what did you find?

how did you find it?

how did you exploit it?

what was the impact?

how can it be fixed/mitigated?

Lab 1:

Category 1:

**Finding passwords**

**Vulnerability 1: Storing plain text passwords**

Users can store passwords in plain text files somewhere on the machine like in the documents folder. You can find these plain text passwords easily by searching for documents with names like passwords.txt or other names.

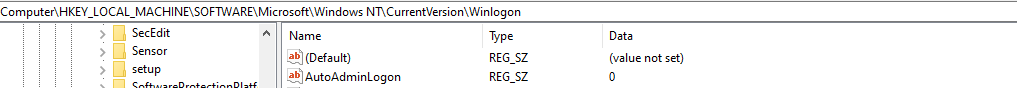
Exploiting this vulnerability is easy because the user stored his password in plain text and because of this you can easily get the credentials of the user

It can be fixed/mitigated by using programs like Keepass or

Password in plain tekst file ergens gezet door de gebruiker

**Vulnerability 2:**

Password in registry editor

**Vulnerability 3:**

Cpassword in xml file van [\\CSTLAB.local](file:///\\CSTLAB.local) en dan zoeken voor een \*xml bestand genaamd groups

**Vulnerability 4:**

Oude versie van windows (end of service)

Category 2: privilege escalation

**Vulnerability 5: (unquoted service path)**

Geen description in windows service,

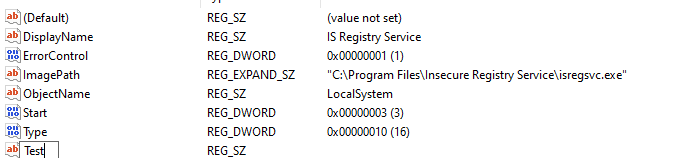
Purpose = privilege escaltion (mitre attack framework)

**Vulnerability 6: insecure registry permissions (**privilege escalation)

IS Registry Service

Registrysvc

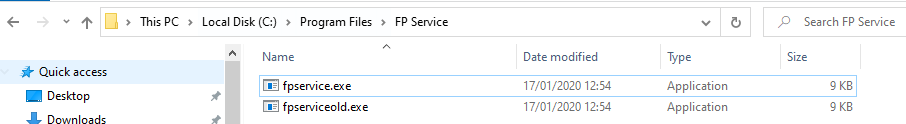
HKLM\SYSTEM\CurrentControlSet\Services



Cmd.exe /c net user /add backdoor B@ckd00r123 && net localgroup administrators backdoor /add

"C:\Program Files\Insecure Registry Service\isregsvc.exe"

**Vulnerability 7 (weak filesystem permissions)**

****

**Vulnerability 8 DMT service (insecure permissions inside service control manager)**

**Dmtsvc**

Sysinternals suite

Accesschk -uwvqc “Everyone” \*

Accesschk64 -uwvqc “Everyone” \*

RW DMTSVC

SERVICE\_CHANGE\_CONFIG kan je veranderen HW hoe exploit je dat

**Vulnerability 9**

C:\Temp netcheck notepad file

Les 2: <->

**Vulnerability 10 (?)**

**Sysinternals**

**Accessschk -uwvqc “Everyone” \***

**Accessschk -uwvqc “lowpriv” \***

**“cmd /c net user fakeadmin1 /add && net localgroups administrators”**

Sc query dmtsvc

SC start dmtsvc

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

Cd\temp\up\sys

Sc config dmtsvc binpath=””

Check computer management of user daaar toegevoegd is

Dit is geen vulnerability

dmt service vulnerability

Fake.bat file convert to bat2exe om als executable te runnen daarna

The vulnerability will lie weak permission in file system, service control manager or ??

Fake.bat rename to fpservice.exe this can happen because weak permissions in file system

Vulnerability 12 (?)

Msiwrapper

Anything third party or homemade services are worth looking at

Alwaysinstallelevated

Hklm\software\policies\Microsoft\installer

hkcu\software\policies\Microsoft\installer

Vulnerability 13 (?) bad system management (administrative mistake)

Not access to location C:\Windows\System32\Tasks

This should only be allowed for administrators because

Vulnerability 14 privilige escalation

Event viewer

Windows log > System

Netcheck

Mytask2

Administrator deletes exe file from task but forgets to cleanup the scheduled task.

Vulnerability 15

Run mimikatz.exe in fake admin cmd window (start mimikatz.exe in temp\x64 folder)

Privilege::debug

(response privilege 20 OK)

Sekurlsa::logonpasswords

Administrator

Stup!dp4ss

**Sysinternals** suite gedownload staat op C temp (RW DMTSVC) k

What is Mimekatz, Mimikatz is both an exploit on Microsoft Windows that extracts passwords stored in memory and software that performs that exploit. It was created by French programmer Benjamin Delpy and is French slang for "cute cats".

