FROM USER TO DOMAIN CONTROLLER

A Journey through the Critical ADCS Vulnerability in Active Directory

Agenda

- INTRODUCTION
- UNDERSTANDING ACTIVE DIRECTORY AND ADCS
- THE INTRICATE WEB OF VULNERABILITY
- TECHNICAL DEEP DIVE
- EXAMPLE SCENARIO
- PRACTICAL DEMONSTRATION
- IMPACT AND CONSEQUENCES
- CYBERSECURITY RESEARCH IMPORTANCE
- CONCLUSION
- Q&A

About Me

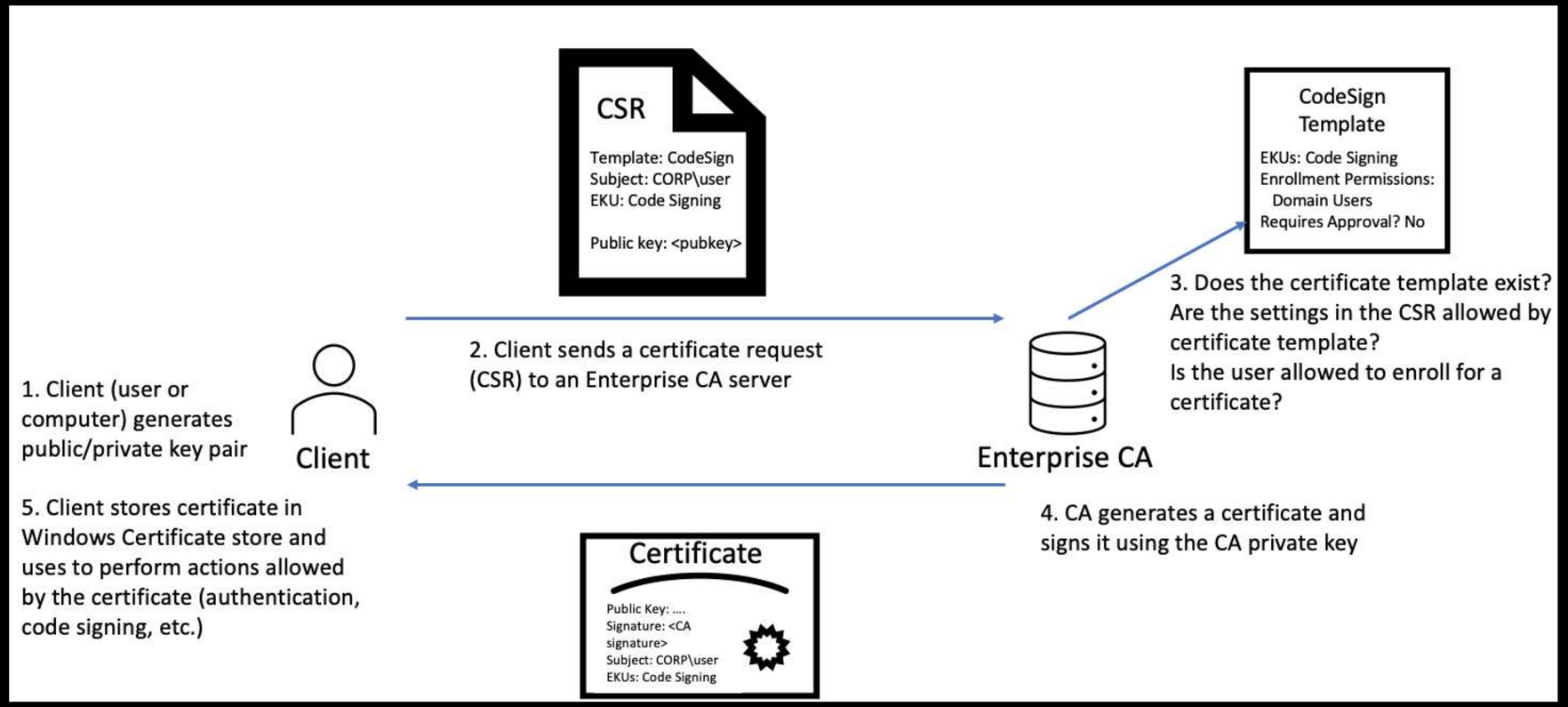
- AppSec Engineer @MoveInSync
- Security Researcher
- CEH Practical v11
- Oracle Cloud Infrastructure Foundations Associate 21'
- β Microsoft Learn Student Ambassador
- Head of Community @NOOB_4rMY
- CTF Admin and Challenge Creator (Bsides)
- Public Speaker, DevSecOps, Cloud

