostex.exe                2760 Console                    2      5,804 K
explorer.exe                  2112 Console                    2     69,192 K
ServerManager.exe             1096 Console                    2     74,044 K
vmtoolsd.exe                  2404 Console                    2     15,776 K
powershell.exe                 728 Console                    2     86,768 K
conhost.exe                   1992 Console                    2     19,344 K
tasklist.exe                  3032 Console                    2      5,252 K
```

- la liste des services en cours d'exécution
  >sc query

```
C:\Users\Administrator>sc query

SERVICE_NAME: BFE
DISPLAY_NAME: Base Filtering Engine
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: BITS
DISPLAY_NAME: Background Intelligent Transfer Service
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
 And so on...
SERVICE_NAME: BrokerInfrastructure
```

7. Identifiez 3 services en cours d'exécution sur le serveur (au choix, services vous semblant intéressants). Décrire ces services, leurs usages. Identifiez les documentations officielles respectives, utiles pour un durcissement de ces services.

8. Créez via l'instance 4 comptes supplémentaires sur le système:
    - ◦ 1 compte administrateur supplémentaire

```
C:\Users\Administrator>net user Admin_2 Password123 /add && net localgroup administrators Admin_2 /add
The command completed successfully.

The command completed successfully.


C:\Users\Administrator>net user

User accounts for \\WIN-9FDQC8NU0HE

-------------------------------------------------------------------------------
Admin_2                  Administrator            Guest
The command completed successfully.
```

    - 2 comptes standards au sein d'un groupe M2SSI

```
C:\Users\Administrator>net localgroup M2SSI /add
The command completed successfully.
```

```
C:\Users\Administrator>net user Stud1 Password1 /add && net localgroup M2SSI Stud1 /add
The command completed successfully.

The command completed successfully.


C:\Users\Administrator>net user Stud2 Password2 /add && net localgroup M2SSI Stud2 /add
The command completed successfully.
```

    - un compte standard dans le groupe STAGIAIRE au mot de passe Password01!

```
C:\Users\Administrator>net localgroup STAGIAIRE /add
The command completed successfully.


C:\Users\Administrator>net user Stag1 Password01! /add && net localgroup STAGIAIRE Stag1 /add
The command completed successfully.
```

9. Où sont stockés les comptes et leurs secrets configurés sur le système de fichier? Proposez 2 méthodes différentes pour récupérer ces fichiers pour une analyse à froid. Décrivez la démarche de récupération. Identifiez les noms d'utilisateurs et leur mot de passe stocké au sein de ces données.
   https://www.thehacker.recipes/ad/movement/credentials/dumping/sam-and-lsa-secrets
    - Methode 1 – Live Windows

   Copy from reg:

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> reg save HKLM\SAM "Z:\my_share\sam.save"
The operation completed successfully.
PS C:\Users\Administrator> reg save HKLM\SYSTEM "Z:\my_share\system.save"
The operation completed successfully.
PS C:\Users\Administrator> reg save HKLM\SECURITY "Z:\my_share\security.save"
The operation completed successfully.
PS C:\Users\Administrator>
```

   Or do a shadow copy of C:\Windows\System32\config:

```
PS C:\Users\Administrator> vssadmin create shadow /for=C:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Successfully created shadow copy for 'C:\'
    Shadow Copy ID: {c54188c7-f4b6-4a98-84f4-60bc94808d52}
    Shadow Copy Volume Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2
PS C:\Users\Administrator> copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\con
fig\SYSTEM C:\Windows\Temp\system.save
PS C:\Users\Administrator> cp C:\Windows\Temp\system Z:\system.save1
```

- Methode 2 - Offline System Access

Bootable Live CD/USB with a Linux -> Navigate to C:\Windows\System32\config -> Copy the SAM, SYSTEM and SECURITY files.

In Windows environments, passwords are stored in a hashed format in registry hives like SAM (Security Account Manager, stores locally cached credentials – SAM secrets: LM or NT hashes) and SECURITY (stores domain cached credentials – LSA secrets: plaintext, LM or NT hashes, etc). SYSTEM contains enough info to decrypt SAM secrets and LSA secrets. For now, we are only interested in locally cached credentials.

Mimicatz dump of secrets [https://github.com/gentilkiwi/mimikatz/releases]:

```
mimikatz # lsadump::sam /sam:"D:\my_share\sam.save" /system:"D:\my_share\system.save"
Domain : WIN-9FDQC8NU0HE
SysKey : 4673ccaa01b241845e9558d0c6f4e06d
Local SID : S-1-5-21-3542280733-1080477990-1394795187

SAMKey : de617268097f2f1b35b64481938045b6

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: 58a478135a93ac3bf058a5ea0e8fdb71

RID  : 000001f5 (501)
User : Guest

RID  : 000003ea (1002)
User : Admin_2
  Hash NTLM: 58a478135a93ac3bf058a5ea0e8fdb71

RID  : 000003ed (1005)
User : Stud1
  Hash NTLM: 64f12cddaa88057e06a81b54e73b949b

RID  : 000003ee (1006)
User : Stud2
  Hash NTLM: c39f2beb3d2ec06a62cb887fb391dee0

RID  : 000003f1 (1009)
User : Stag1
  Hash NTLM: 7c4fe5eada682714a036e39378362bab
```

```
mimikatz # lsadump::secrets /security:"D:\my_share\security.save" /system:"D:\my_share\system.save"
Domain : WIN-9FDQC8NU0HE
SysKey : 4673ccaa01b241845e9558d0c6f4e06d

Local name : WIN-9FDQC8NU0HE ( S-1-5-21-3542280733-1080477990-1394795187 )
Domain name : WORKGROUP

Policy subsystem is : 1.12
LSA Key(s) : 1, default {d1e0003e-f916-6a38-0b53-18f67571e631}
  [00] {d1e0003e-f916-6a38-0b53-18f67571e631} 0391219ca0907c37ee0b601794e8d218fccb95acb8f52f4f28d37244ab13bd2a

Secret  : DefaultPassword
cur/text: Password123
old/text: ROOT#123

Secret  : DPAPI_SYSTEM
cur/hex : 01 00 00 00 6a 41 7b e9 e0 34 1f aa bd 7c 83 c9 2f 25 3f e5 20 c4 ed 9c 7e ff 3b 09 2c f7 fb 4d 75 3a 9
f eb 1a b5 5c 4f 51 7c 0a dc
    full: 6a417be9e0341faabd7c83c92f253fe520c4ed9c7eff3b092cf7fb4d753a9feb1ab55c4f517c0adc
    m/u : 6a417be9e0341faabd7c83c92f253fe520c4ed9c / 7eff3b092cf7fb4d753a9feb1ab55c4f517c0adc
old/hex : 01 00 00 00 55 0b 07 be cc e6 4f 90 bb 45 62 4a 4a dc 7f 91 50 a8 90 cc dd dc d2 a3 ce 33 5a 29 49 3d 6
0 6f 25 a5 03 2e 42 39 b1 96
    full: 550b07becce64f90bb45624a4adc7f9150a890ccdddcd2a3ce335a29493d606f25a5032e4239b196
    m/u : 550b07becce64f90bb45624a4adc7f9150a890cc / dddcd2a3ce335a29493d606f25a5032e4239b196
```

