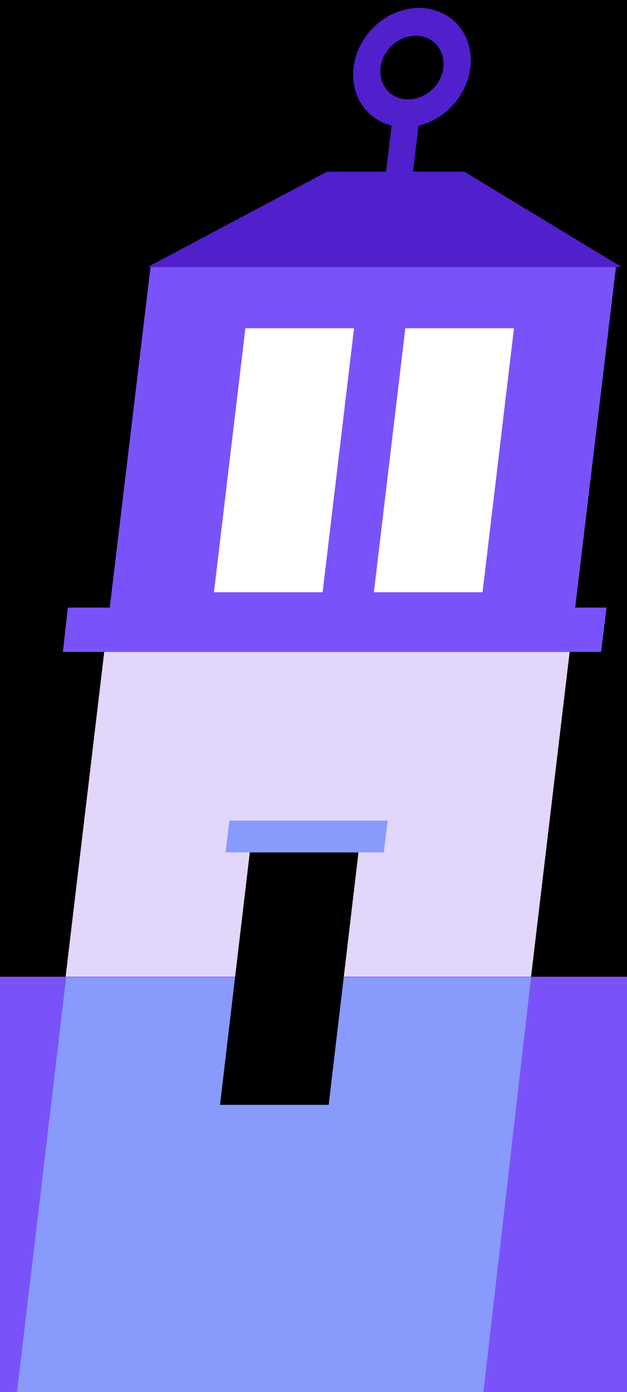
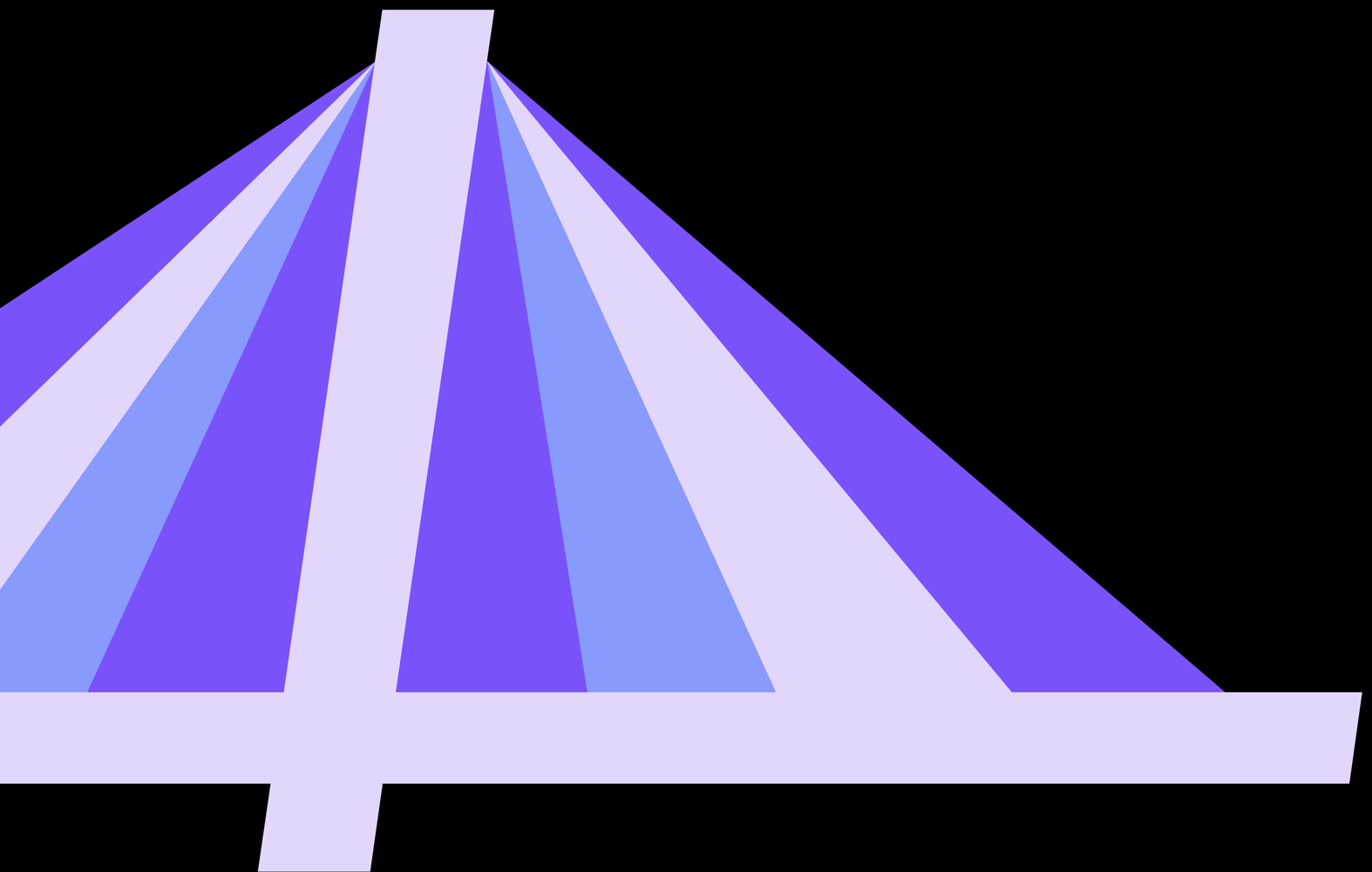
HYBRID
IDENTITY
PROTECTION

conf25

CHARLESTON





End the ESCape Clause!

Jake Hildreth
Principal Security Consultant
Semperis

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Jake Hildreth

Principal Security Consultant
Semperis

Husband, Dad, Recovering Sysadmin

25 years in Information Technology

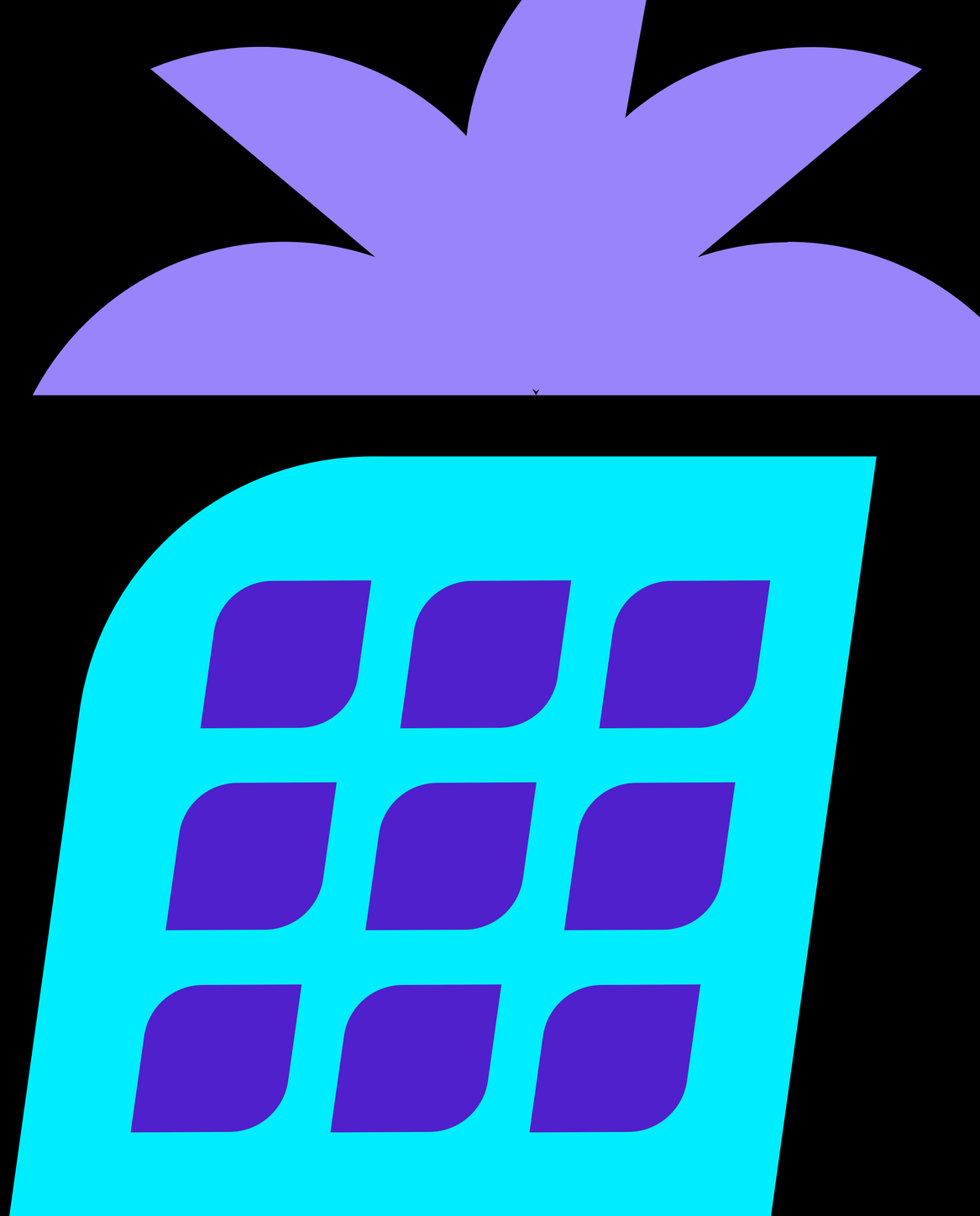
Member of the Semperis BP & R Team

Microsoft MVP for Identity + PowerShell

Builder of Tools and Toys

Agenda

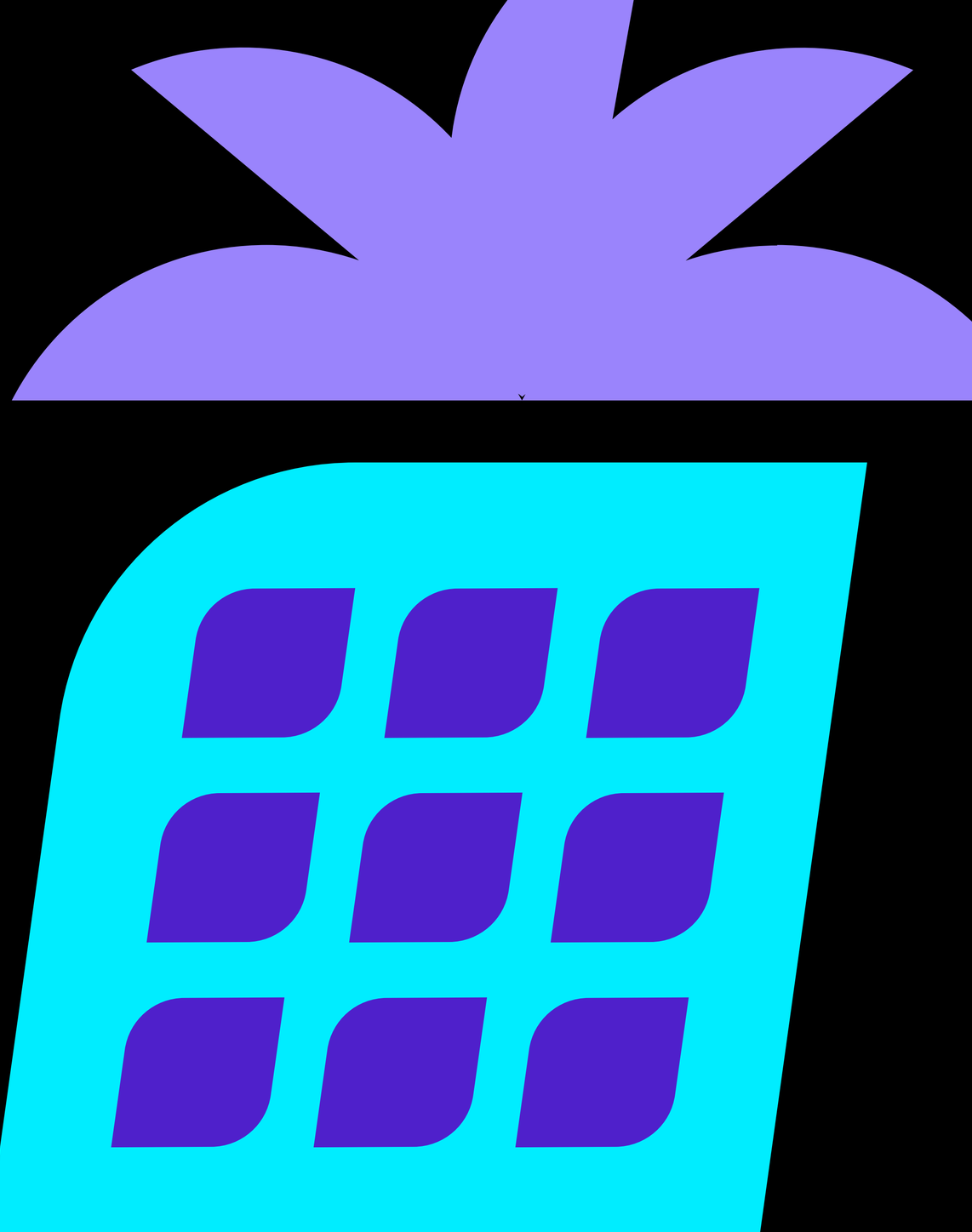
- Active Directory Certificate Services Security Overview