Mimikatz is a tool that is commonly used by hackers and security professionals to extract sensitive information, such as passwords and credentials, from a system's memory.

How do you set debug in Mimikatz?

To do that, simply write 'privilege::debug'. The debug privilege allows debugging a process that they normally wouldn't have access to. Note: ERROR kuhl\_m\_privilege\_simple; RtlAdjustPrivilege (20) c0000061 means that you do not have the require privilege to run the command. Try running Mimikatz as an administrator.

* **Windows Services =** hoe insecure services vinden zonder description en exploiten. Accesschk -uwvqc “lowpriv” \* (moet je domain controller wel opgestart hebben anders everyone)
* Sc query dmtsvc deze service heeft een unquoted service path or is an insecure services en dit kan geëxploiteerd worden.
* Nog iets met sc config dmtsvc doen? Maakt .bat file genaamd fake. Forceren service te starten. (sc config dmtsvc=”cmd /c net user /add”?? commando checken). Met control S het file opslaan met bat fake.bat? De bat file (hoe uitspreken bash file?) in executable. Bat2.exe.net
* Are there weak permissions? FilePermissions Properties have executable en hier exe MSI Wrapper, software microsoft installer, veil framework. Microsoft MSI wrapper buiten virtual box gedownload en vervolgens geimporteerd in virtual box met shared file en vervolgens in module 5 windows omgeving gezet. WAAR?
* **Why did Mike mention Veil framework be carefull with tools or do we need to investigate this?**
* Hadden password gecheckt in eerste les of die niet ergens rond slingerde? Registry auto log, file system, build-in service in registry. Query everything in powershell. What is the **difference between command prompt (cmd) en powershell?** Through registry powershell password sysvol unattended.
* **Scheduled task**? Event manager of andere tool?
* **In Skill assessment Quick way, unquoted service path poor file permission(s), target machine how to find this? Name order? Similar system comparison. Via powershell or script…**
* Services running on a system, local services not powerful, local system, network… volgens mij is het .\ (not ./)
* Scheduled Task, where you type also Services or CMD now **Task Scheduler**
* **Onder** C:Windows, System32 Task, Je zou GEEN toegang moeten hebben tot System32 als lowpriv user dit is iets voor iemand met admin rechten. Zoeken naar netchecker. Poor system management not Microsoft. You can see tasks migrated (backup, of old taks). Event view via event manager or taks manager? Event viewer, Application Service (log), Microsoft, Windows, Task Scheduler zoeken… **(wat doen met c temp, bat, netcheck ??)** What task started, net check in operational create custom view. **Mytask2? 2 Scheduled taks, netcheck, drop bat.file, mytask2, binary which does have exe drop in folder get. Scheduled task. Start folder. System configuration, password, services, scheduled task.**

**Low privilege to admin. With these admin rights command prompt.**

**Cmd run asadministrator .\xxxx**

Windows Defender uitzetten is lateral movement (exclude in Windows Defender)

Mimikatz github. Remove debug from..

* All passwords in memory of uit memory halen, there are plaintext in memory. Wdigest (get password in plaintext). Credential manager, windows credentials, local host, password
* Mimikatz in temp, cd mimikatz -trunk ? (user rights, Never do it in local policy. Why it does not work…
* Via x64 group policy deny all, user debug psexec services are not?? Psexec -s -i cmd/ accepteula
* Whoami (psexec do your mimikatz (machine accunt $ at the end not particular usefull or does it make a file or folder invisable?
* NOT via SYSVOL, still the old way
* Angry IP Scanner downloaden, start, vind je admin 192.168.56.110 local repository?
* REAL ADMIN dir [\\192\168.56.110\C$](file:///\\192\168.56.110\C$) local build (it is **the same account, shared admin account across the domain**, **not using Windows LAPS**, local administrator password solution. <https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview>
* C$ (share) you do not see with $ build in share, you have your admin.
* Repro, bat, exe, msi, eigen admin te maken NIET REAL ADMIN
* REAL ADMIN with Mimikatz
* Defense evasion credentials, MIMIKATZ & Microsoft Defender excluding Wachtwoord Wdigest
* Local admin = Angry IP, Ps executable. Whoami? Dir [\\192.168.56.150\C$](file:///\\192.168.56.150\C$) (Local Administrator password solution= windows laps)
* Cd temp\, cd sys\ host name? Psexec image file execution, vulnerability Petya (PS exec) set a key in the registery service. Image file execution. Ps exec to copy psexe. (block petya, microsoft kwam met block psexe -r geen oplossing, psexe on remote machine. Moeten we hier iets mee doen, eerst iets lezen over Petya of het als kwetsbaarheid noemen..
* Onthou, we are still ourselves but with Tom (tinyco) his keys. We are admin on a domain controller. Dcsync to be a new domain controller
* All hashes in this lab (lmtl) l