Impacket's secretsdump dump:

```
isav@DESKTOP-9KVQ2B3:~$ python3 secretsdump.py -sam '/mnt/d/my_share/sam.save' -security '/mnt/d
/my_share/security.save' -system '/mnt/d/my_share/system.save' LOCAL
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x4673ccaa01b241845e9558d0c6f4e06d
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Admin_2:1002:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
Stud1:1005:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
Stud2:1006:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0:::
Stag1:1009:aad3b435b51404eeaad3b435b51404ee:7c4fe5eada682714a036e39378362bab:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] DefaultPassword
(Unknown User):Password123
[*] DPAPI_SYSTEM
dpapi_machinekey:0x6a417be9e0341faabd7c83c92f253fe520c4ed9c
dpapi_userkey:0x7eff3b092cf7fb4d753a9feb1ab55c4f517c0adc
[*] Cleaning up...
```

NT hash

From LSA secrets we already got a plaintext password

We paste these NTLM hashes in a ‚hashes' input file.

```
isav@DESKTOP-9KVQ2B3:~$ cat hashes
58a478135a93ac3bf058a5ea0e8fdb71
64f12cddaa88057e06a81b54e73b949b
c39f2beb3d2ec06a62cb887fb391dee0
7c4fe5eada682714a036e39378362bab
```

Time to crack the hashes with hashcat [https://tools.kali.org/password-attacks/hashcat].
>hashcat -m 1000 -a 0 ./hashes ./10mil_password_list –force

In this command, -m stands for hash mode(e.g, 1000 stands for NTLM hash), -a stands for attack mode (e.g., 0 stands for straight attack); ‚10mil_password_list' is a dictionary of weak passwords found on the Internet.

```
Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

INFO: Removed 1 hash found in potfile.

* Device #1: build_opts '-cl-std=CL1.2 -I OpenCL -I /usr/share/hashcat/OpenCL -D LOCAL_MEM_TYPE=2
 VENDOR_ID=64 -D CUDA_ARCH=0 -D AMD_ROCM=0 -D VECT_SIZE=8 -D DEVICE_TYPE=2 -D DGST_R0=0 -D DGST_R
 -D DGST_R2=2 -D DGST_R3=1 -D DGST_ELEM=4 -D KERN_TYPE=1000 -D _unroll'
Dictionary cache hit:
* Filename..: ./10mil_password_list
* Passwords.: 999998
* Bytes.....: 8529108
* Keyspace..: 999998

64f12cddaa88057e06a81b54e73b949b:Password1
c39f2beb3d2ec06a62cb887fb391dee0:Password2
Approaching final keyspace - workload adjusted.


Session..........: hashcat
Status...........: Exhausted
Hash.Type........: NTLM
Hash.Target......: ./hashes
Time.Started.....: Tue Sep 24 19:58:15 2024 (1 sec)
Time.Estimated...: Tue Sep 24 19:58:16 2024 (0 secs)
Guess.Base.......: File (./10mil_password_list)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2088.6 kH/s (0.37ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 3/4 (75.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 999998/999998 (100.00%)
Rejected.........: 0/999998 (0.00%)
Restore.Point....: 999998/999998 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: vjq6frrfeyn -> vjht008

Started: Tue Sep 24 19:58:13 2024
Stopped: Tue Sep 24 19:58:17 2024
isav@DESKTOP-9KVQ2B3:~$ hashcat -m 1000 -a 0 ./hashes ./10mil_password_list --force --show
58a478135a93ac3bf058a5ea0e8fdb71:Password123
c39f2beb3d2ec06a62cb887fb391dee0:Password2
64f12cddaa88057e06a81b54e73b949b:Password1
```

Dictionary cracking of weak passwords through Hashcat

In summary, we have exfiltrated the registry hives that contain credentials and important information for decryption so we can do a cold analysis on a separate machine. With the help of tools for dumping, we got a table of users <-> hashes, and with hashcat we managed to crack the hashes, resulting in plaintext passwords.

11. Passwords are stored in a cryptographic format - NTLM hashes. The NTLM hash is encoded by taking the user's password and converting it into a 16-byte key using an MD4 hash function. This key is divided into two halves of 8 bytes each, which are used as input to three rounds of DES encryption to generate a 16-byte output that represents the NTLM hash. More on this, https://www.vaadata.com/blog/understanding-ntlm-authentication-and-ntlm-relay-attacks/#what-is-ntlm.

    NTLM lack salting and are vulnerable to brute-force attacks and rainbow tables. With modern hardware, NTLM hashes can be cracked relatively quickly, especially if the passwords are weak or common.

12. PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework. PowerShell runs on Windows, Linux, and macOS [learn.microsoft.com/en-us/powershell/scripting].
    - Lister les comptes sur le systeme

    >Get-WmiObject -Class Win32_UserAccount -Filter "LocalAccount=True"
    [superuser.com/questions/1718616/list-all-user-accounts-with-an-active-presence-on-the-local-device]

```
PS C:\Users\Administrator> Get-WmiObject -Class Win32_UserAccount -Filter "LocalAccount=True"


AccountType : 512
Caption     : WIN-9FDQC8NU0HE\Administrator
Domain      : WIN-9FDQC8NU0HE
SID         : S-1-5-21-3542280733-1080477990-1394795187-500
FullName    :
Name        : Administrator

AccountType : 512
Caption     : WIN-9FDQC8NU0HE\Admin_2
Domain      : WIN-9FDQC8NU0HE
SID         : S-1-5-21-3542280733-1080477990-1394795187-1002
FullName    :
Name        : Admin_2

AccountType : 512
Caption     : WIN-9FDQC8NU0HE\Guest
Domain      : WIN-9FDQC8NU0HE
SID         : S-1-5-21-3542280733-1080477990-1394795187-501
FullName    :
Name        : Guest

AccountType : 512
Caption     : WIN-9FDQC8NU0HE\Stag1
Domain      : WIN-9FDQC8NU0HE
```

    - Lister les processus en cours d'execution

    >Get-Process

```
PS C:\Users\Administrator> Get-Process

Handles  NPM(K)    PM(K)      WS(K) VM(M)   CPU(s)     Id ProcessName
-------  ------    -----      ----- -----   ------     -- -----------
    137      11     3116      11504    97    14.81   1992 conhost
     47       6      828       3604    52     0.02   2692 conhost
    252      11     1688       3444    42     0.83    336 csrss
    231      13     1732      12264    83    30.52   2108 csrss
    199      13     3208      10028    48     0.45   1748 dllhost
    244      31    27028      44776   149    12.22   2968 dwm
   1628      89    71284     126828   544    79.20   2112 explorer
      0       0        0          4     0              0 Idle
    678      19     3980       9468    37     4.55    516 lsass
    906      15     8608      18148   172     0.45   2168 msdt
    162      12     2288       6660    40     0.05   1804 msdtc
    609      37    79248      92396   638     7.33    728 powershell
    368      41    46404      59292   616     2.27   2716 sdiagnhost
    499      48   106132     112324   757    33.58   1096 ServerManager
    207       9     2372       5340    18     6.34    508 services
     52       2      292       1028     4     0.02    216 smss
    381      20     3136       8744    70     0.31   1052 spoolsv
    372      33     9992      11756    52     2.92    304 svchost
```

- Lister les mises a jour installees sur votre serveur

>Get-Hotfix

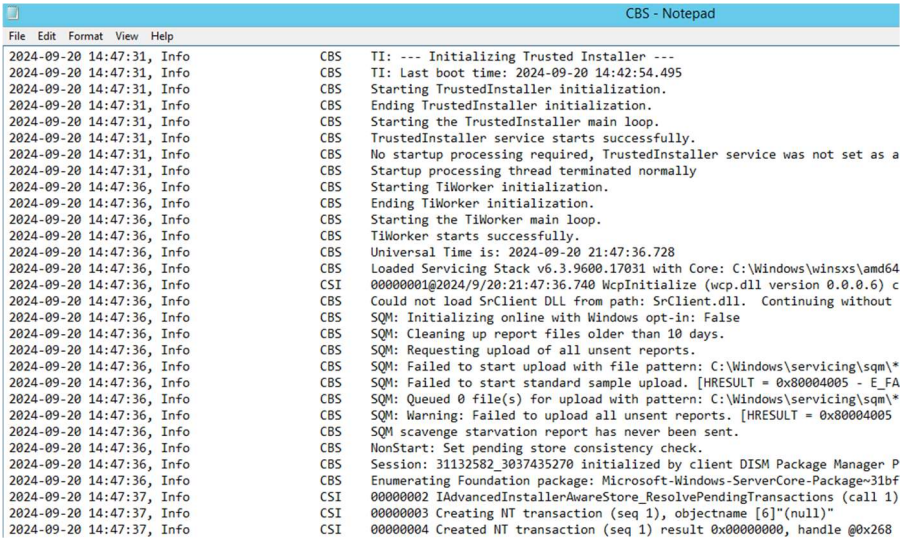
```
   Connection-specific DNS Suffix  . : localdomain
PS C:\Users\Administrator> Get-Hotfix

Source        Description      HotFixID      InstalledBy          InstalledOn
------        -----------      --------      -----------          -----------
WIN-9FDQC8... Update           KB2919355     WIN-9FDQC8NUOHE\A... 3/21/2014 12:00:00 AM
WIN-9FDQC8... Update           KB2919442     WIN-9FDQC8NUOHE\A... 3/21/2014 12:00:00 AM
WIN-9FDQC8... Update           KB2937220     WIN-9FDQC8NUOHE\A... 3/21/2014 12:00:00 AM
WIN-9FDQC8... Update           KB2938772     WIN-9FDQC8NUOHE\A... 3/21/2014 12:00:00 AM
WIN-9FDQC8... Update           KB2939471     WIN-9FDQC8NUOHE\A... 3/21/2014 12:00:00 AM
WIN-9FDQC8... Hotfix           KB2949621     WIN-9FDQC8NUOHE\A... 3/21/2014 12:00:00 AM
WIN-9FDQC8... Update           KB2999226     WIN-9FDQC8NUOHE\A... 9/20/2024 12:00:00 AM
```

13. Proposez une stratégie technique pour vérifier par analyse à froid que le système est à jour dans ses correctifs de sécurité.

    The documentation found at https://learn.microsoft.com/en-us/windows/deployment/update/windows-update-logs suggests to us that for our Windows Server 2012 R2 machine, we are interested is just the following file:

Log file	Location	Description	When to use
CBS.log	%systemroot%\Logs\CBS	This log provides insight on the update installation part in the servicing stack.	To troubleshoot the issues related to Windows Update installation.