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

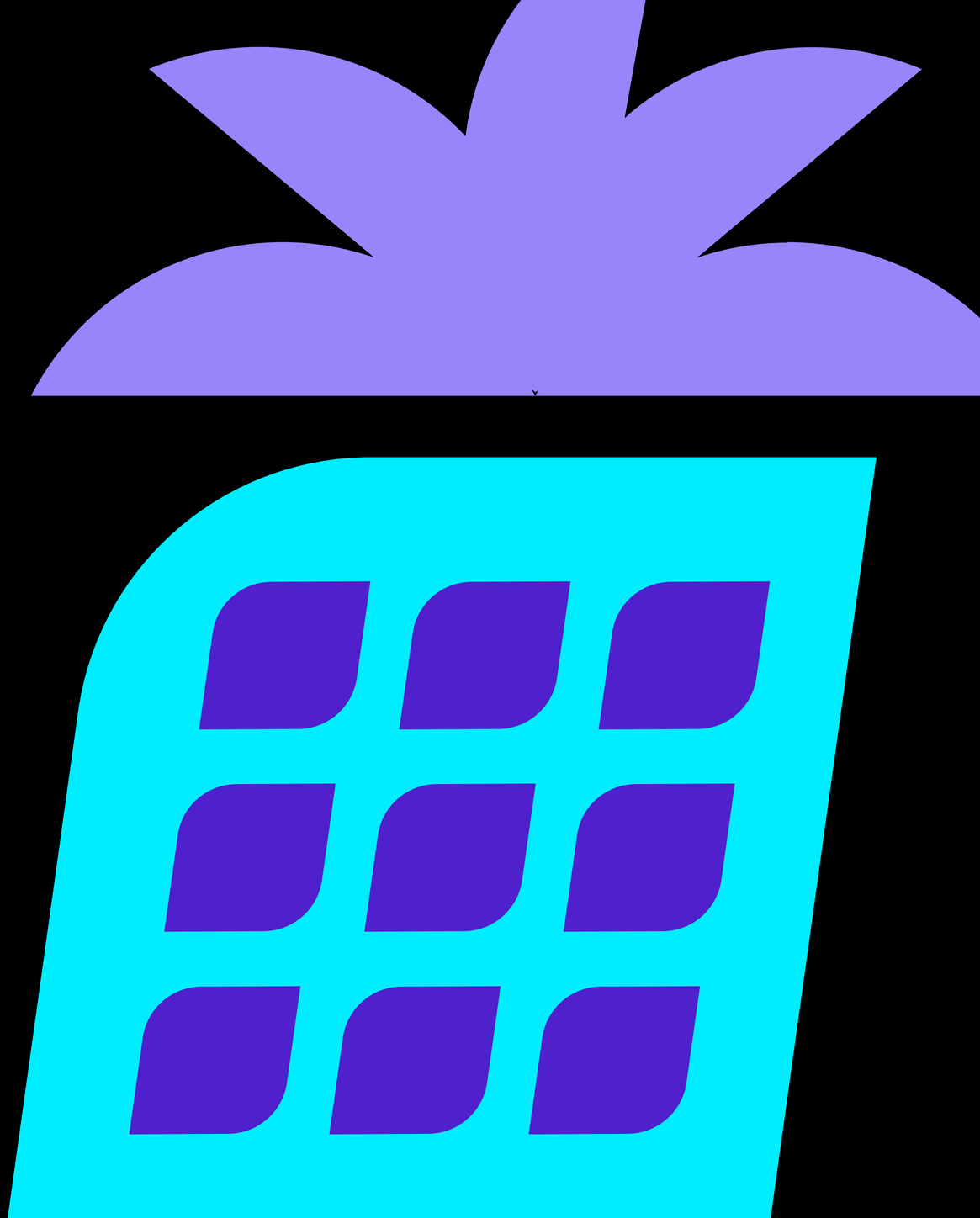
Agenda

- Active Directory Certificate Services Security Overview
- Most Common Privilege Escalation Attacks



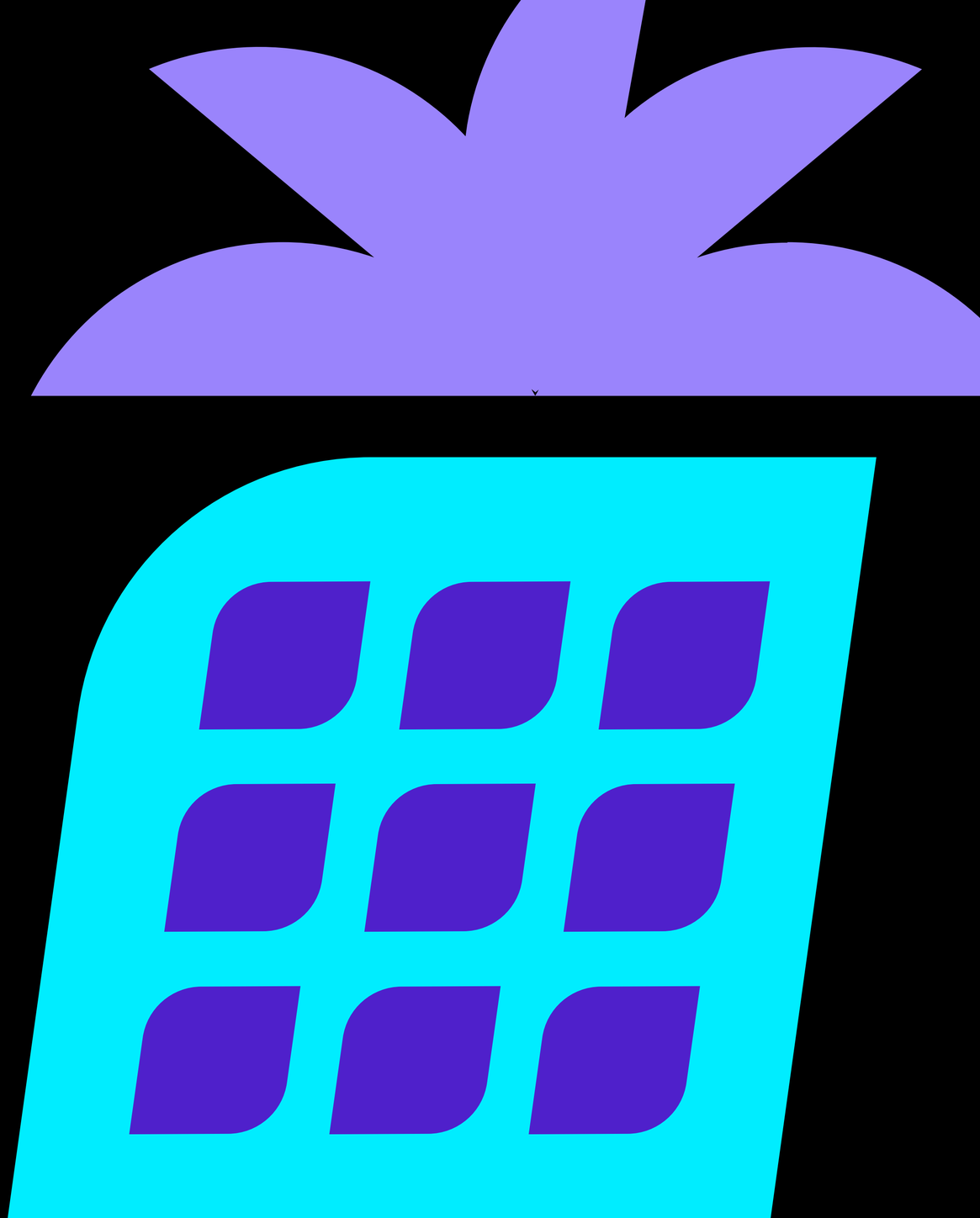
Agenda

- Active Directory Certificate Services Security Overview
- Most Common Privilege Escalation Attacks
- Example Combination Attacks & Attack Paths



Agenda

- Active Directory Certificate Services Security Overview
- Most Common Privilege Escalation Attacks
- Example Combination Attacks & Attack Paths
- Limitations of Current Tools



Agenda

- Active Directory Certificate Services Security Overview
- Most Common Privilege Escalation Attacks
- Example Combination Attacks & Attack Paths
- Limitations of Current Tools
- Introducing ESCalator

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

A Quick Overview of Active Directory Certificate Services Security

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

aka “AD CS”

HYBRID IDENTITY PROTECTION conf25

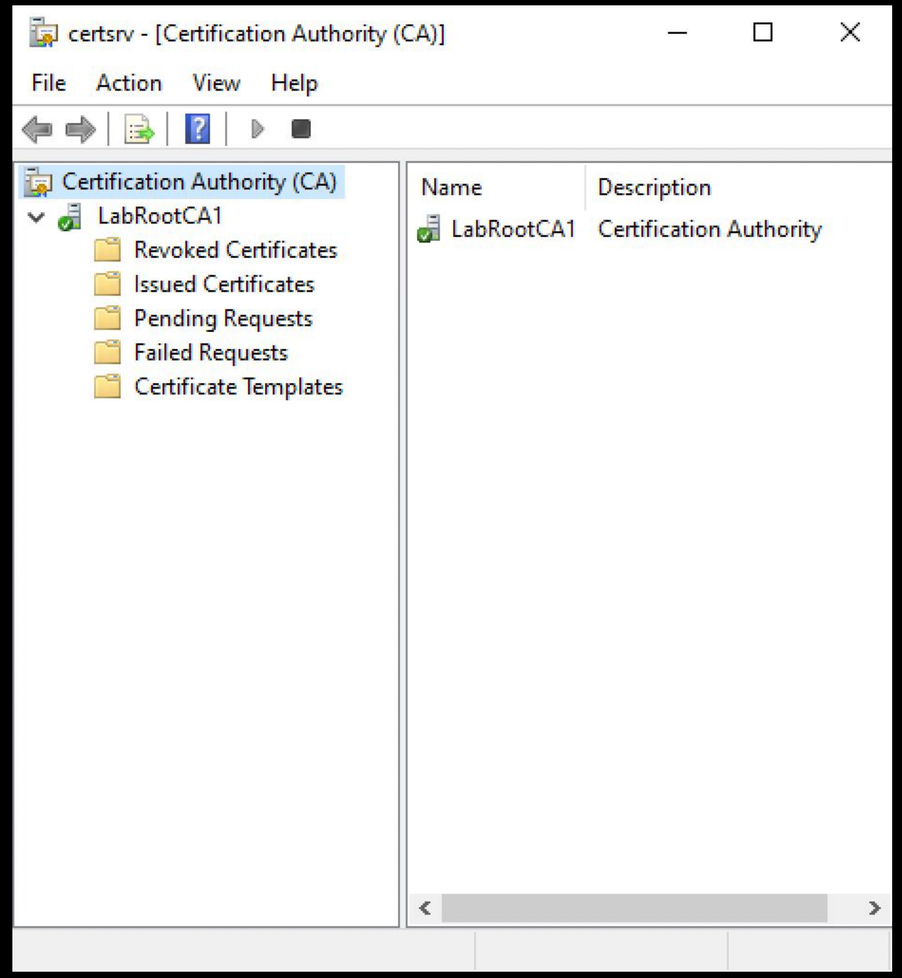
CHARLESTON

aka “a baroque disaster”