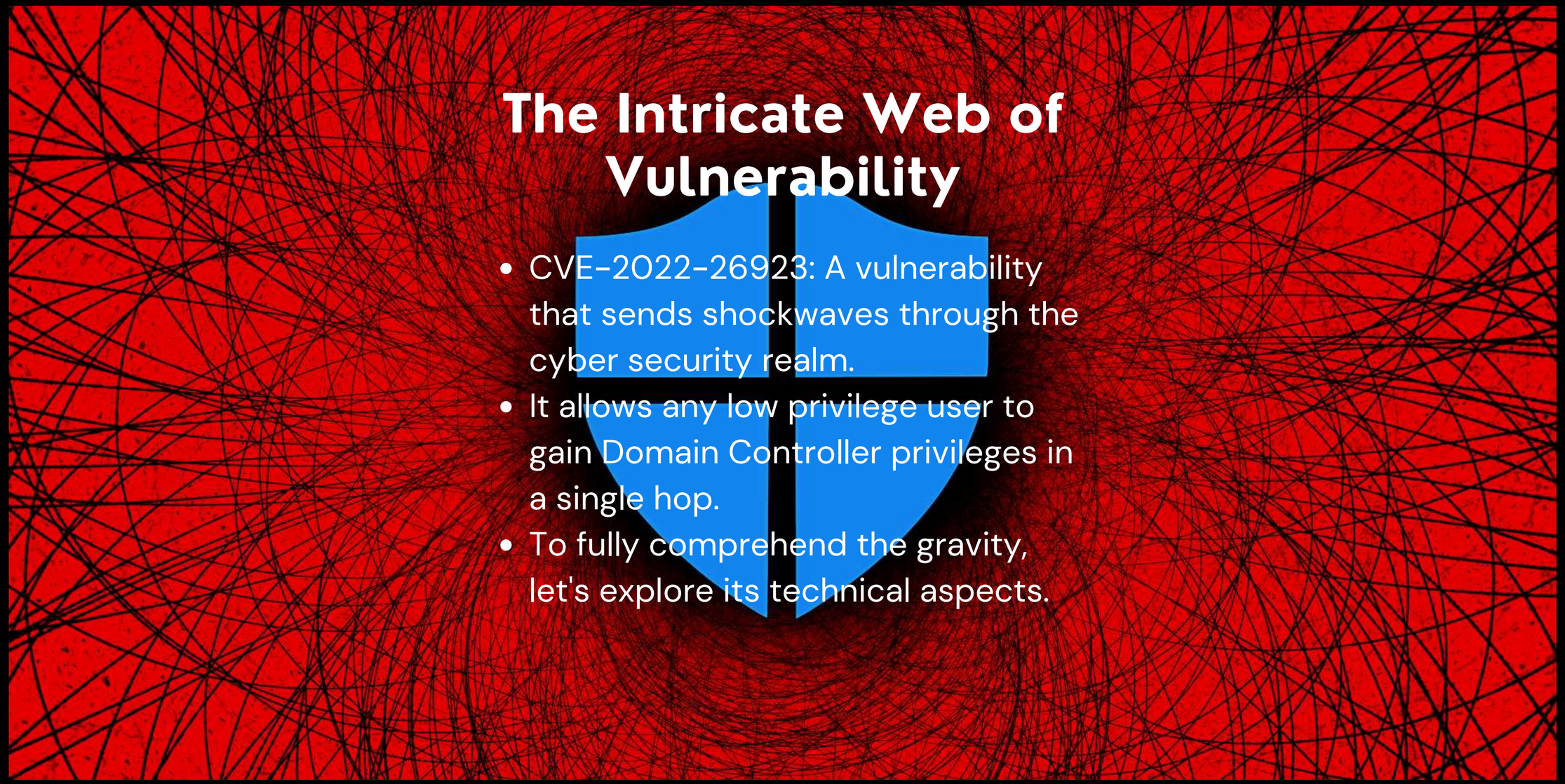
Introduction

Today, we dive into the dark underbelly of cyber security.
Brace yourselves as we uncover a critical vulnerability that threatens the very heart of Active Directory.
Get ready to explore CVE-2022-26923 and its potential consequences.