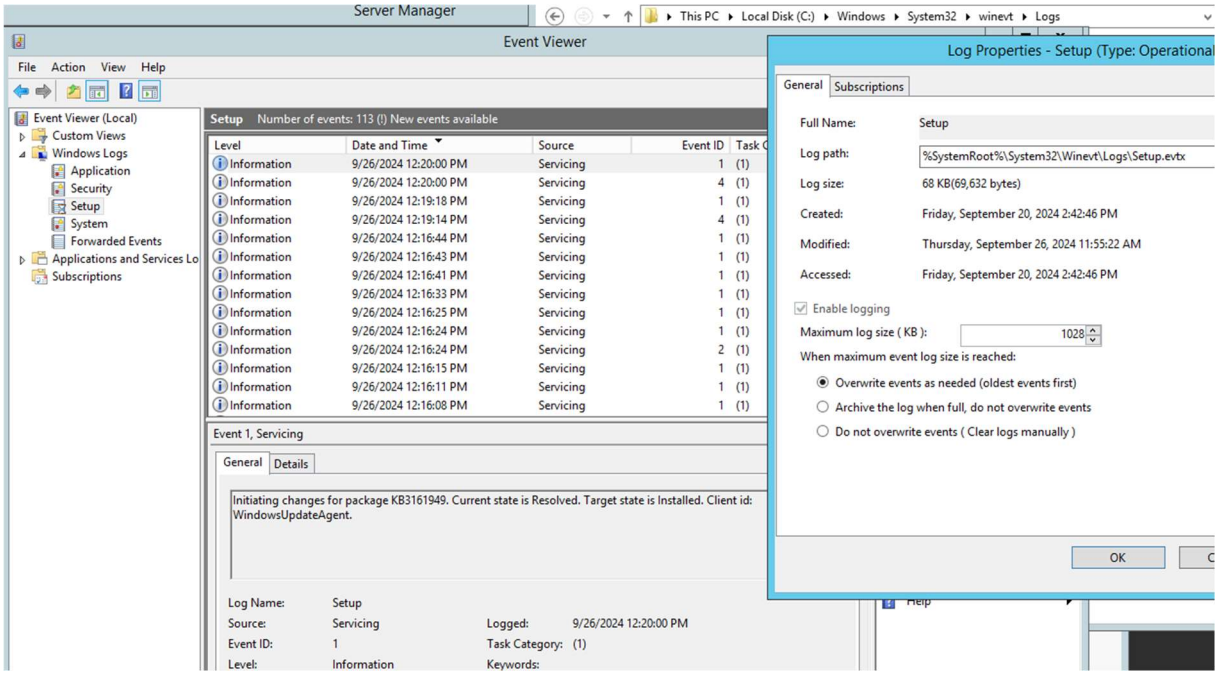
To obtain it, we can either boot from a live USB and copy our file or use shadow copy (a short summary/example of the steps is found in exercise 9).



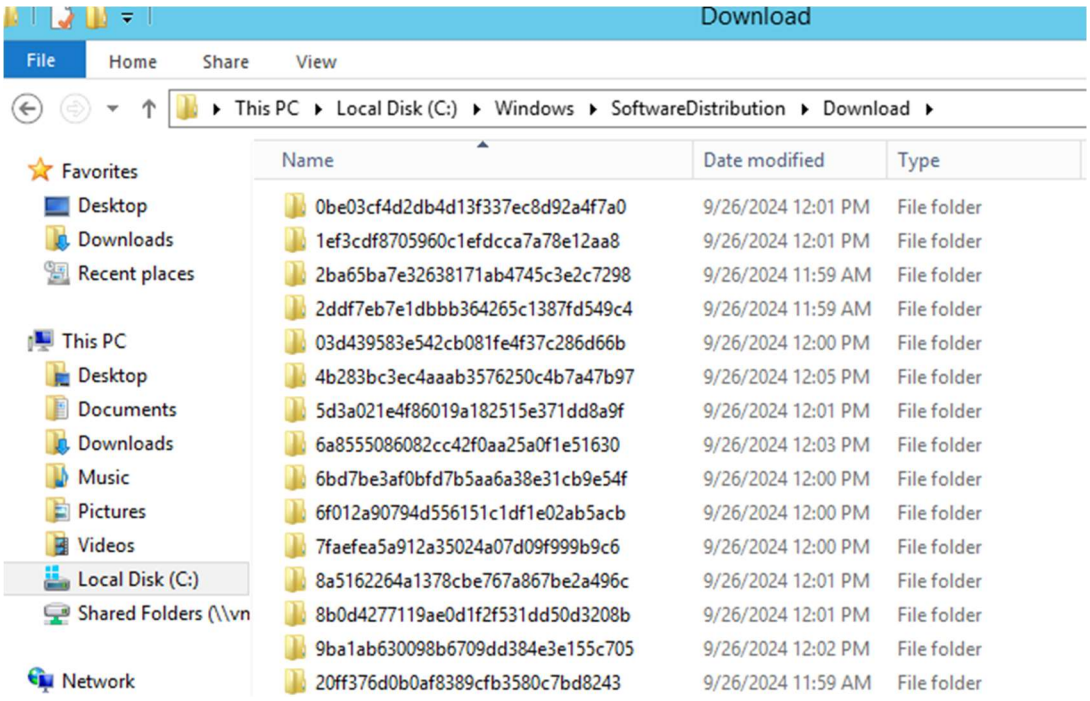
Example of CBS.log

Theoretically, we would cross-referrence the information gathered with Microsoft Security Update Guide. For newer versions of Windows, we would also check the C:\Windows\Logs\WindowsUpdate\windowsupdate.log.

In my exercise, after starting an update and looking through EventViewer -> Windows Logs, I could find that update events are logged in the Setup category. So another file of interest is located at C:\System32\Winevt\Logs\Setup.evtx. Also, temporary files for updates are stored at C:\Windows\SoftwareDistribution\Download.