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

AD CS Overview

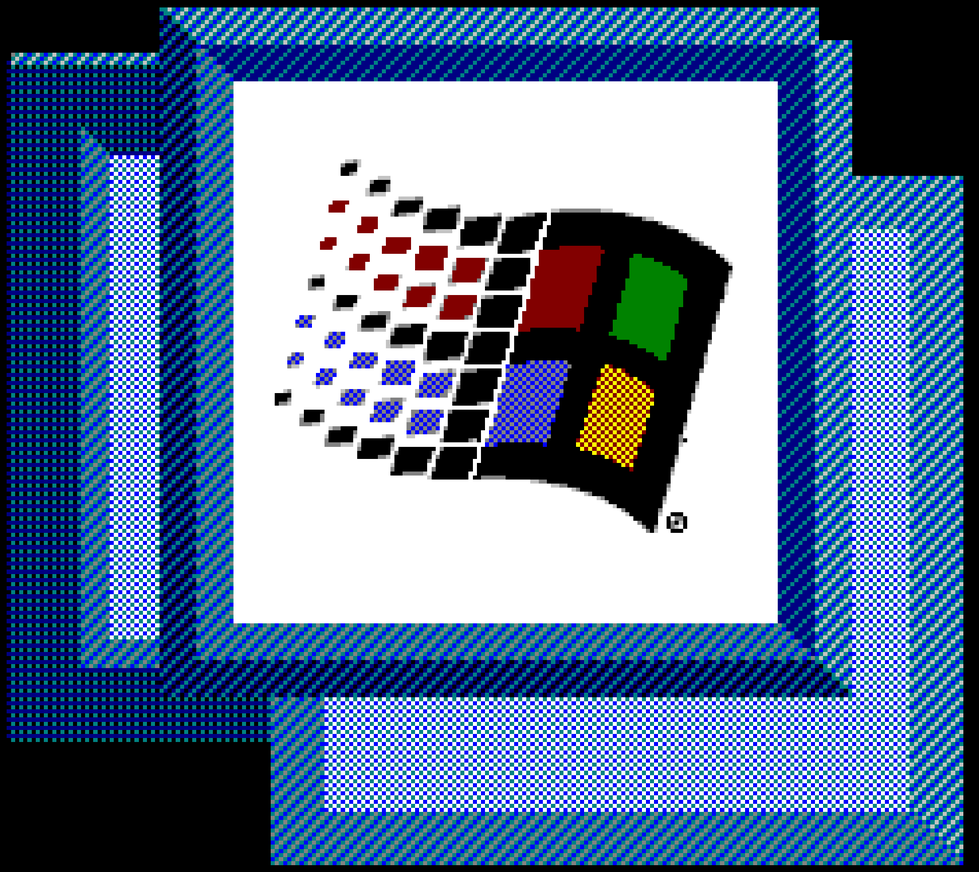
- A *very* Microsoft implementation of Public Key Infrastructure (PKI)



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

AD CS Overview

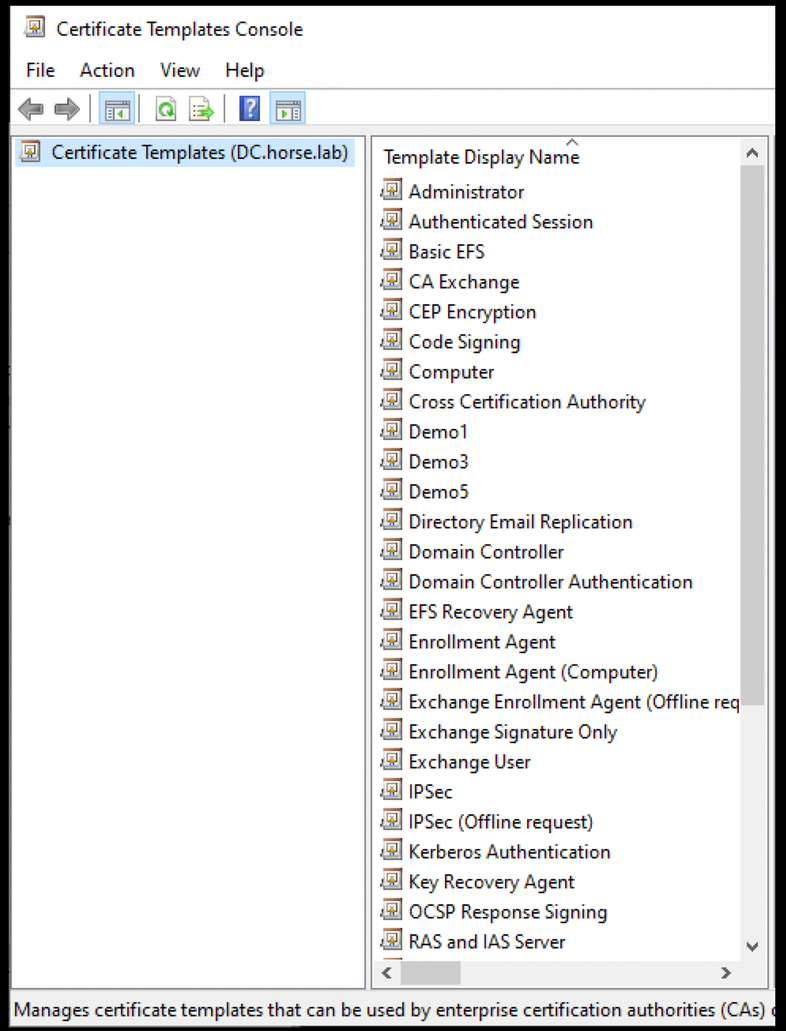
- A *very* Microsoft implementation of Public Key Infrastructure (PKI)
- Available since Server 2000



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

AD CS Overview

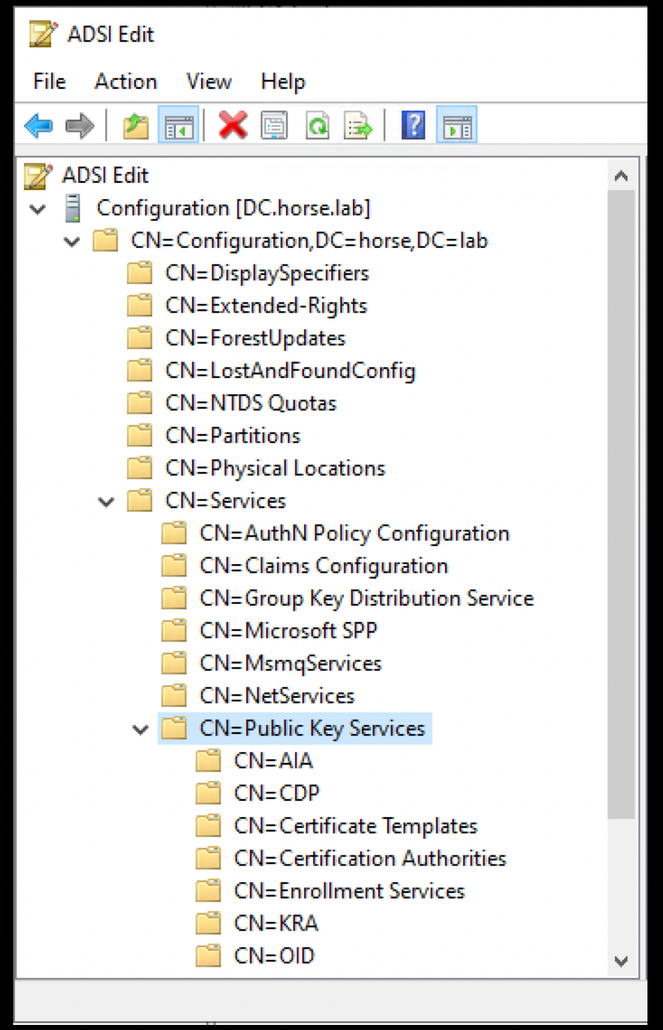
- A *very* Microsoft implementation of Public Key Infrastructure (PKI)
- Available since Server 2000
- Simplifies & standardizes common PKI tasks



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

AD CS Overview

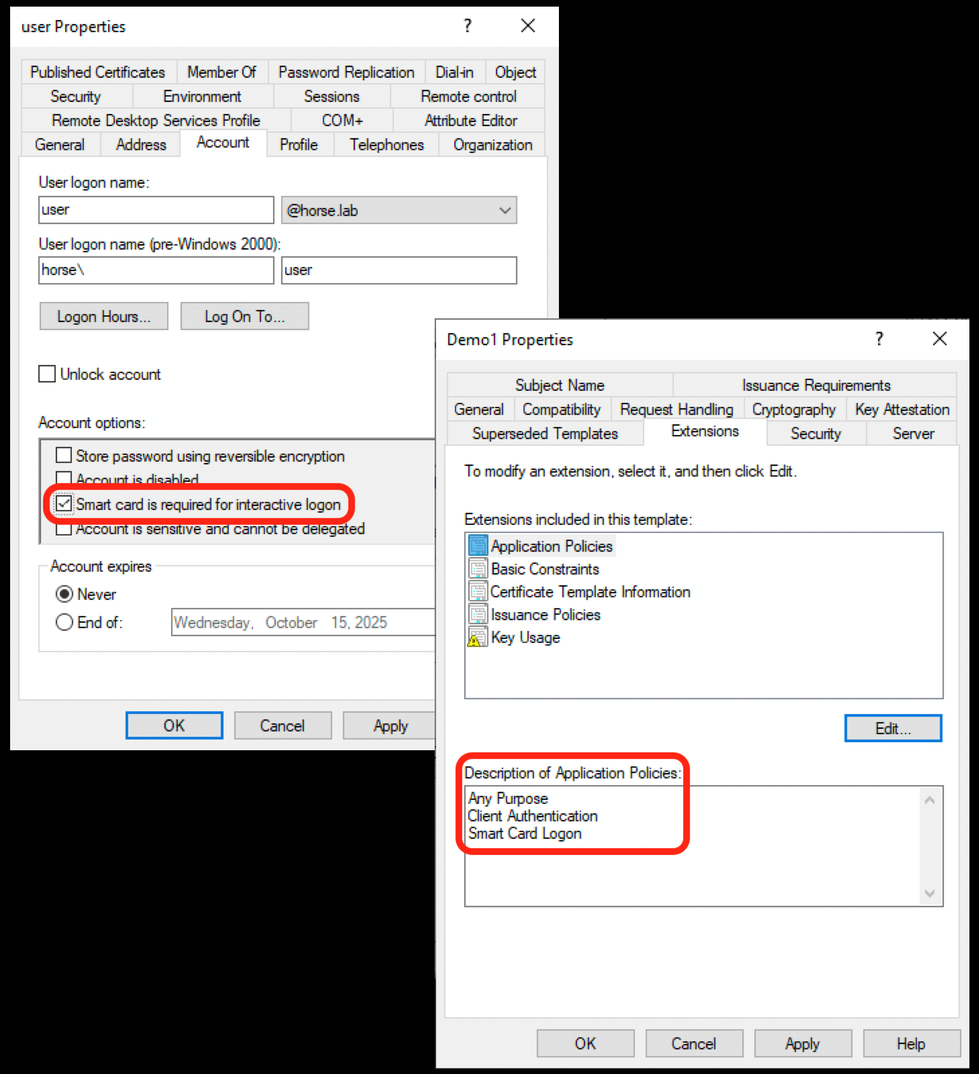
- A *very* Microsoft implementation of Public Key Infrastructure (PKI)
- Available since Server 2000
- Simplifies & standardizes common PKI tasks
- Tightly integrated with Active Directory



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

AD CS Overview

- A *very* Microsoft implementation of Public Key Infrastructure (PKI)
- Available since Server 2000
- Simplifies & standardizes common PKI tasks
- Tightly integrated with Active Directory
- Enables Certificate-Based Authentication



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

AD CS Overview

- A *very* Microsoft implementation of Public Key Infrastructure (PKI)
- Available since Server 2000
- Simplifies & standardizes common PKI tasks
- Tightly integrated with Active Directory
- Enables Certificate-Based Authentication
- *Just enough* configuration available to ensure you step on *at least* one rake