Understanding Active Directory and ADCS

- AD is Microsoft's centralized identity management system used by countless organizations.
- Manages authentication, authorization, and other network services.
- Active Directory Certificate Services (ADCS) is a server role that functions as Microsoft’s public key infrastructure PKI implementation





The Intricate Web of Vulnerability

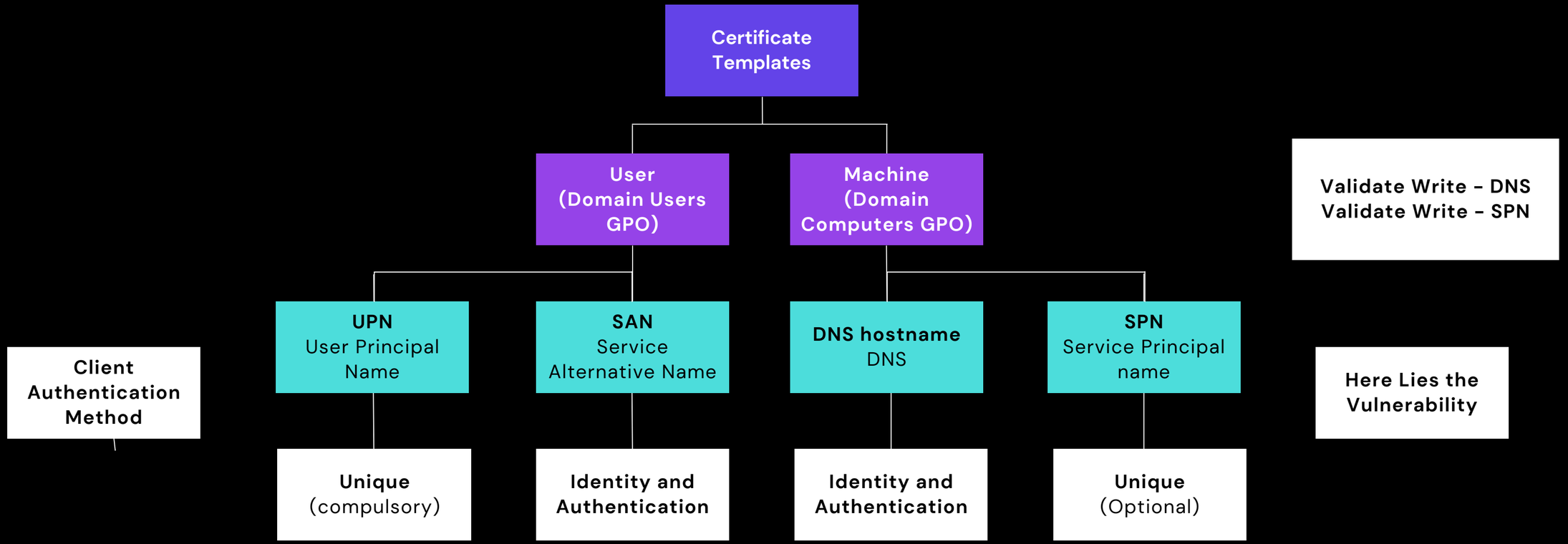
- CVE-2022-26923: A vulnerability that sends shockwaves through the cyber security realm.
- It allows any low privilege user to gain Domain Controller privileges in a single hop.
- To fully comprehend the gravity, let's explore its technical aspects.

Technical Deep Dive

- The vulnerability stems from an insecure configuration in Active Directory Certificate Services (ADCS).
- Exploit involves manipulating the Extended Key Usage (EKU) and Key Usage (KU) fields of an X.509 certificate.
- Attacker crafts a rogue certificate using **Machine Certificate Template** with elevated privileges.
- Authenticates to the Certificate Authority (CA) service, gains Domain Controller privileges.

Now, to understand further, first we need to understand the Certificate templates why are we using them?

ADCS


Certificate Templates
User (Domain Users GPO)
Machine (Domain Computers GPO)
Validate Write - DNS
Validate Write - SPN
UPN
User Principal Name
SAN
Service Alternative Name
DNS hostname
DNS
SPN
Service Principal name
Client Authentication Method
Here Lies the Vulnerability
Unique
(compulsory)
Identity and Authentication
Identity and Authentication
Unique
(Optional)