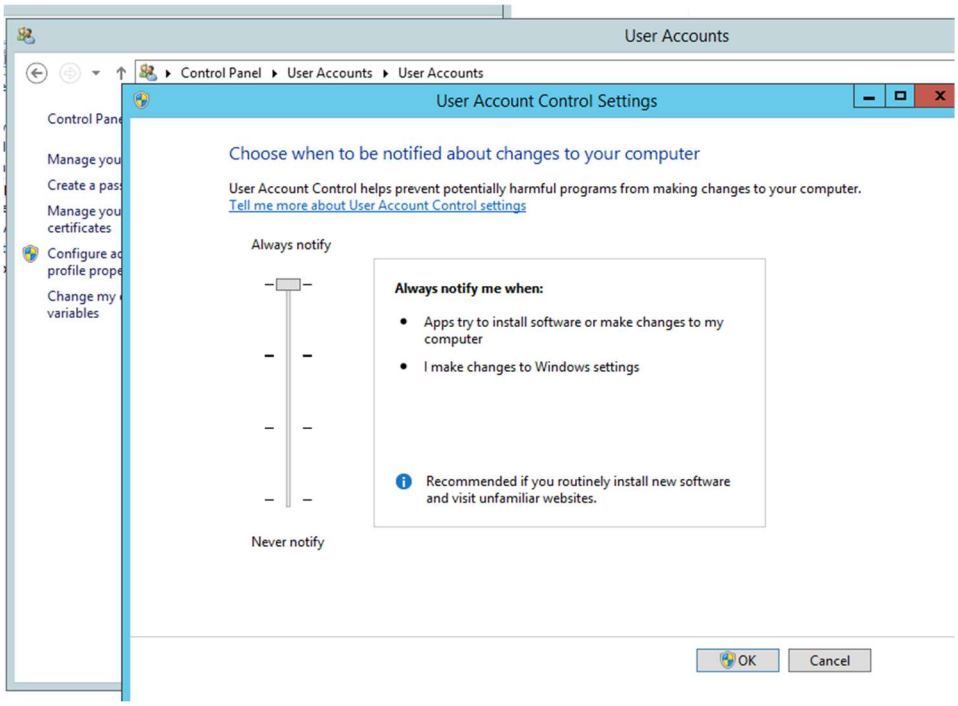
EventViewer -> Windows Logs -> Setup : events for any setup/update operation



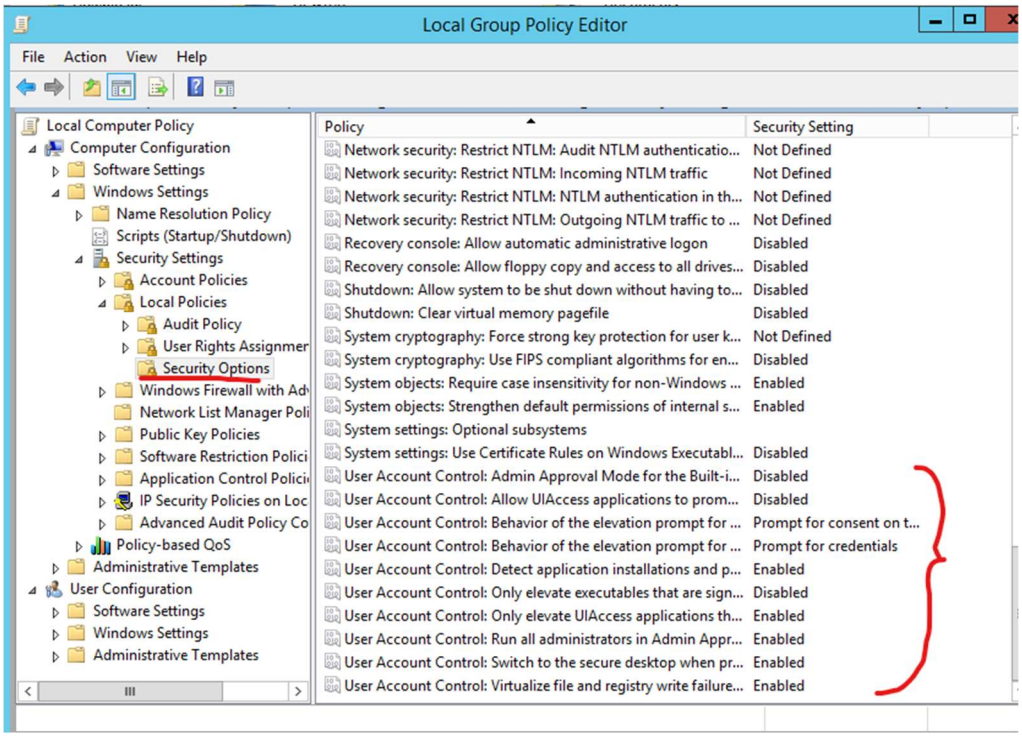
Temporary files for updates are stored in %WINDIR%\SoftwareDistribution\Download

14. Qu'est ce que l'UAC? Comment est-il configuré par défaut ? Quelles sont vos recommandations ? Appliquez-les.
    https://learn.microsoft.com/en-us/windows/security/application-security/application-control/user-account-control/
    User Account Control (UAC) is a Windows security feature designed to protect the operating system from unauthorized changes. When changes to the system require administrator-level permission, UAC notifies the user, giving the opportunity to approve or deny the change. UAC improves the security of Windows devices by limiting the access that malicious code has to execute with administrator privileges.