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

AD CS Security Pre-History

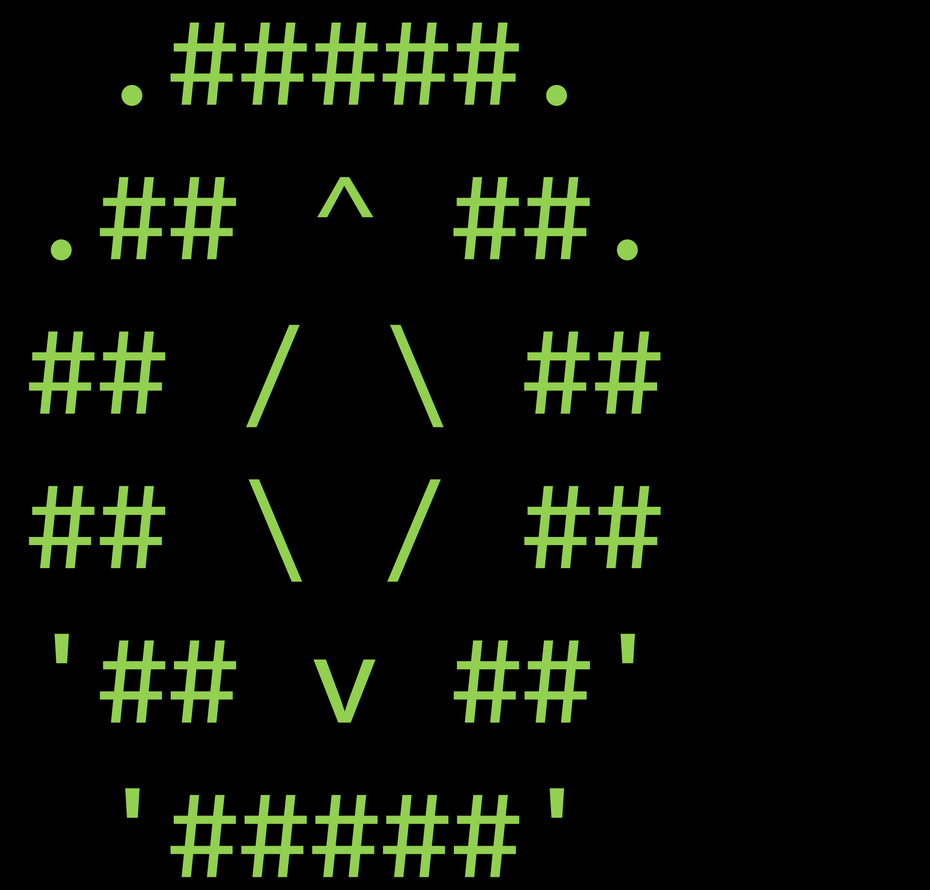
- **Early 2016:** KeyFactor

Hidden Dangers: Certificate Subject Alternative Names (SANs)

January 7, 2016

AD CS Security Pre-History

- **Early 2016:** KeyFactor
- **Fall 2016:** Benjamin Delpy



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

AD CS Security Pre-History

- **Early 2016:** KeyFactor
- **Fall 2016:** Benjamin Delpy
- **Summer 2019:** Elkement

Sizzle @ hackthebox – Unintended: Getting a Logon Smartcard for the Domain Admin!

Written by elkement in Control and IT, Cyber, punktwissen, Science and Technology on June 1, 2019

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

AD CS Security Pre-History

- **Early 2016:** KeyFactor
- **Fall 2016:** Benjamin Delpy
- **Summer 2019:** Elkement
- **Summer 2020:** Elkement again!

Impersonating a Windows Enterprise Admin with a Certificate: Kerberos PKINIT from Linux

Written by elkement in Control and IT, Cyber, punktwissen, Science and Technology on June 21, 2020

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

AD CS Security Pre-History

- **Early 2016:** KeyFactor
- **Fall 2016:** Benjamin Delpy
- **Summer 2019:** Elkement
- **Summer 2020:** Elkement
- **Fall 2019:** Christoph Falta

README BSD-3-Clause license

PoshADCS

PoshADCS is the result of my current research in finding attack paths against an Active Dircetory Domain through ADCS (Active Directory Certificate Services). The script is still in a very beta-stage at the moment so use it only if you know what you are doing.

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

AD CS Security Pre-History

- **Early 2016:** KeyFactor
- **Fall 2016:** Benjamin Delpy
- **Summer 2019:** Elkement
- **Summer 2020:** Elkement
- **Fall 2019:** Christoph Falta
- **Fall 2020:** Maciej Kosz & Mike Jankowski-Lorek

One of the commonly recommended solutions to increase the security of user accounts in the on-premise Active Directory is to require **two-factor authentication using Smart Cards**. Not everyone knows that Windows Smart Card implementation has undergone a significant change years ago that has not been clearly reflected in the publicly available documentation. Since **Public Key Infrastructure (PKI) security is not a typical piece of knowledge**, therefore many enterprises may be at risk.

September 15, 2020 Written by: CQURE Experts 10 min read

The tale of Enhanced Key (mis)Usage

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

AD CS Security Pre-History

- **Early 2016:** KeyFactor
- **Fall 2016:** Benjamin Delpy
- **Summer 2019:** Elkement
- **Summer 2020:** Elkement
- **Fall 2019:** Christoph Falta
- **Fall 2020:** Maciej Kosz & Mike Jankowski-Lorek
- **Fall 2020:** Carl Sörqvist

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

AD CS Security Pre-History

- **Early 2016:** KeyFactor
- **Fall 2016:** Benjamin Delpy
- **Summer 2019:** Elkement
- **Summer 2020:** Elkement
- **Fall 2019:** Christoph Falta
- **Fall 2020:** Maciej Kosz & Mike Jankowski-Lorek
- **Fall 2020:** Carl Sörqvist
- **Fall 2020:** Ceri Coburn

Attacking Smart Card Based Active Directory Networks

Posted on 4th October 2020 by CCob

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

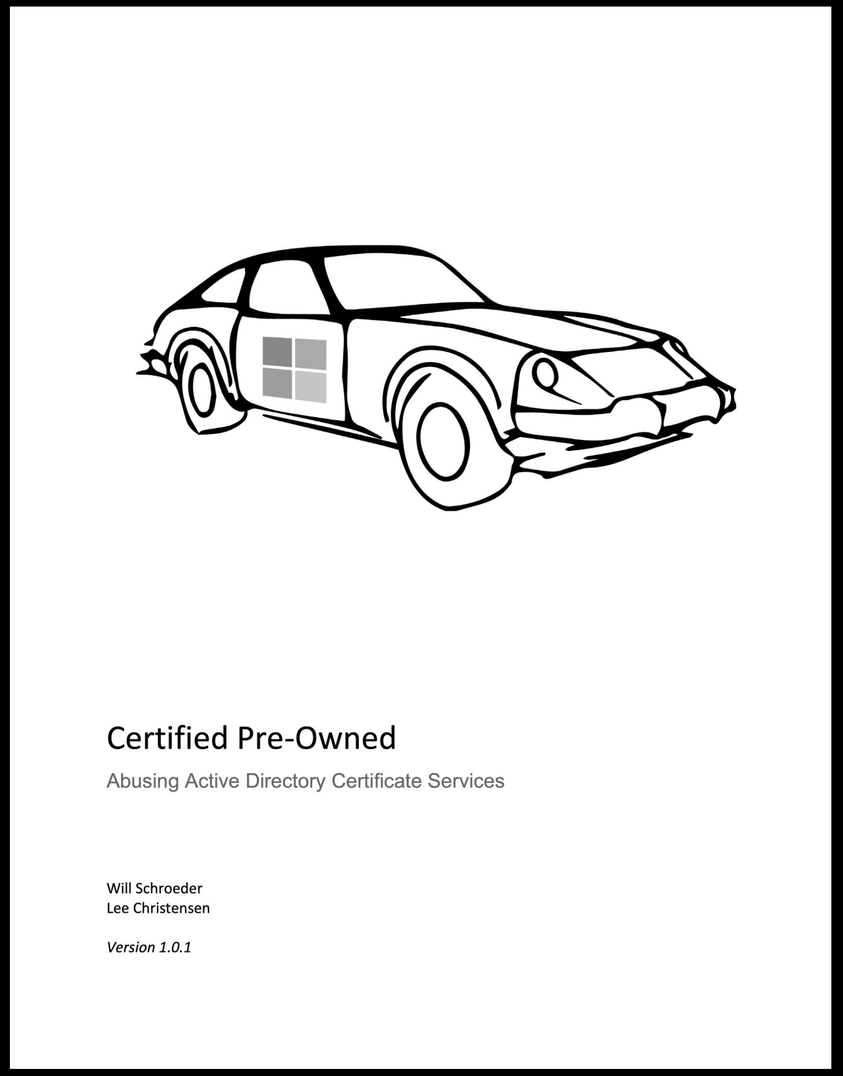
A Watershed Moment

Summer 2021:

Will Schroeder &

Lee Chagolla-Christensen

Released “Certified Pre-Owned”



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

A Watershed Moment

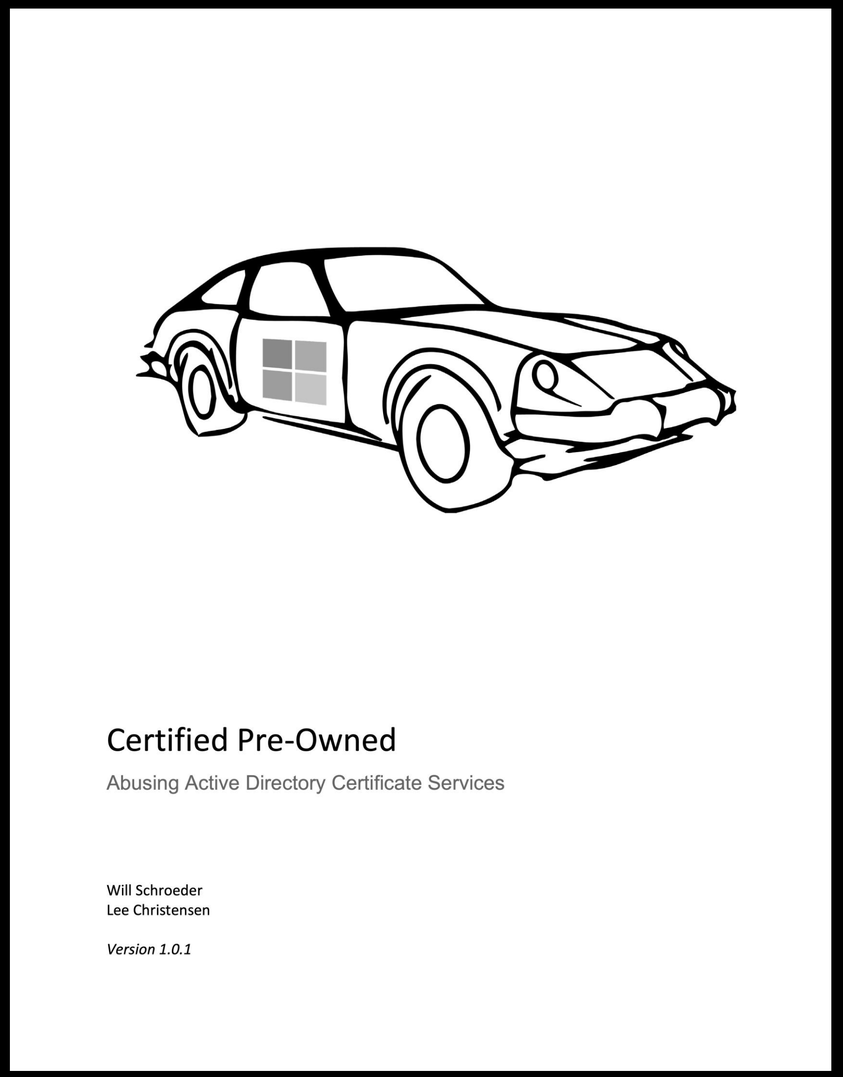
Summer 2021:

Will Schroeder &

Lee Chagolla-Christensen

Released “Certified Pre-Owned”

140 pages of gold:



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

A Watershed Moment

Summer 2021:

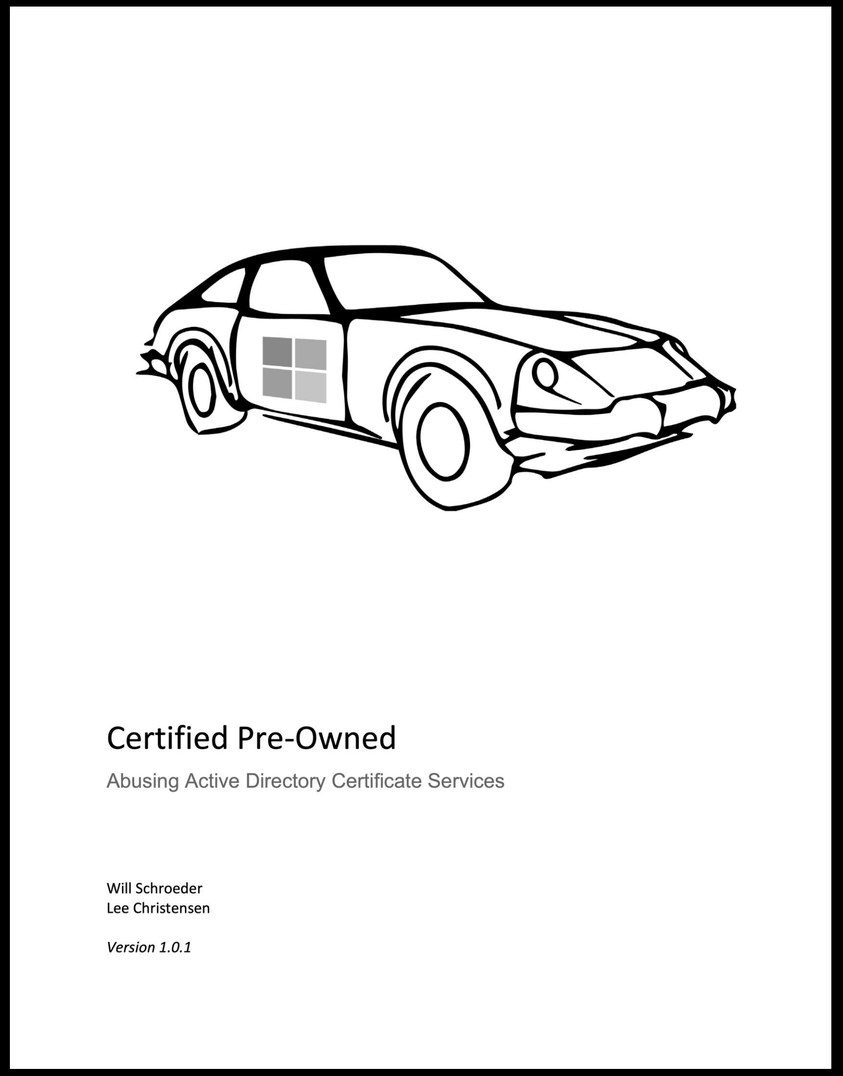
Will Schroeder &

Lee Chagolla-Christensen

Released “Certified Pre-Owned”