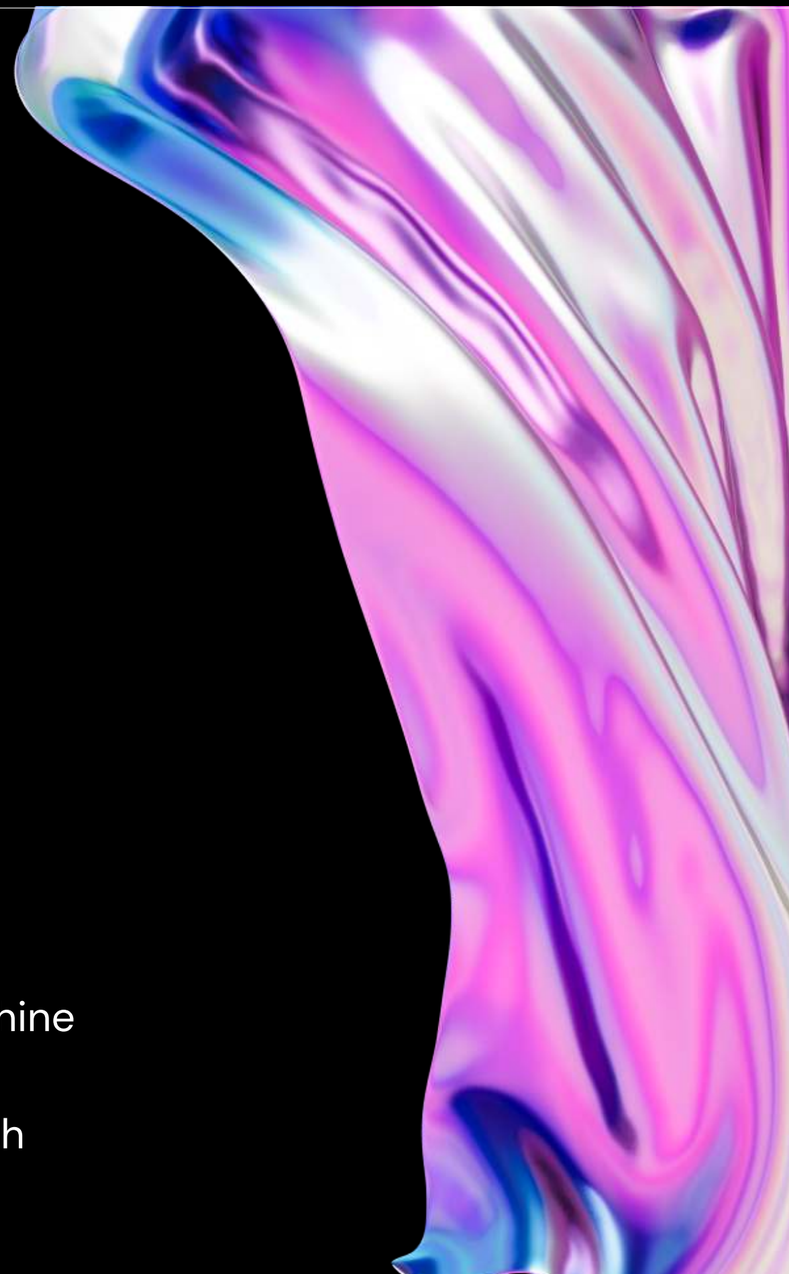
Why use Machine Cert Template?

BYOD feature

FOR USERS

Machine Accounts

UPTO 10



- Difficult for enterprises to issue certificates for all the BYODs
- So, USER get all admin writes for that BYOD, to issue certificates as well using machine template
- BYOD allows employees to use their preferred devices, which they are familiar with and comfortable using. This familiarity often leads to increased productivity

Practical Demonstration

Step 1

Compromise the creds of a low privelege AD user

Step 2

Use those creds to enroll a new host on the doman

Step 3

Alter the DNS hostname attribute of Computer AD Object to that of a privelege host, e.g., DC

Step 4

Remove the SPN attributed to bypass the unique SPN conflict issue

Step 5

Request Machine Certificate using default template

Step 6

Perform Kerberos Authentication with the received template now as priveleged machine account instead of our fake machine account.

Impact and Consequences

Consequences range from unauthorized data access to complete network compromise.

The impact of CVE-2022-26923 allows low privilege users to gain Domain Controller privileges in a single hop.

Attackers gain control over critical systems, wreaking havoc with minimal effort.
The potential ramifications include financial loss, reputational damage, and legal implications.

Cybersecurity Research Importance

Certified Pre-Owned!