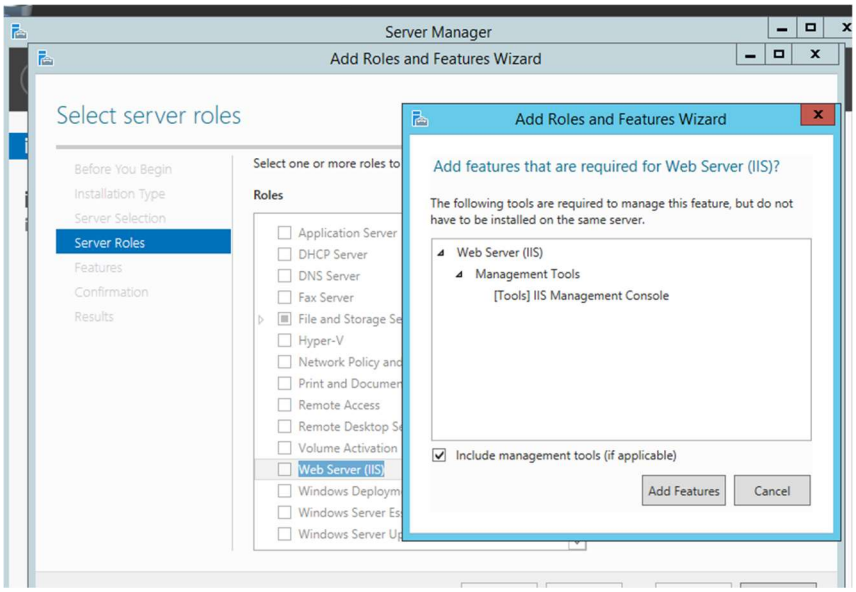
UAC is enabled by default, and you can configure it if you have administrative privileges. Going to ‚Control Panel' -> ‚User Accounts' -> ‚Change User Account Control setting' we can check and modify the level of alerts. In a professional environment, it's best to keep it at the highest level.



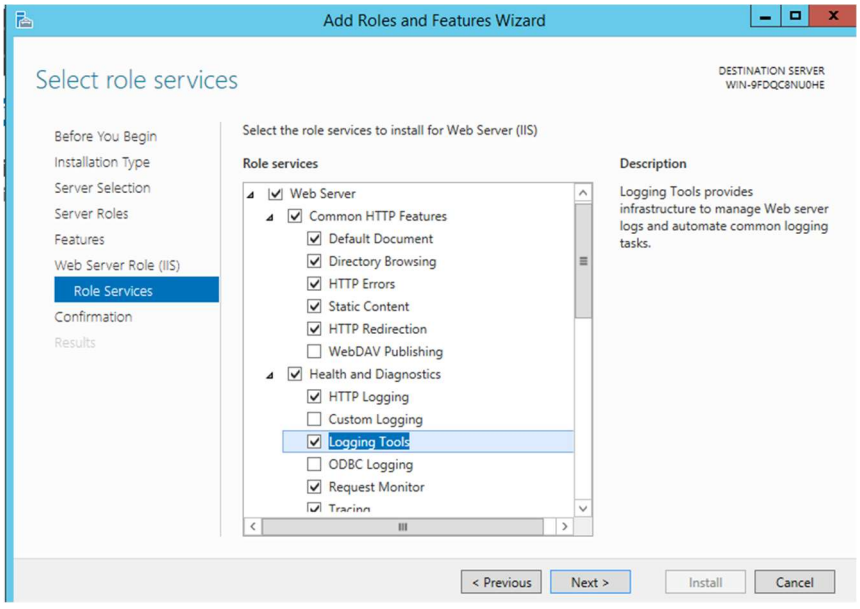
For more security options related to UAC, we have to go Group Policies Manager, by pressing Win+R and executing „gpedit.msc". In the following image i have highlighted the section we are interested in. An administrator should check all of these options so he can enable everything deemed necessary to properly secure the system.



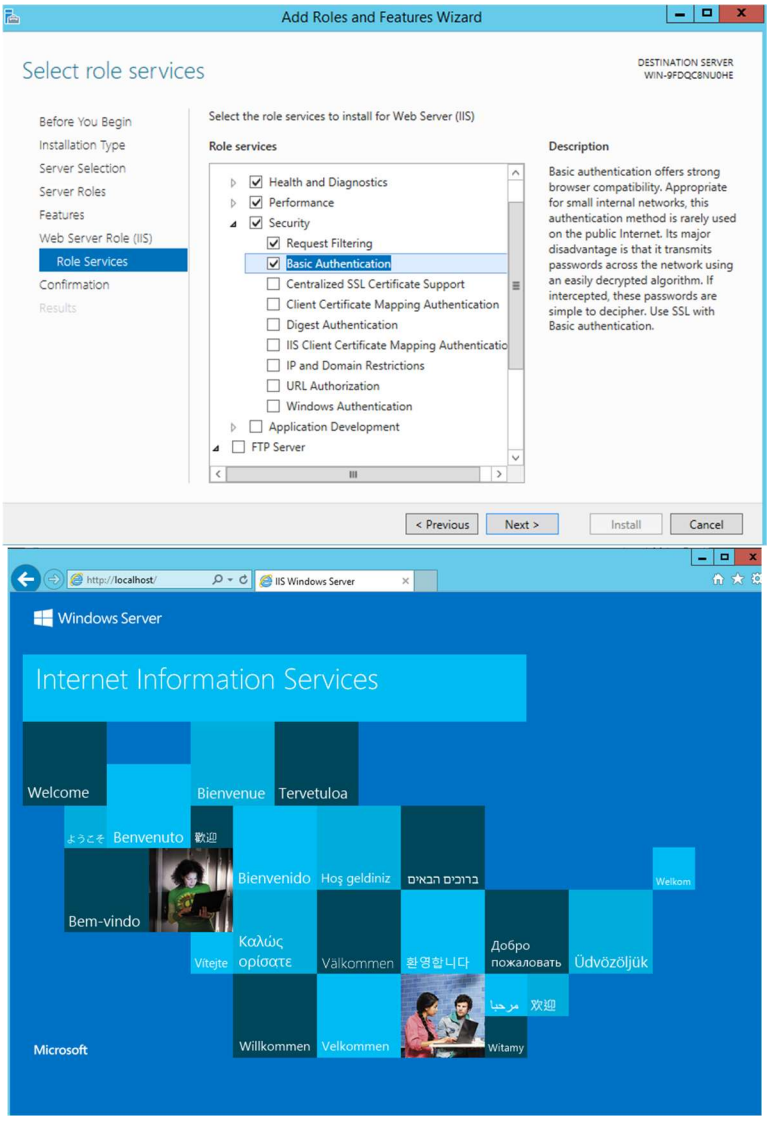
15. Installez un serveur IIS suivant votre serveur Windows. Configurez le en suivant les meilleures pratiques de sécurité. Expliquez votre démarche et votre mise en oeuvre.
Following the documentation found at learn.microsoft.com/en-us/iis/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012, to install an IIS web server we need to go to Server Manager -> Add roles and features and select the option for it.