140 pages of gold:

Certificate Theft



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

A Watershed Moment

Summer 2021:

Will Schroeder &

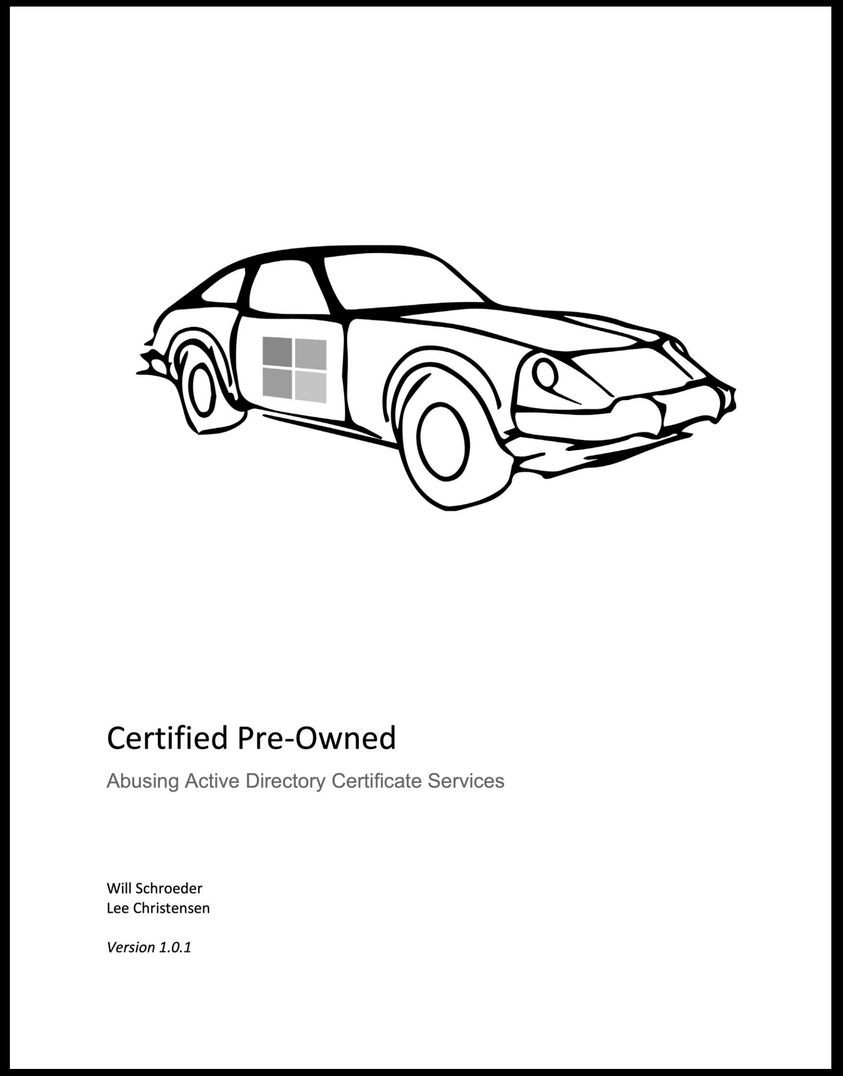
Lee Chagolla-Christensen

Released “Certified Pre-Owned”

140 pages of gold:

Certificate Theft

Persistence



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

A Watershed Moment

Summer 2021:

Will Schroeder &

Lee Chagolla-Christensen

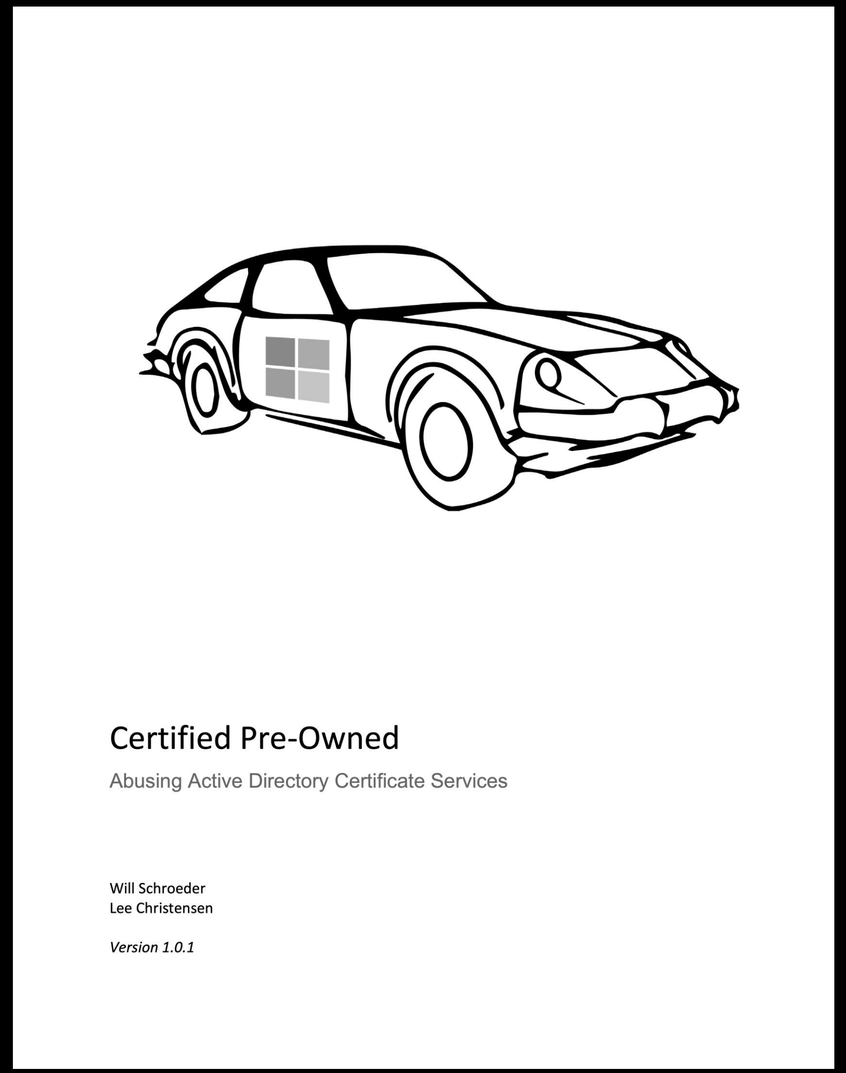
Released “Certified Pre-Owned”

140 pages of gold:

Certificate Theft

Persistence

Privilege Escalation



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

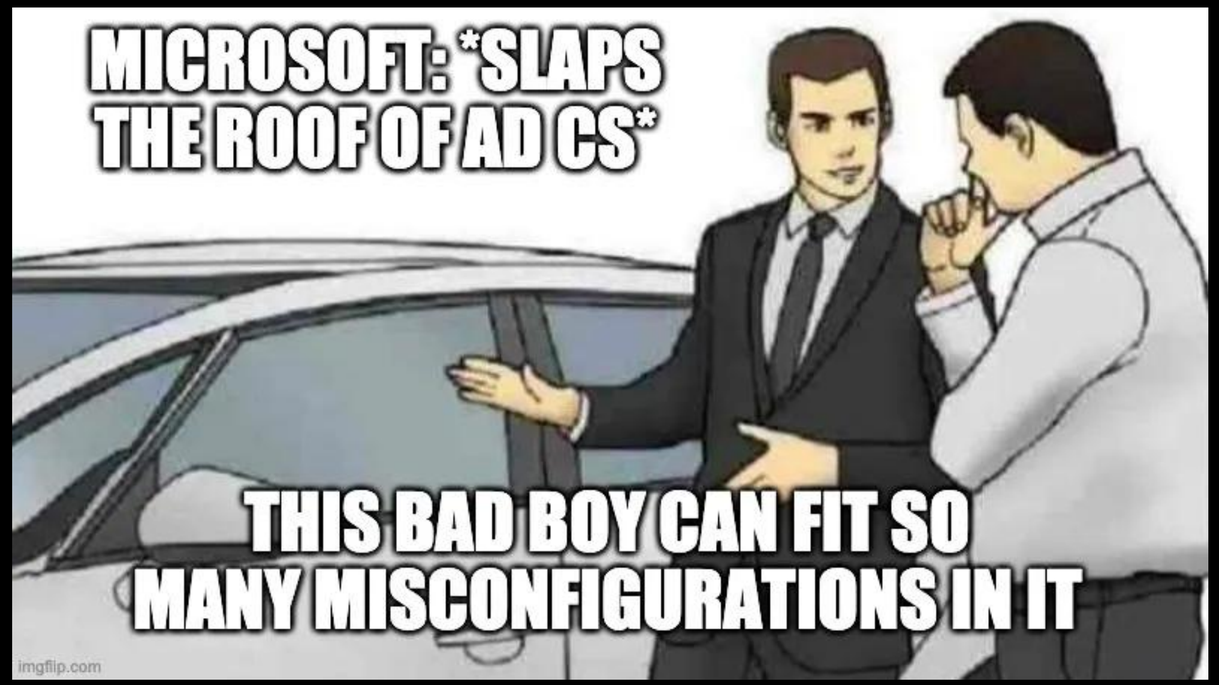
A Watershed Moment

And this absolute banger…

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

A Watershed Moment

And this absolute banger…



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

A Watershed Moment…

Active Directory Certificate Services-based Privilege Escalation Attacks Targeting Templates, Certification Authorities, and other PKI-related objects

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

A Watershed Moment…

Active Directory Certificate Services-based Privilege Escalation Attacks Targeting Templates, Certification Authorities, and other PKI-related objects

…a mouthful.

…In Marketing?

How about…

…In Marketing?

How about…

ESC?

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Hindsight is Always 20/20

- **Early 2016:** KeyFactor
- **Fall 2016:** Benjamin Delpy
- **Summer 2019:** Elkement
- **Summer 2020:** Elkement
- **Fall 2019:** Christoph Falta
- **Fall 2020:** Maciej Kosz & Mike Jankowski-Lorek
- **Fall 2020:** Carl Sörqvist
- **Fall 2020:** Ceri Coburn

Hindsight is Always 20/20

- **Early 2016:** KeyFactor – **ESC6**

- **Summer 2019:** Elkement – **ESC4**
- **Summer 2020:** Elkement – **ESC1**
- **Fall 2019:** Christoph Falta – **ESC1 & ESC4**
- **Fall 2020:** Maciej Kosz & Mike Jankowski-Lorek – **ESC1 & ESC6**
- **Fall 2020:** Carl Sörqvist – **ESC1**

Modern AD CS Security

- Certifried + Eight new ESCs

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Modern AD CS Security

- Certifried + Eight new ESCs

- Oliver Lyak, Institut for Cyber Risk
- Sylvain Heineger, Compass Security
- Hans-Joachim Knobloch, m2trust
- Jonas Bülow Knudsen, SpecterOps
- Justin Bollinger, TrustedSec

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Modern AD CS Security

- Certifried + Eight new ESCs

• Oliver Lyak, Institut for Cyber Risk	Certifried, ESC9, 10, 16
• Sylvain Heineger, Compass Security	ESC11
• Hans-Joachim Knobloch, m2trust	ESC12
• Jonas Bülow Knudsen, SpecterOps	ESC13, 14
• Justin Bollinger, TrustedSec	ESC15

Modern AD CS Security

- Certifried + Eight new ESCs
- Red Team/Pentesters LOVE ESCs

Modern AD CS Security

- Certifried + Eight new ESCs
- Red Team/Pentesters LOVE ESCs

- APT29 used ESC1 in early 2022

Modern AD CS Security

- Certifried + Eight new ESCs
- Red Team/Pentesters LOVE ESCs
- APT29 used ESC1 in early 2022
- Strong Enforcement mode & other fixes

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Modern AD CS Security

- Certifried + Eight new ESCs
- Red Team/Pentesters LOVE ESCs
- APT29 used ESC1 in early 2022
- Strong Enforcement mode & other fixes

- Popular Free AD Security Tools that analyze AD CS vulnerabilities:
  - Purple Knight
  - Forest Druid
  - BloodHound
  - PingCastle

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Modern AD CS Security

- Certifried + Eight new ESCs
- Red Team/Pentesters LOVE ESCs

- Popular Free AD Security Tools that analyze AD CS vulnerabilities:
  - Purple Knight
  - Forest Druid
  - BloodHound
  - PingCastle

