Windows Attack Lab - Step 3 - Situational Awareness & Privilege Escalation on Windows 10 Client

After having established the initial connection to your Windows 10 client via RDP, we will first assess the situation on the machine. This should give you an idea about the available attack surface and possible options to escalate your privileges.

Your current user tmassie is a regular user on the machine and does not have local admin privileges.

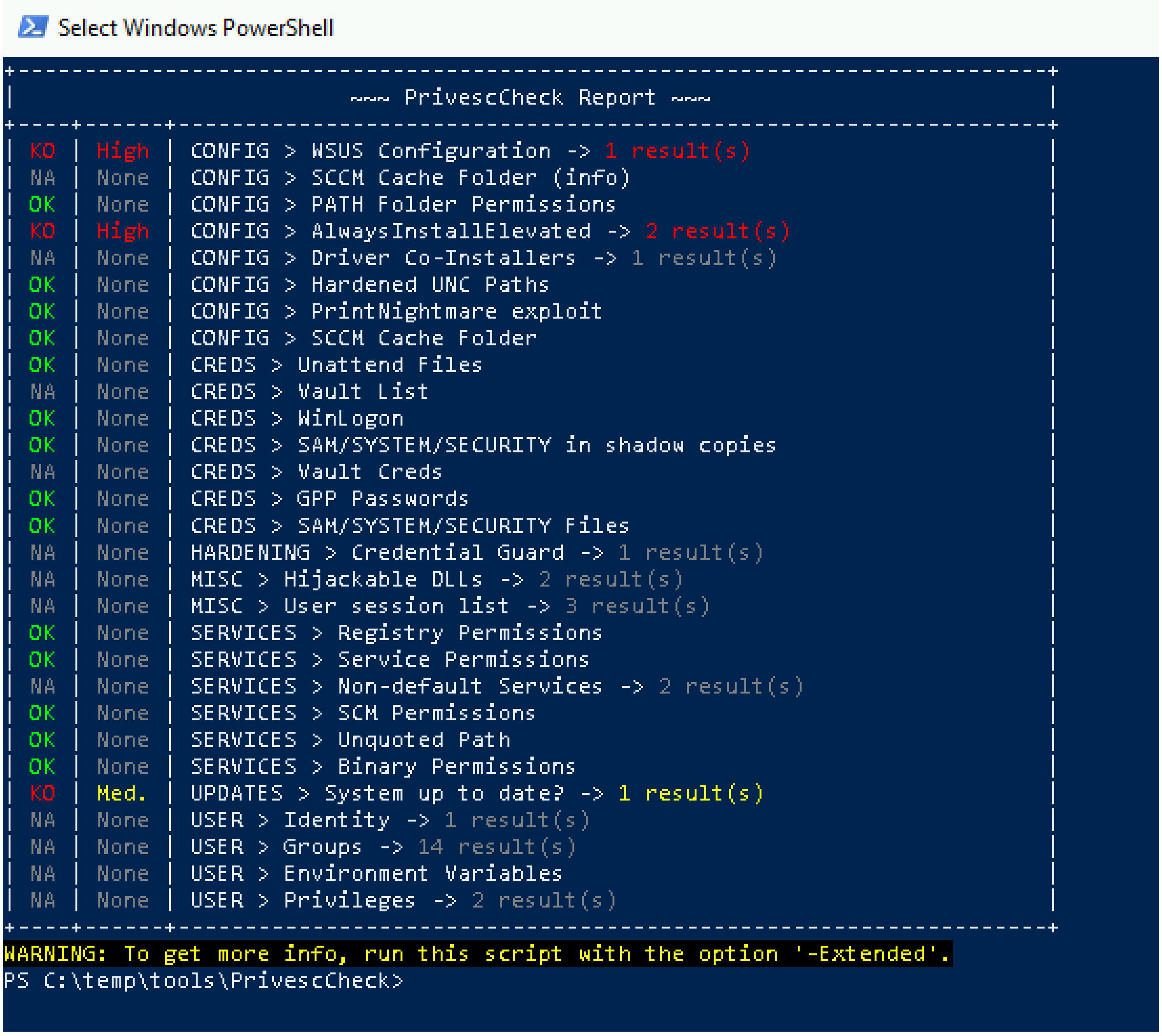
Author

- Knöpfel, Daniel
- Duijts, Michael

Methodology

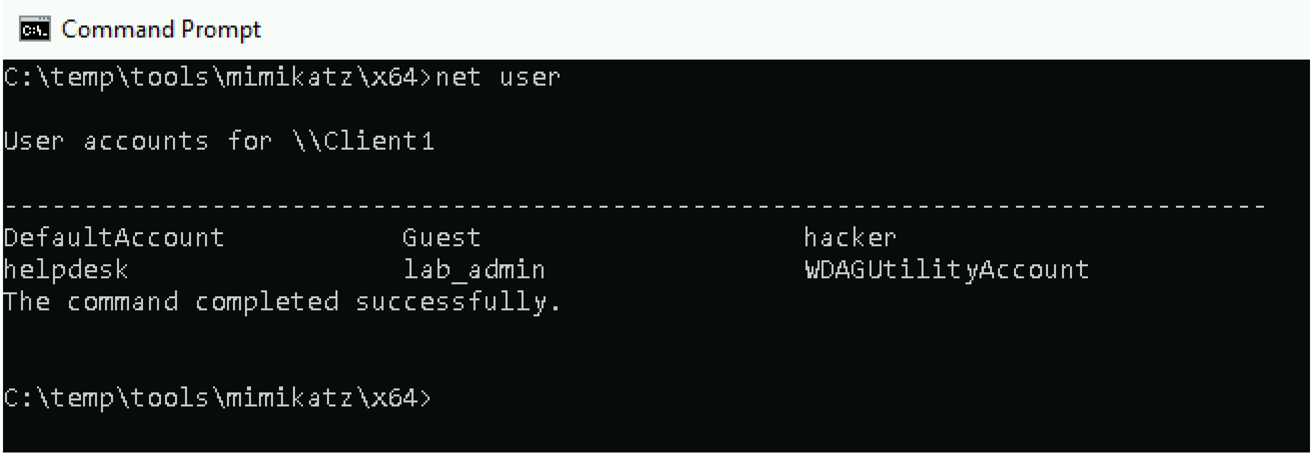
PrivescCheck

```
Import-Module .\PrivescCheck.ps1
Invoke-PrivescCheck
```



```
+------------------------------------------------------------------------------+
|                          ~~~ PrivescCheck Report ~~~                         |
+----+------+------------------------------------------------------------------+
| KO | High | CONFIG > WSUS Configuration -> 1 result(s)                       |
| NA | None | CONFIG > SCCM Cache Folder (info)                                |
| OK | None | CONFIG > PATH Folder Permissions                                 |
| KO | High | CONFIG > AlwaysInstallElevated -> 2 result(s)                    |
| NA | None | CONFIG > Driver Co-Installers -> 1 result(s)                     |
| OK | None | CONFIG > Hardened UNC Paths                                      |
| OK | None | CONFIG > PrintNightmare exploit                                  |
| OK | None | CONFIG > SCCM Cache Folder                                       |
| OK | None | CREDS > Unattend Files                                           |
| NA | None | CREDS > Vault List                                               |