Acknowledgement

Will Schroeder

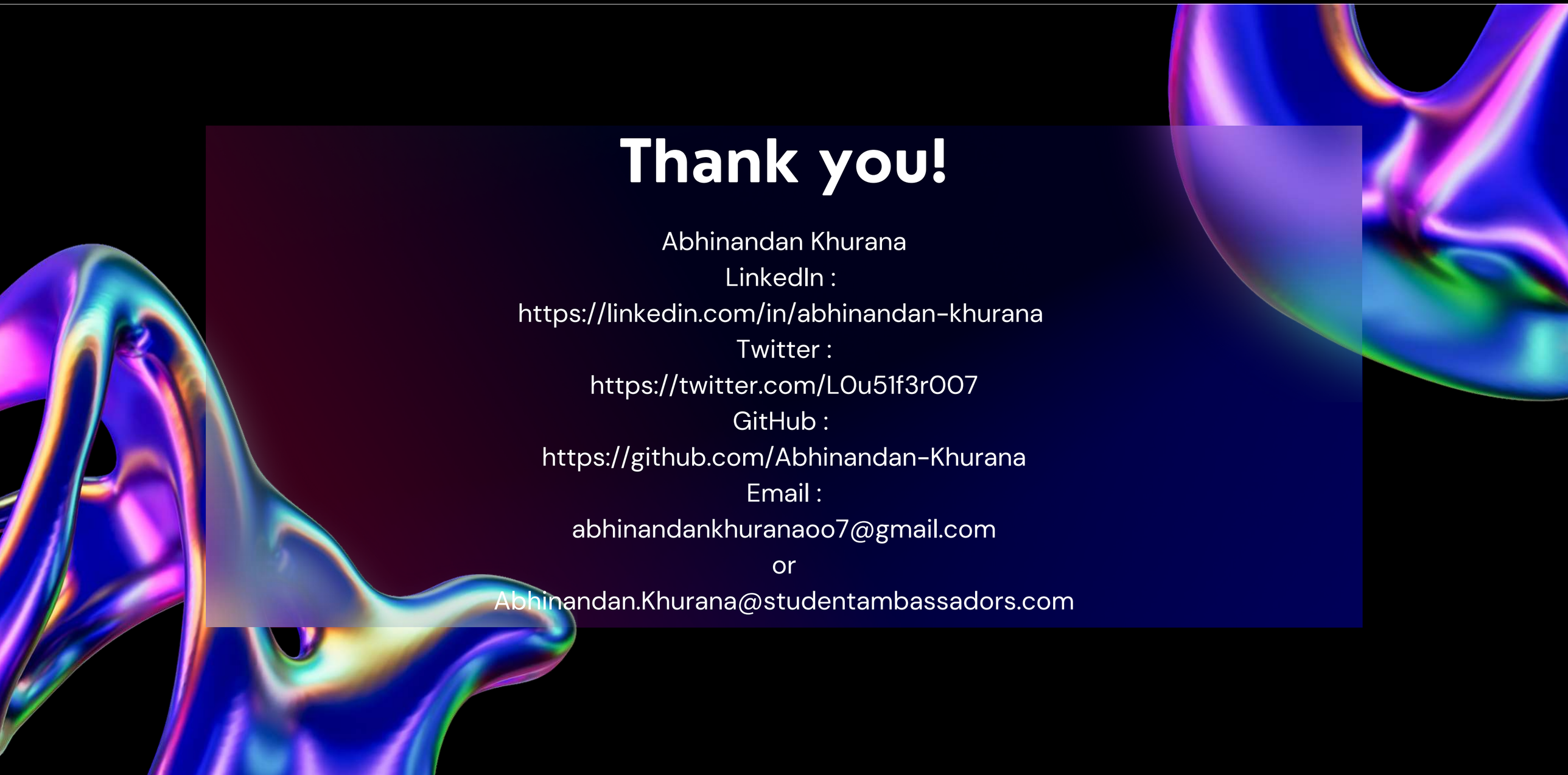
@harmj0y

Lee Christensen

@tifkin_

QnA!

How?	When?
Why?	Whatever XD
Workshop Materials	Hehehe :)



Thank you!

Abhinandan Khurana
LinkedIn :
https://linkedin.com/in/abhinandan-khurana
Twitter :
https://twitter.com/L0u51f3r007
GitHub :
https://github.com/Abhinandan-Khurana
Email :
abhinandankhuranaoo7@gmail.com
or
Abhinandan.Khurana@studentambassadors.com

Resources

Certipy github - https://github.com/ly4k/Certipy
Impacket github - https://github.com/SecureAuthCorp/impacket
Whitepaper - https://posts.specterops.io/certified-pre-owned-d95910965cd2
Read the research - https://research.ifcr.dk/certifried-active-directory-domain-privilege-escalation-cve-2022-26923-9e098fe298f4
addcomputers.py - https://github.com/SecureAuthCorp/impacket/blob/master/examples/addcomputer.py

Rest Stay tuned, may update AD lab setup and helpful notes over my github in future.
(https://github.com/Abhinandan-Khurana/)
Video Practical link - https://vimeo.com/846019015?share=copy