- APT29 used ESC1 in early 2022
- Strong Enforcement mode & other fixes

- Popular Free AD CS-specific Tools that dig a bit deeper:
  - Certify
  - Certipy
  - PSPKIAudit
  - Locksmith

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Modern AD CS Security

- Popular Free AD CS-specific Tools that dig a bit deeper:
  - Certify
  - Certipy
  - PSPKIAudit
  - Locksmith (shameless, I know)

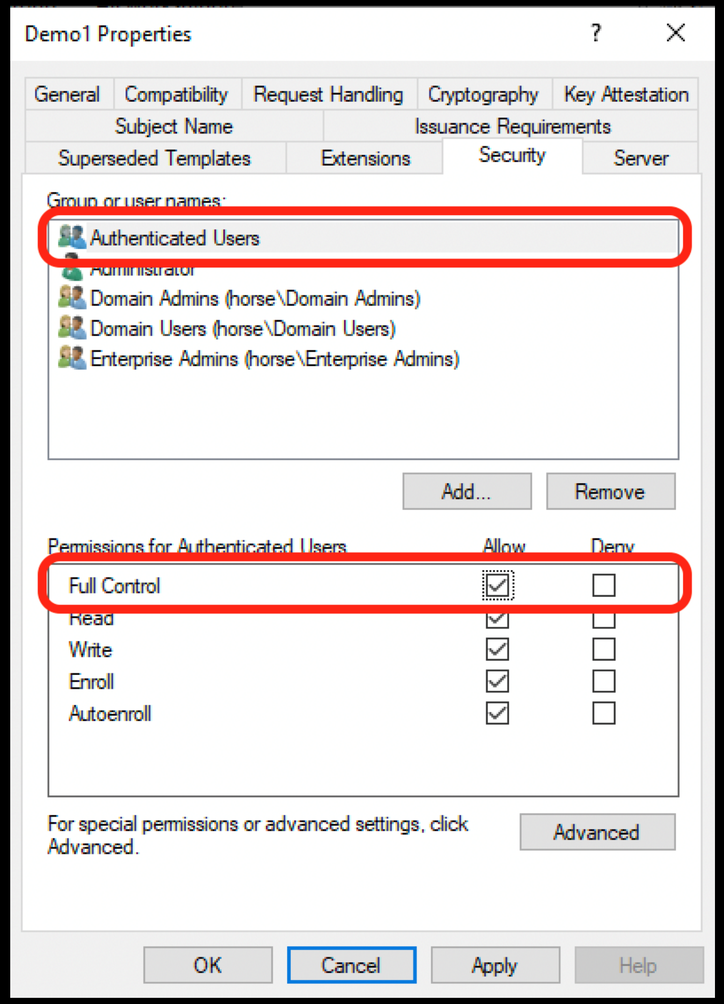
HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Common ESCs

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

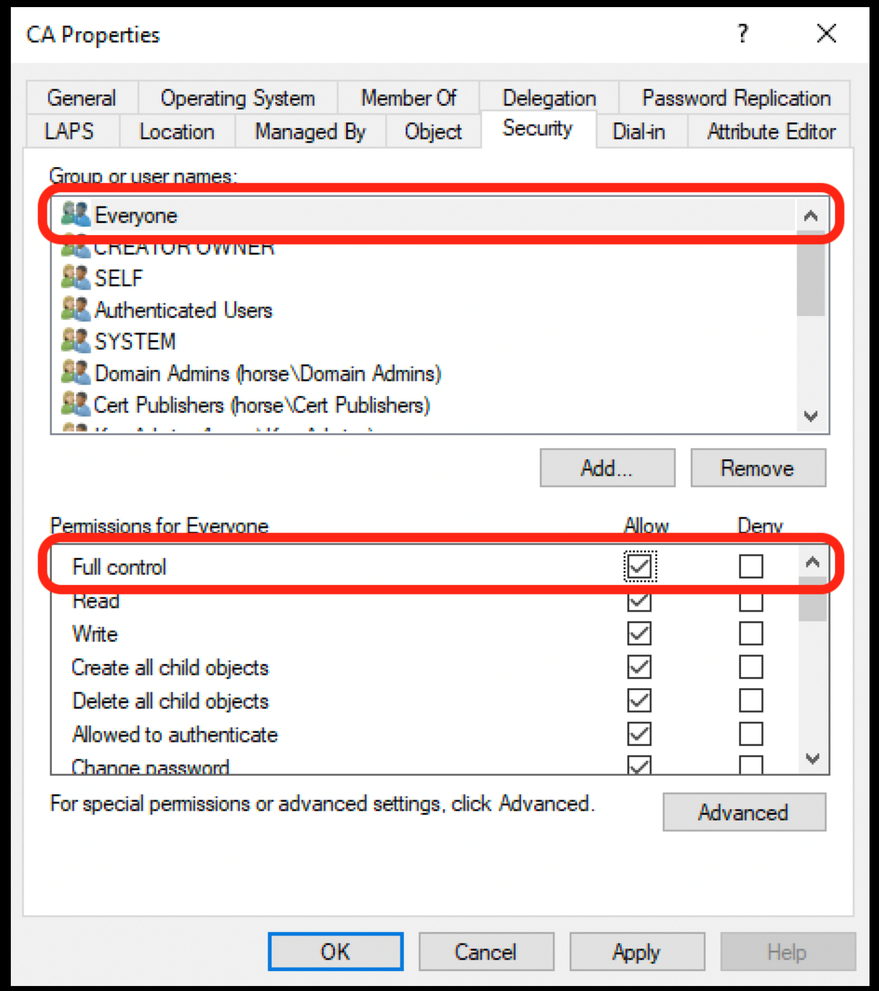
Domain Escalation 4 aka ESC4



- Description: Vulnerable access controls
- Impacted Objects: Certificate templates
- Risk: Info-Critical
- Remediation: Principle of Least Privilege

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

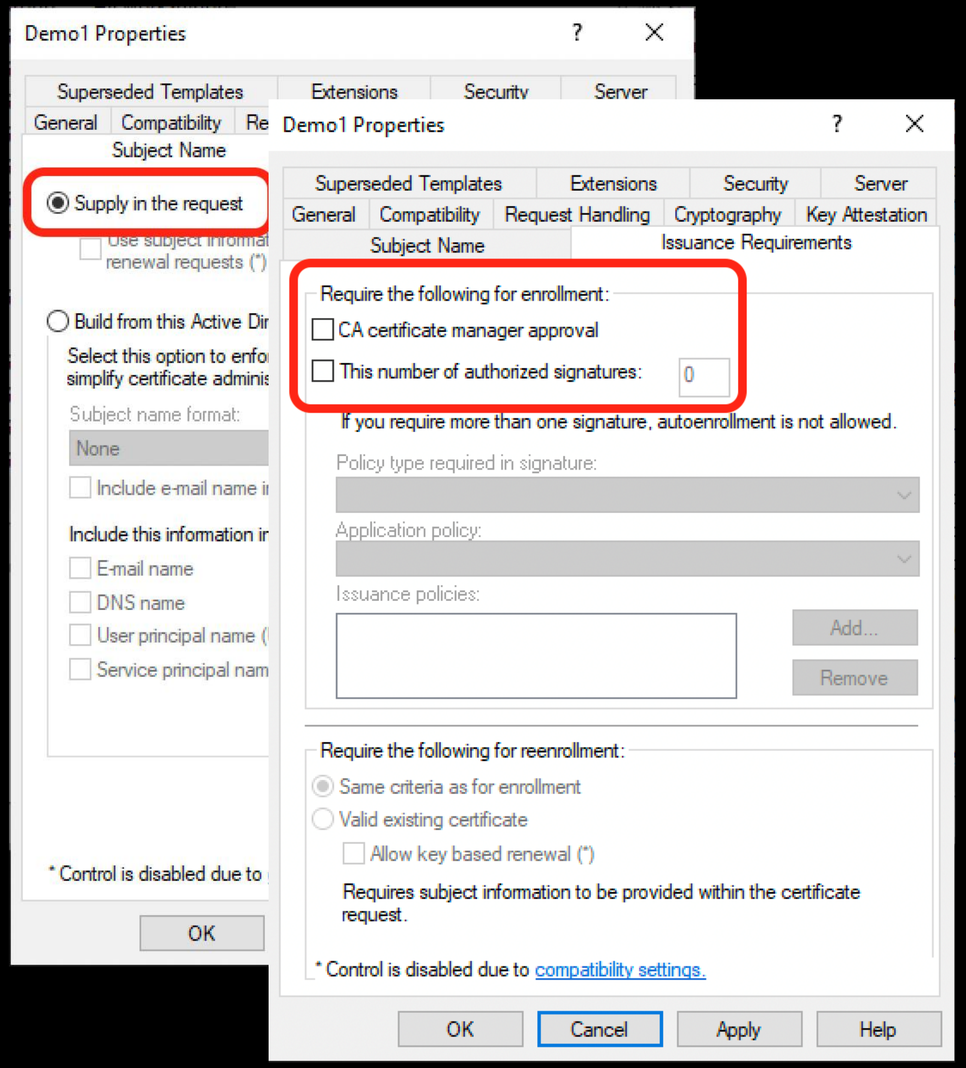
Domain Escalation 5 aka ESC5



- Description: Vulnerable access controls
- Impacted Objects: Any other PKI object
- Risk: Info-Critical
- Remediation: Principle of Least Privilege

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

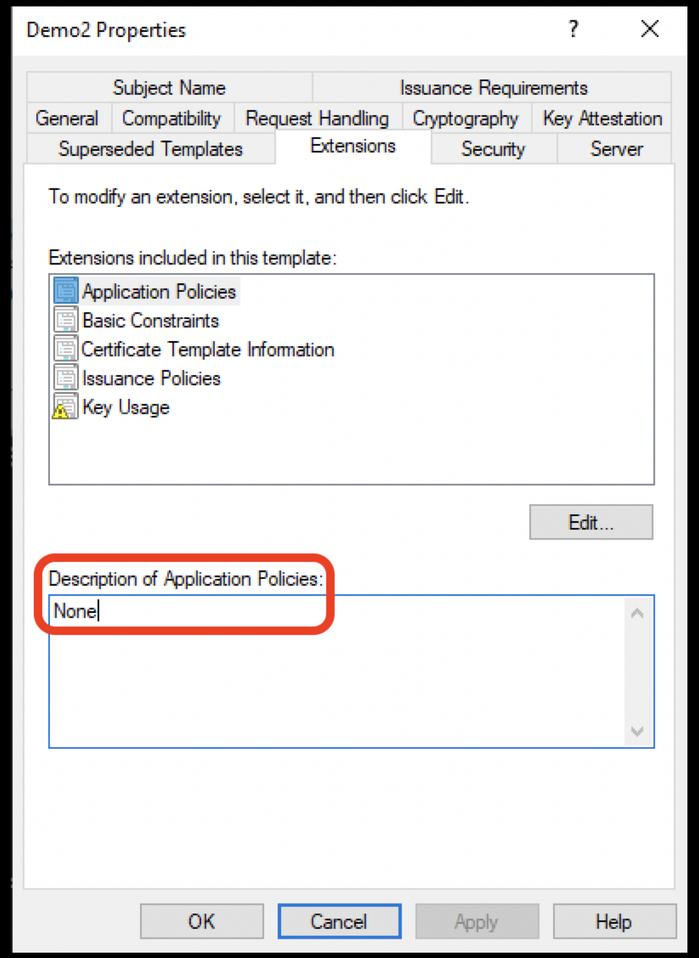
Domain Escalation 1 aka ESC1



- Description:
  - Template usable for Client Authentication
  - Subject Alternative Name (SAN) allowed
  - ”Manager Approval” not required
  - Enabled for enrollment
  - Low-privileged principals can enroll
- Risk: Low-Critical
- Remediation: Very situation-specific

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Other Common Vulnerabilities