The next step is to check what role services should our web server have. We take into consideration Logging, Requests monitoring, authentification and encryption tools, etc., but limit IIS features to essentials only.

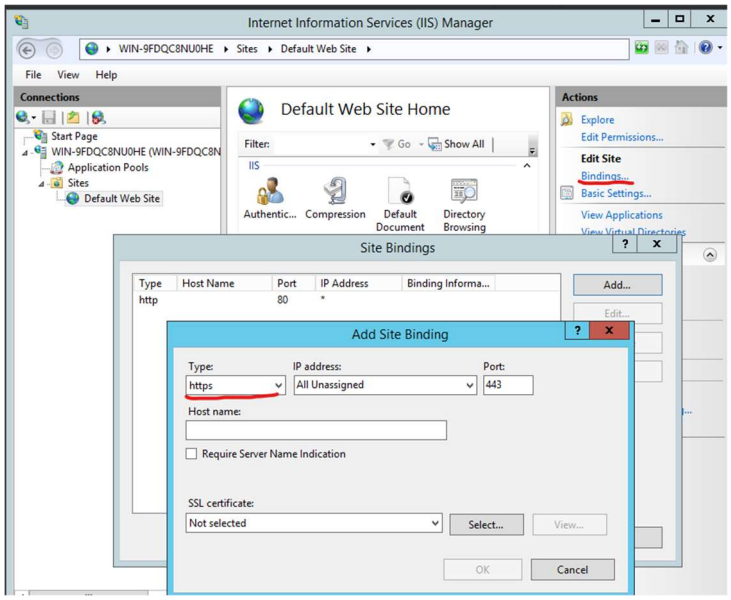


Install Wizard – role services for IIS web server



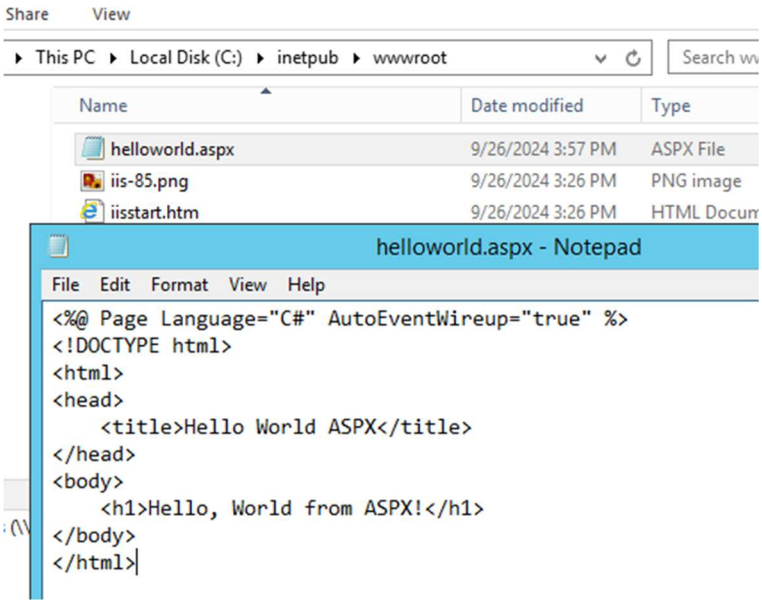
Our web server is up!

IIS manager is the management application. From here, we can disable any unused modules (this reduces the attack surface), configure access rights to the web directories as to ensure the least privileges, enable logging and monitoring, or configure HTTPS and disable HTTP, setting proper authentication and authorization and many more. As a bonus step, the web server could be tested for vulnerabilities to identify potential security issues.



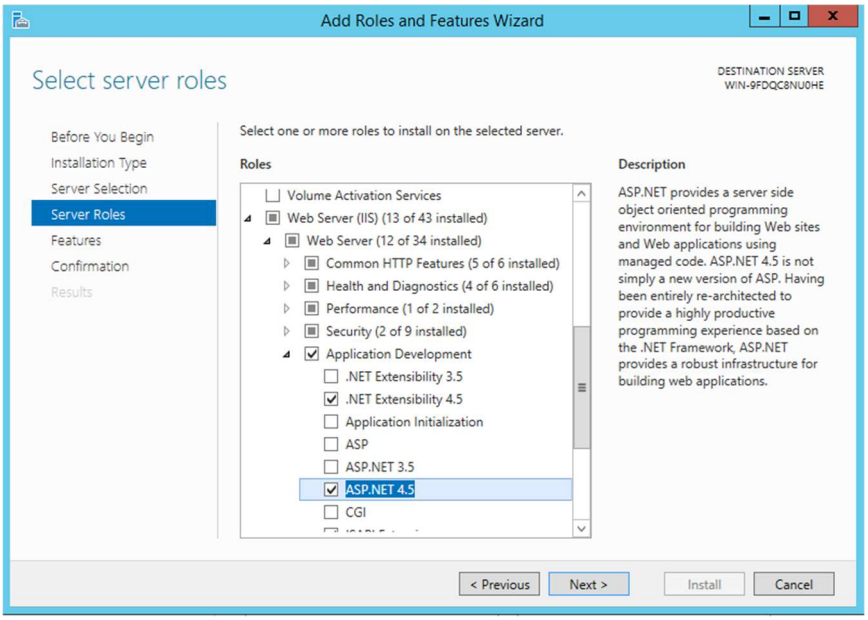
Configuring HTTPS

16. Déposez une page Helloworld ASPX à la racine de votre serveur. Exposez cette ressource sur une interface réseau. Montrez que vous pouvez accéder à la page depuis votre système Hôte.
    Sources:
    https://www.youtube.com/watch?v=VMyMag9_vmc
    https://learn.microsoft.com/en-us/aspnet/core/tutorials/publish-to-iis?view=aspnetcore-8.0&tabs=visual-studio
    We will start by creating a file named „helloworld.aspx" inside or web server root (C:\inetpub\wwwroot).

