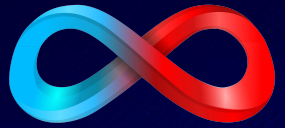
# Certified Impersonation ADCS ESC2 Abuse

# 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 these  primary divisions:

1. Cyber Range Labs
2. Up-Skilling Platform
3. Infinity Learning Platform

CWL provides customized on-site training for organizations and accepts bulk orders for corporate upskilling. For inquiries or more details, feel free to reach out at **support@cyberwarfare.live.**

# About Speaker

## Ranjitha V

Security Engineer@CWL

Ranjitha V is a Blue Team Security Engineer at CyberWarfare Labs. Interested in Cloud and On-Premise Defense Operations.

# What is AD CS?

- Active Directory Certificate Services is Microsoft's Public Key Infrastructure (PKI) solution used in Active Directory environments.
- It allows organizations to issue and manage digital certificates for users, computers, and services.
- These certificates are trusted across the domain and can be used for authentication.

# Important Components in AD CS

- Certificate Authority (CA)
  - The trusted server responsible for issuing certificates.
- Certificate Templates
  - Define the rules for certificate enrollment.
- Certificates
  - Digital identities used for authentication.
- Private Key
  - A secret key linked to the certificate.

# Why Attackers Target AD CS

- AD CS is highly trusted inside Active Directory.
- If misconfigured, attackers can:
    - Request certificates for privileged users
    - Authenticate without passwords
    - Maintain persistence
    - Bypass password resets

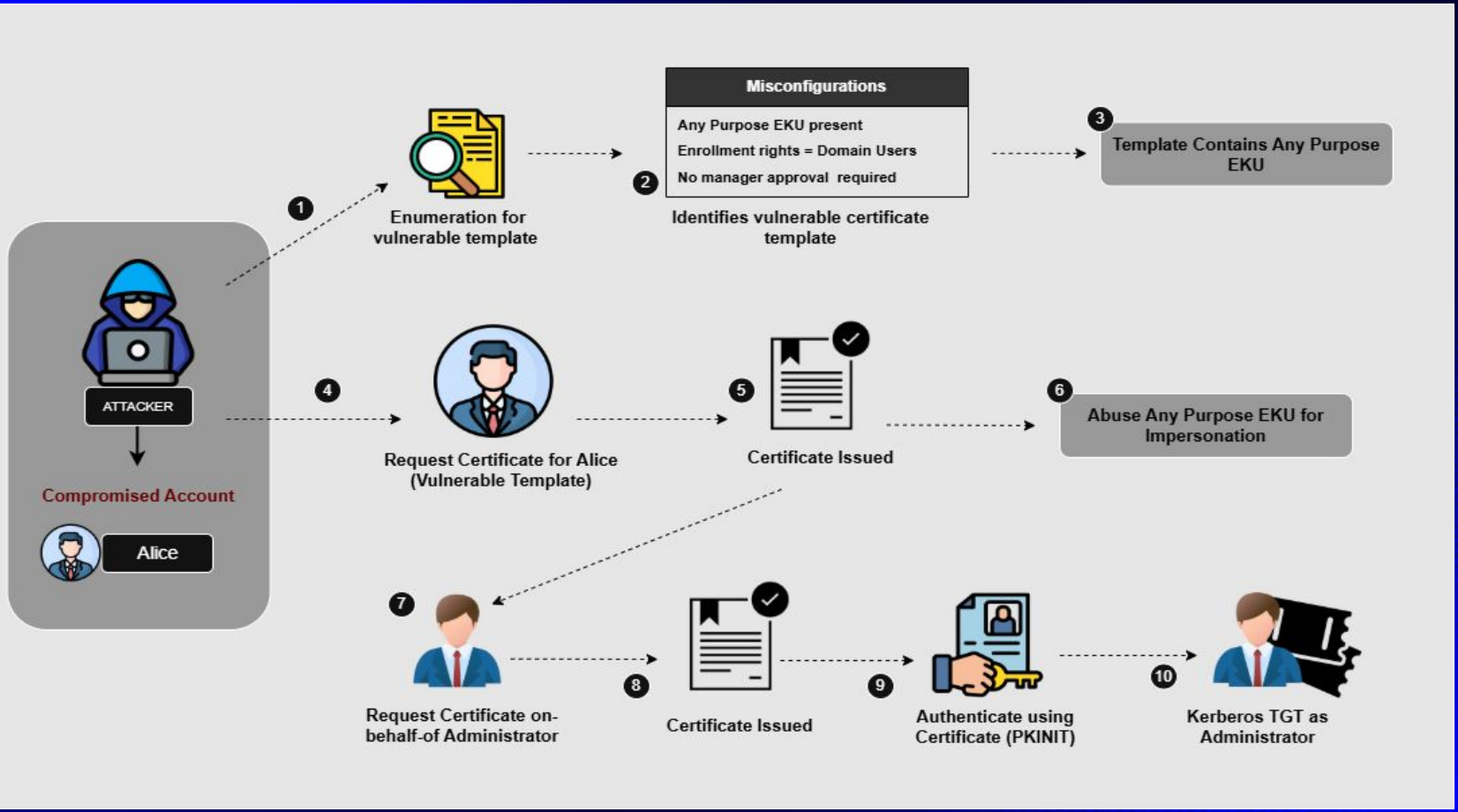
# What is ESC2?

- ESC2 is an AD CS misconfiguration where a certificate template contains the Any Purpose EKU or does not properly restrict certificate usage.
- EKU stands for Enhanced Key Usage.
- It defines what a certificate can be used for, such as:
    - Client Authentication
    - Smart Card Logon
    - Code Signing

# Why ESC2 Happens ?

- Low Privileged Users Can Enroll
- Any Purpose EKU is Present
- Authentication is Allowed
- No Approval Requirement
- Result
    - Attackers may obtain certificates that can be abused for authentication and privilege escalation.

# ESC2 Attack Flow



# ESC2 Detection


LOGGING


1. Detect Initial Access By Compromised Account
2. Detect Enumeration Activity by Compromised Account
3. Detect Certificate Requests by Compromised Account
4. Correlate Certificate Issuance and Confirm ESC2 Abuse
5. Detect Kerberos Authentication Using Certificate

# Preventing ESC2 Abuse

- Secure Certificate Templates
    - Remove unnecessary enrollment permissions
    - Restrict low privileged user access
    - Avoid using “Any Purpose EKU”
    - Define only required EKUs
    - Require Approval
- Enable manager approval or authorized signatures before certificate issuance.

# Preventing ESC2 Abuse

- Regular Auditing
    - Review certificate templates regularly for insecure configurations.
- Monitoring
    - Certificate requests
    - Certificate issuance
    - Authentication using certificates

# Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings

Please Contact :

**support@cyberwarfare.live**

To know more about our offerings, please visit: **https://cyberwarfare.live**