- ESC2 – SubCA/Any Purpose
  - Common in virtualized environments

Other Common Vulnerabilities

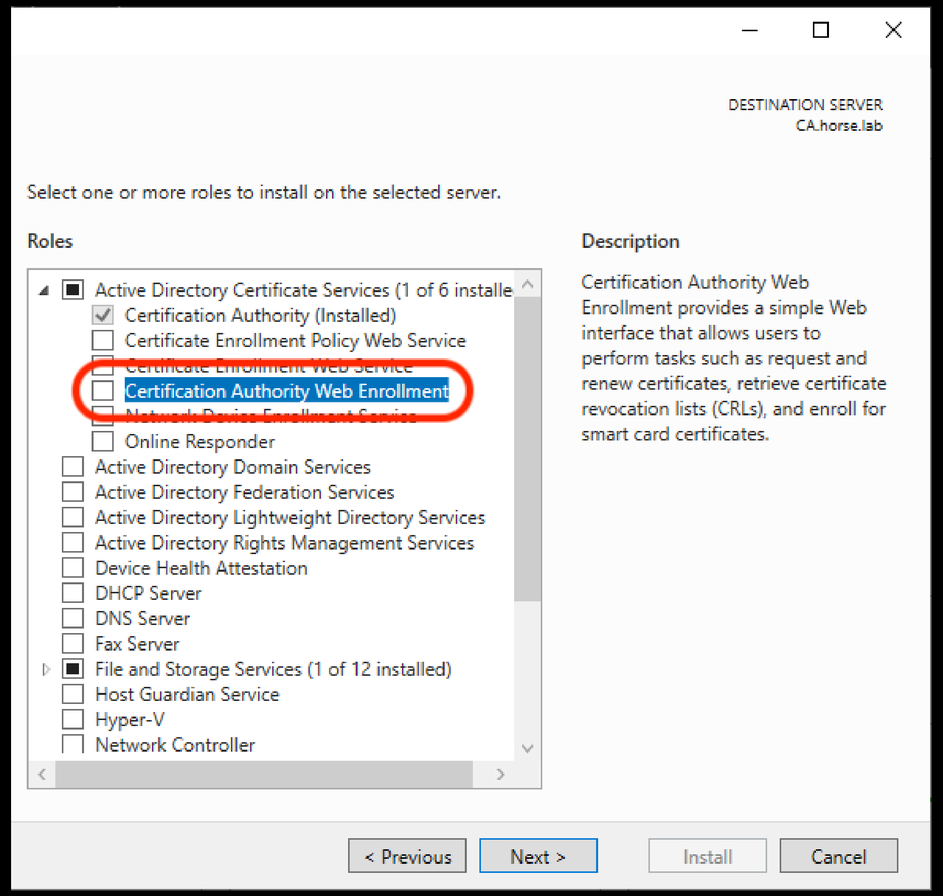
```
PS C:\> certutil -getreg Policy\EditFlags
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\
CertSvc\Configuration\LabRootCA1\PolicyModules\
CertificateAuthority_MicrosoftDefault.Policy\
EditFlags:

  EditFlags REG_DWORD = 150146 (1376582)
    EDITF_REQUESTEXTENSIONLIST -- 2
    EDITF_DISABLEEXTENSIONLIST -- 4
    EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
    EDITF_ENABLEAKIKEYID -- 100 (256)
    EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
    EDITF_ATTRIBUTESUBJECTALTNAME2 -- 40000 (262144)
    EDITF_ENABLECHASECLIENTDC -- 100000 (1048576)
CertUtil: -getreg command completed successfully.
```

- ESC2 – SubCA/Any Purpose
  - Common in virtualized environments
- ESC6 – SAN on Everything!
  - Common in MDM environments
  - *Mostly* neutered by Strong Mapping

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Other Common Vulnerabilities



- ESC2 – SubCA/Any Purpose
  - Common in virtualized environments
- ESC6 – SAN on Everything!
  - Common in MDM environments
  - *Mostly* neutered by Strong Mapping
- ESC8 – Relay to HTTP/S Enrollment Endpoints
  - *Extremely* common in older AD CS deployments

HYBRID IDENTITY PROTECTION conf25

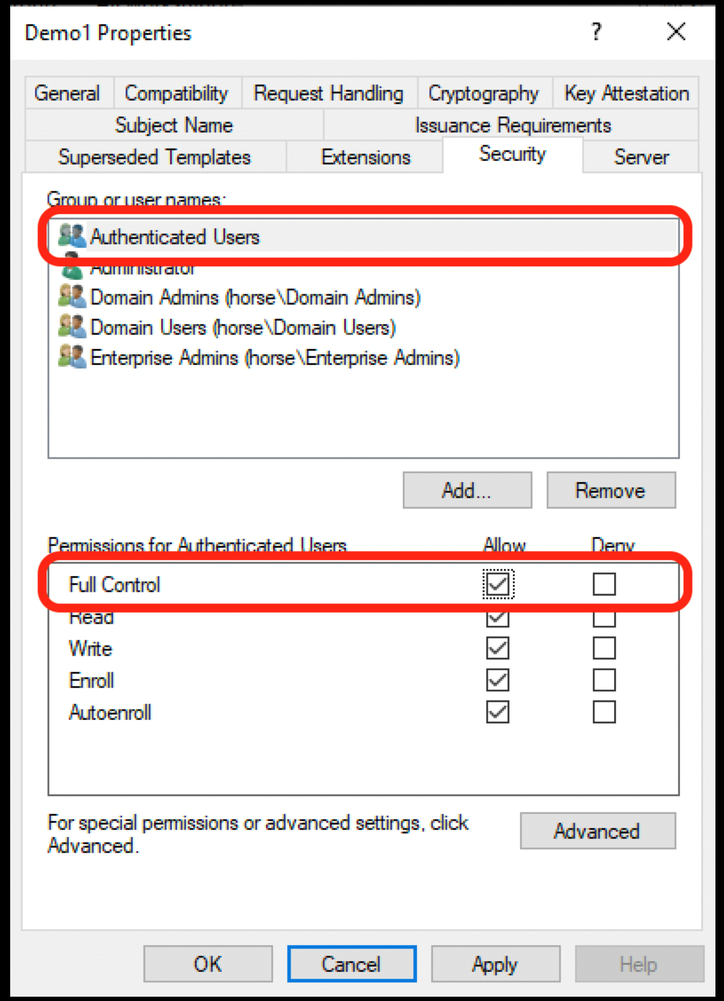
CHARLESTON

Combinations & Attack Paths

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

ESC4 → ESC1

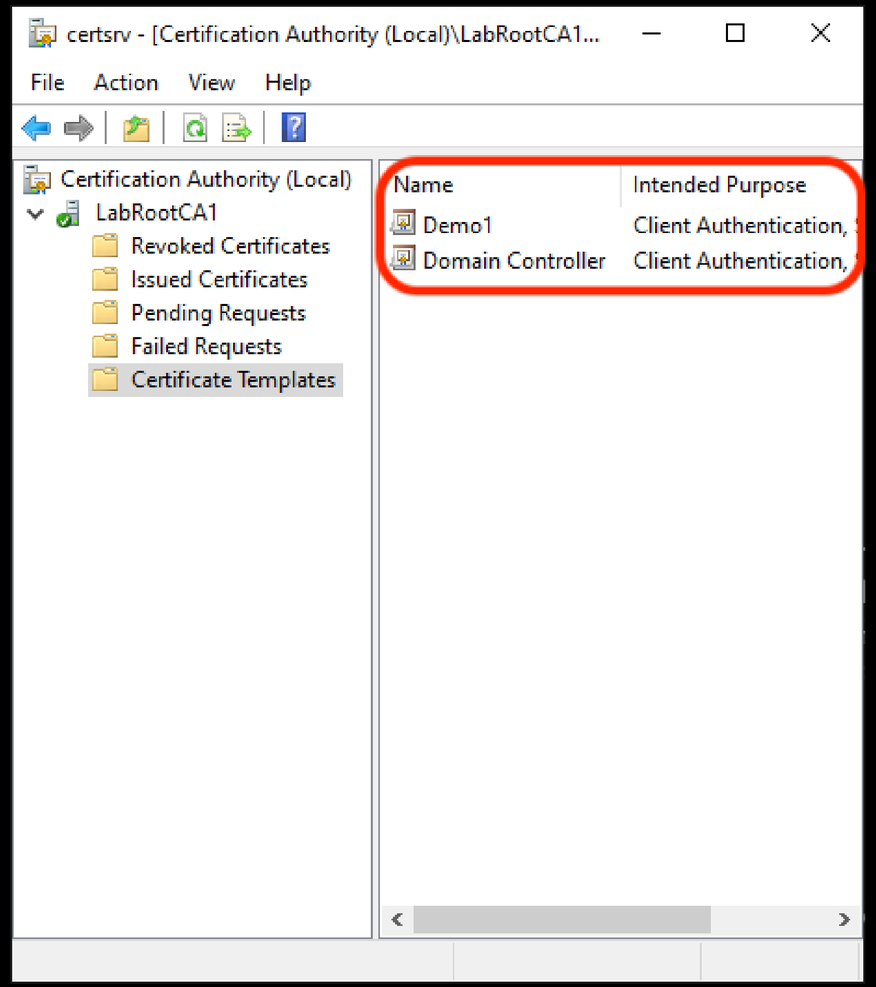
- Required Conditions:
  - **Low-privileged principals** have **Dangerous Rights** on a **Certificate Template** object



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

ESC4 → ESC1

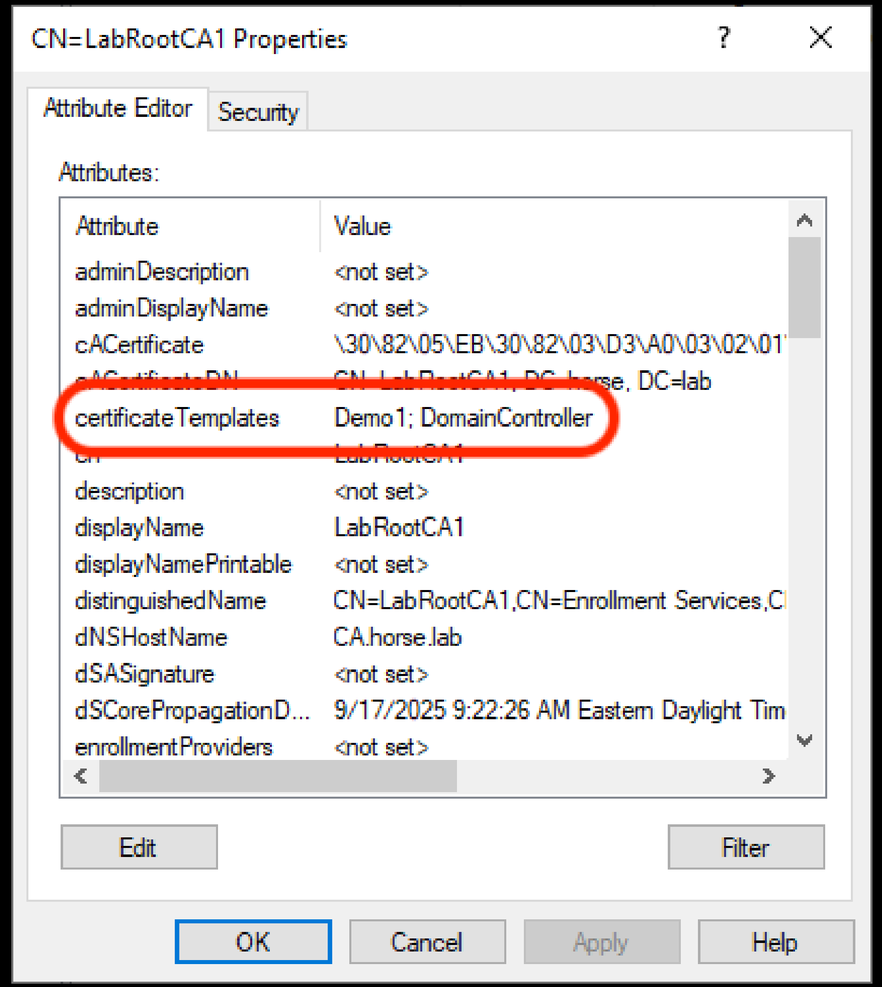
- Required Conditions:
  - Low-privileged principals have Dangerous Rights on a Certificate Template object
  - The Certificate Template is **Enabled** for enrollment on one or more **Certification Authorities (CA)**



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

ESC4 → ESC1

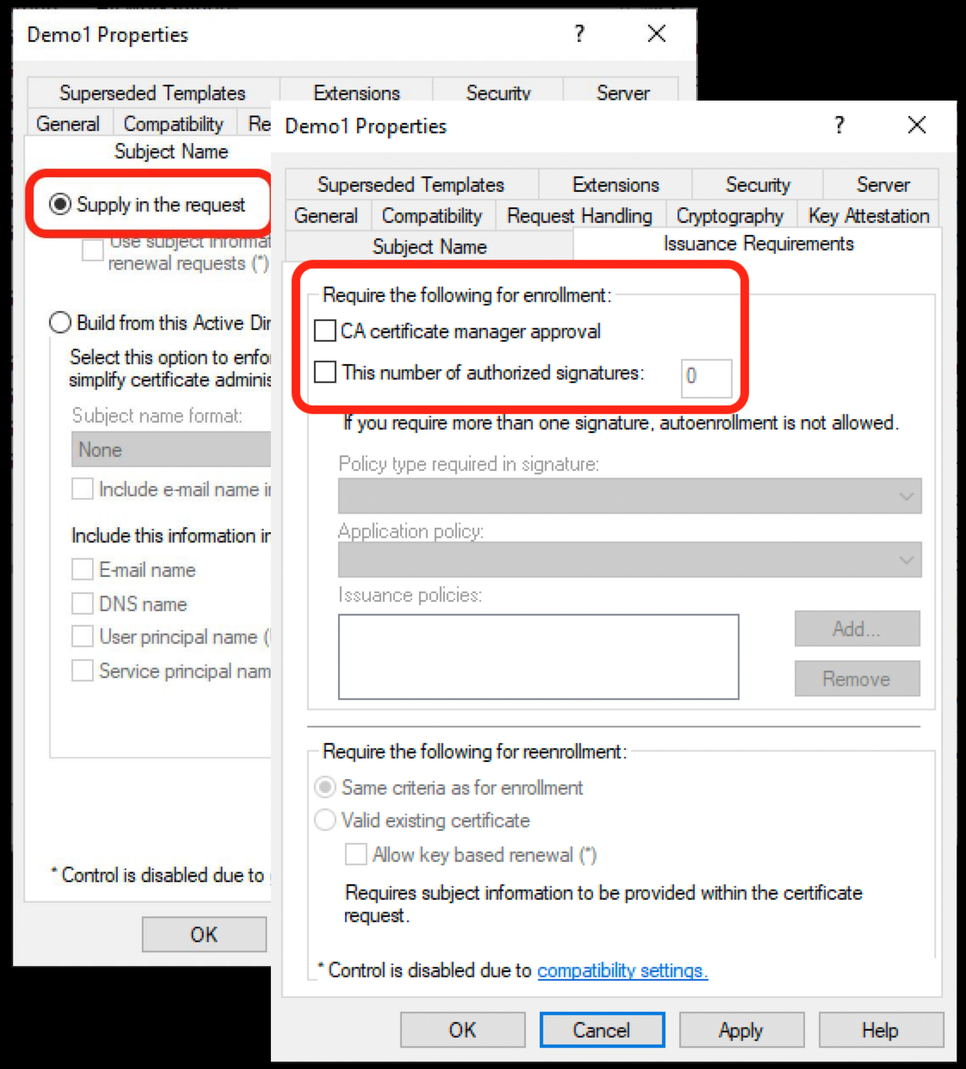
- Required Conditions:
  - Low-privileged principals have Dangerous Rights on a Certificate Template object
  - The Certificate Template is **Enabled** for enrollment on one or more **Certification Authorities (CA)**