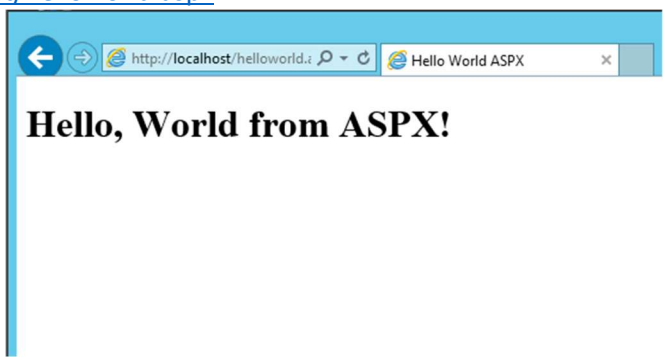


helloworld.aspx

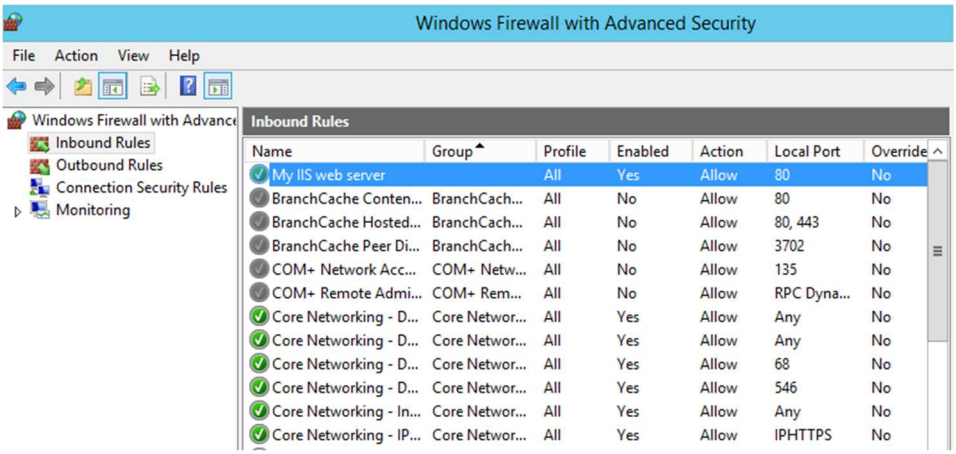
Next step is to enable the ASP.NET feature. Server manager -> Add feature and roles -> Install wizard -> Roles, check under IIS - Application development -> ASP.NET.



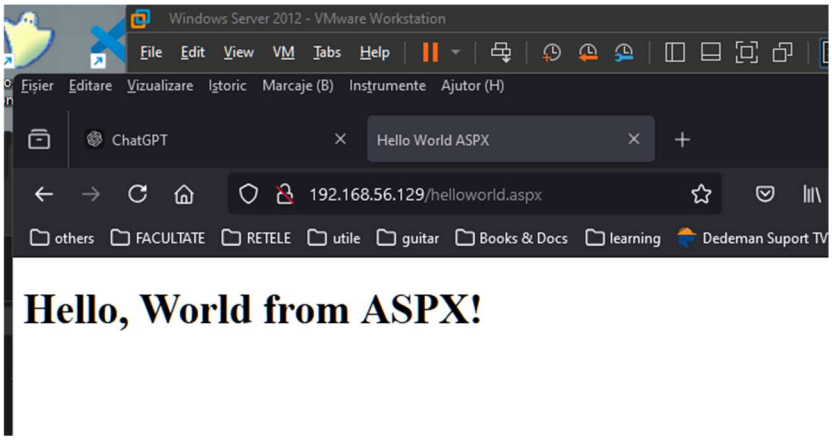
After installation is done, we can check if helloworld.aspx is accesible by navigating to http://localhost/helloworld.aspx.



To bind it to the network interface, we check in IIS manager -> Sites -> ‚Default Web Site' -> bindings. We ensure that there is a HTTP binding with an appropiate IP address (or unassigned, for our case) and port 80. Then, in Windows Firewall we create a new inbound rule for port 80 to allow traffic.



Finally, we test access from the host machine.



Accesible from the host machine

17. Citez deux méthodes pour se connecter à distance sur votre serveur Windows (méthodes "nativement" supportées). Décrivez rapidement les 2 services / protocoles et les ports par défaut sur lesquels ils sont exposés. Depuis un hôte Linux, connectez-vous à distance à votre serveur en utilisant des clients initiés en ligne de commande.
    There are two primary methods natively supported:
    - Remote Desktop Protocol (RDP)

    Remote Desktop Services (RDS) use RDP (TCP, port 3389) to allow graphical remote access [https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/remote-desktop-services-overview].win
    - Windows Management Instrumentation (WMI) over Windows Remote Management (WinRM)

    Windows Remote Management (WinRM) is the Microsoft implementation of the WS-Management protocol, which is a standard Simple Object Access Protocol (SOAP)-based, firewall-friendly protocol that allows interoperation between hardware and operating systems from different vendors [https://learn.microsoft.com/en-us/windows/win32/winrm/portal]. It uses ports 5985 for HTTP (unsecured, rare) and 5986 for HTTPS (secured with SSL/TLS).

    For remote access to our Windows Server we need to check:
    - RDP is enabled (System -> Remote -> Allow remote connections
    - Firewall inbound rules permit traffic
    - Firewall profile is set to Private / Domain. In my case, this was blocking
      In Powershell:
      >Get-NetConnectionProfile # check profile and get exact network name
      >Set-NetConnectionProfile -Name " Network-Name" -NetworkCategory Private

To connect from a Linux host, we can use ‚rdesktop' [https://blog.helpwire.app/rdesktop-linux/].

>rdesktop $ipaddress