| OK | None | CREDS > WinLogon                                                 |
| OK | None | CREDS > SAM/SYSTEM/SECURITY in shadow copies                     |
| NA | None | CREDS > Vault Creds                                              |
| OK | None | CREDS > GPP Passwords                                            |
| OK | None | CREDS > SAM/SYSTEM/SECURITY Files                                |
| NA | None | HARDENING > Credential Guard -> 1 result(s)                      |
| NA | None | MISC > Hijackable DLLs -> 2 result(s)                            |
| NA | None | MISC > User session list -> 3 result(s)                          |
| OK | None | SERVICES > Registry Permissions                                  |
| OK | None | SERVICES > Service Permissions                                   |
| NA | None | SERVICES > Non-default Services -> 2 result(s)                   |
| OK | None | SERVICES > SCM Permissions                                       |
| OK | None | SERVICES > Unquoted Path                                         |
| OK | None | SERVICES > Binary Permissions                                    |
| KO | Med. | UPDATES > System up to date? -> 1 result(s)                      |
| NA | None | USER > Identity -> 1 result(s)                                   |
| NA | None | USER > Groups -> 14 result(s)                                    |
| NA | None | USER > Environment Variables                                     |
| NA | None | USER > Privileges -> 2 result(s)                                 |
+----+------+------------------------------------------------------------------+
WARNING: To get more info, run this script with the option '-Extended'.
PS C:\temp\tools\PrivescCheck>
```

Neuer User:



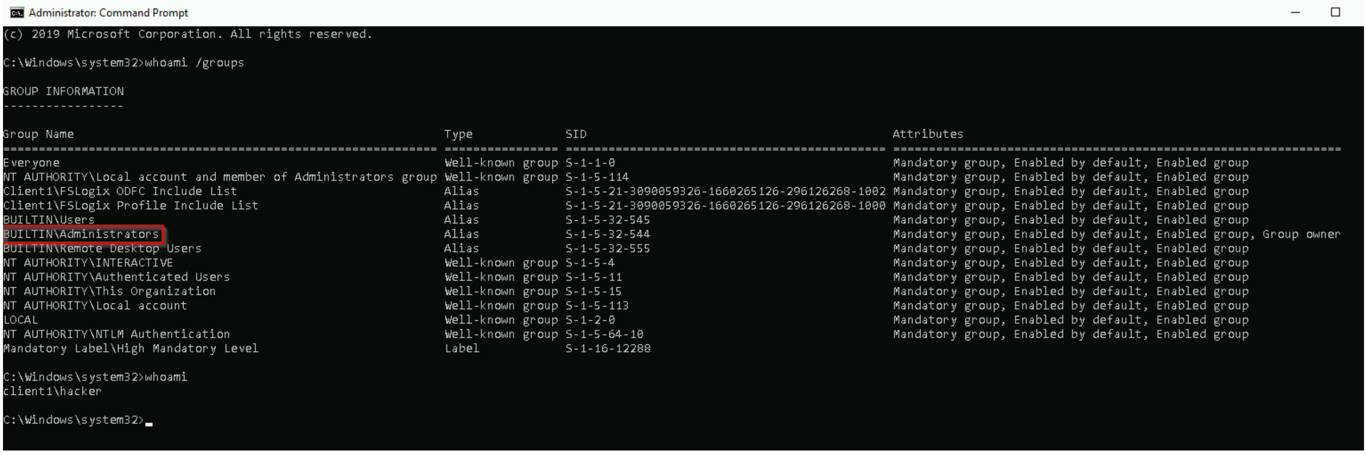
```
C:\temp\tools\mimikatz\x64>net user

User accounts for \\Client1

-------------------------------------------------------------------------------
DefaultAccount           Guest                    hacker
helpdesk                 lab_admin                WDAGUtilityAccount
The command completed successfully.


C:\temp\tools\mimikatz\x64>
```

Gruppen vom neuen User:



```
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami /groups

GROUP INFORMATION
-----------------

Group Name                                                    Type             SID                                           Attributes
============================================================= ================ ============================================= ===============================================================
Everyone                                                      Well-known group S-1-1-0                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account and member of Administrators group Well-known group S-1-5-114                                     Mandatory group, Enabled by default, Enabled group
Client1\FSLogix ODFC Include List                             Alias            S-1-5-21-3090059326-1660265126-296126268-1002 Mandatory group, Enabled by default, Enabled group
Client1\FSLogix Profile Include List                          Alias            S-1-5-21-3090059326-1660265126-296126268-1000 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                                                 Alias            S-1-5-32-545                                  Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                                        Alias            S-1-5-32-544                                  Mandatory group, Enabled by default, Enabled group, Group owner
BUILTIN\Remote Desktop Users                                  Alias            S-1-5-32-555                                  Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                                      Well-known group S-1-5-4                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users                              Well-known group S-1-5-11                                      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization                                Well-known group S-1-5-15                                      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account                                    Well-known group S-1-5-113                                     Mandatory group, Enabled by default, Enabled group
LOCAL                                                         Well-known group S-1-2-0                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication                              Well-known group S-1-5-64-10                                   Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level                          Label            S-1-16-12288

C:\Windows\system32>whoami
client1\hacker

C:\Windows\system32>_
```

Answers

- Explain the vulnerability you used for privilege escalation.
  - The registry setting "AlwaysInstallElevated" is set to 1 (for machine and user). This means that any msi installer runs as admin without the UAC dialog prompting the user to confirm or enter username/password (which is what would happen on the used windows machine)
- Can you use the new user account to log on to another machine and why?
  - No, the created user is a local account
- Explain if the cmd.exe was started in an elevated context and how you can tell that from the output of whoami /groups?
  - we see that the hacker belongs to the Administrators group (BUILTIN\Administrators).
- If yes, explain how you “bypassed” UAC?
  - As explained before, we managed to create an admin user via Msi and the "AlwaysInstallElevated" vulnerability. We can now use our admin user for any UAC prompt.
- How can you prevent such an attack?
  - Ensure "AlwaysInstallElevated" is NOT set to 1 (true).