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

ESC4 → ESC1

- Required Conditions:
  - Low-privileged principals have Dangerous Rights on a Certificate Template object
  - The Certificate Template is **Enabled** for enrollment on one or more Certification Authorities (CA)
- Attacker Process:
  - **Modifies** the vulnerable ESC4 template to match ESC1 conditions



ESC4 → ESC1

- Required Conditions:
  - Low-privileged principals have Dangerous Rights on a Certificate Template object
  - The Certificate Template is **Enabled** for enrollment on one or more Certification Authorities (CA)
- Attacker Process:
  - **Modifies** the vulnerable ESC4 template to match ESC1 conditions
  - **Requests** a certificate containing the **SAN** of a Tier 0 principal

```
.\Certify.exe request
/ca:ca.horse.lab\LabRootCA1
/template:Demo1
/altname:Administrator
/sid:[domain RID]-500
```

ESC4 → ESC1

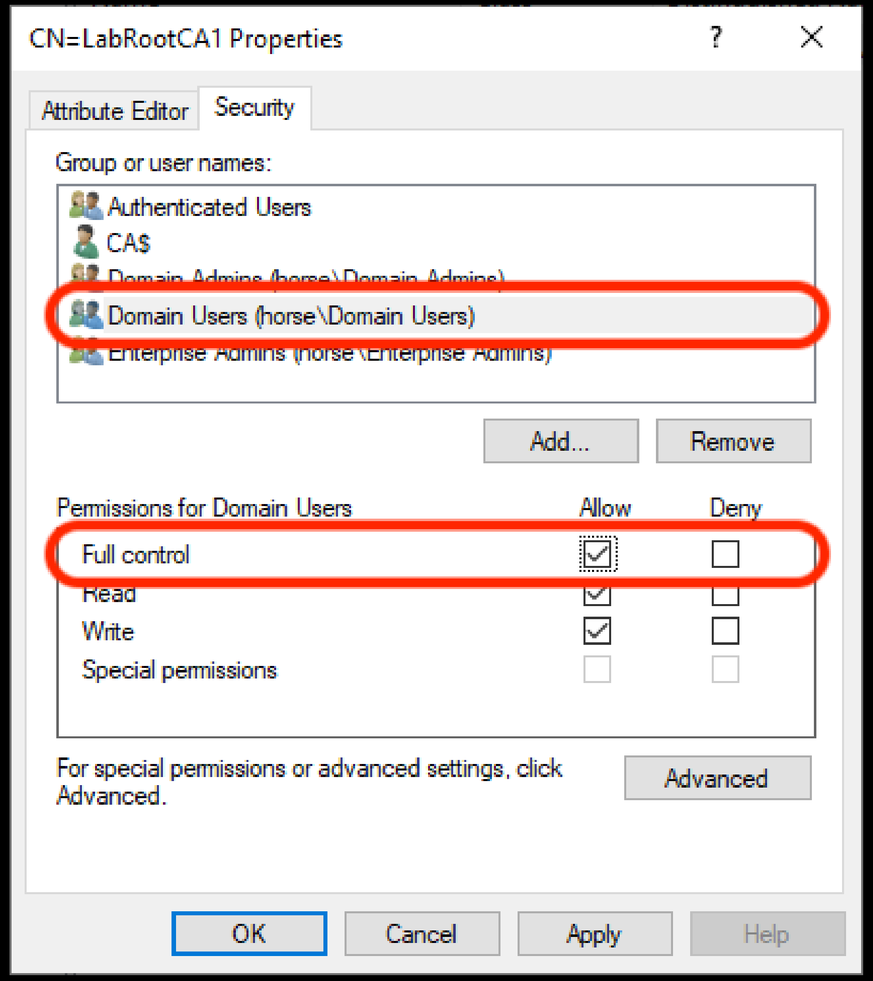
- Required Conditions:
  - Low-privileged principals have Dangerous Rights on a Certificate Template object
  - The Certificate Template is **Enabled** for enrollment on one or more Certification Authorities (CA)
- Attacker Process:
  - **Modifies** the vulnerable ESC4 template to match ESC1 conditions
  - **Requests** a certificate containing the SAN of a Tier 0 principal
  - **Authenticates** as Tier 0 principal

```
.\Rubeus.exe asktgt
/user:Administrator
/certificate:.\Demo1.pfx
/aes256 /ptt
```

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

ESC4 + ESC5 = ESC1

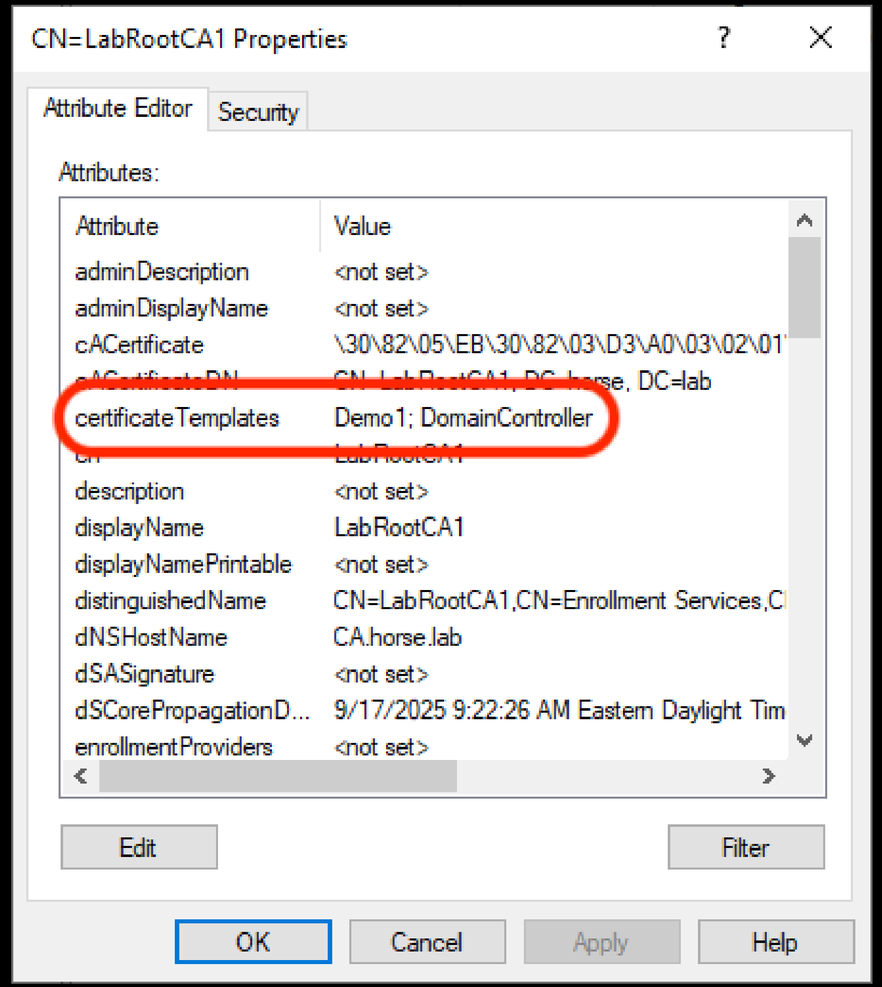
- Required Conditions:
  - Low-privileged principals have Dangerous Rights on a Certificate Template object
  - **Low-privileged principals** have **Dangerous Rights** on an **Enrollment Services** object (aka Issuing CA)



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

ESC4 + ESC5 = ESC1

- Required Conditions:
  - Low-privileged principals have Dangerous Rights on a Certificate Template object
  - Low-privileged principals have Dangerous Rights on an Enrollment Services object (aka Issuing CA)
- Attacker Process:
  - Modifies ESC4 template → ESC1
  - **Modifies** CA object to enable ESC1 template for enrollment



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

ESC4 + ESC5 = ESC1

- Required Conditions:
  - Low-privileged principals have **Dangerous Rights** on a **Certificate Template** object
  - Low-privileged principals have **Dangerous Rights** on an **Enrollment Services** object (aka an Issuing CA)
- Attacker Process:
  - Modifies ESC4 template → ESC1
  - Modifies CA object to enable ESC1 template for enrollment
  - **Requests** certificate as Tier 0 principal and **Authenticates**

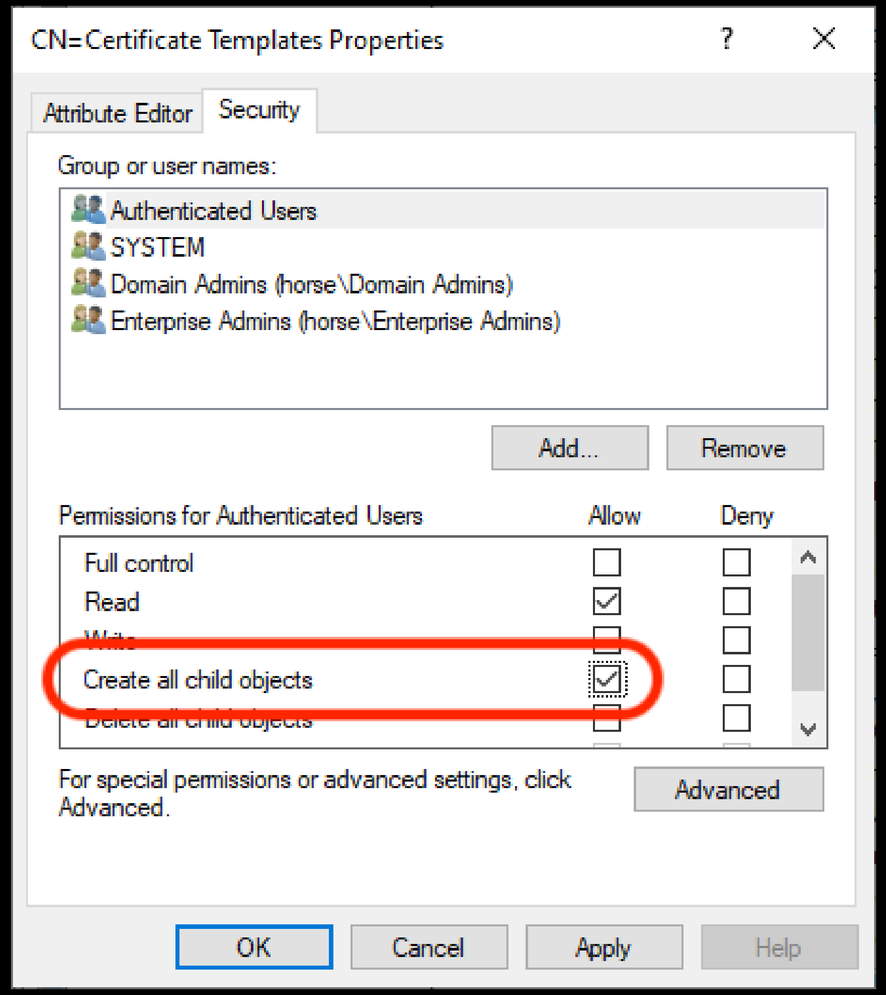
```
.\Certify.exe request
/ca:ca.horse.lab\LabRootCA1
/template:Demo1
/altname:Administrator
/sid:[domain RID]-500
```

```
.\Rubeus.exe asktgt
/user:Administrator
/certificate:.\Demo1.pfx
/aes256 /ptt
```

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

ESC5 + ESC5 = ESC1

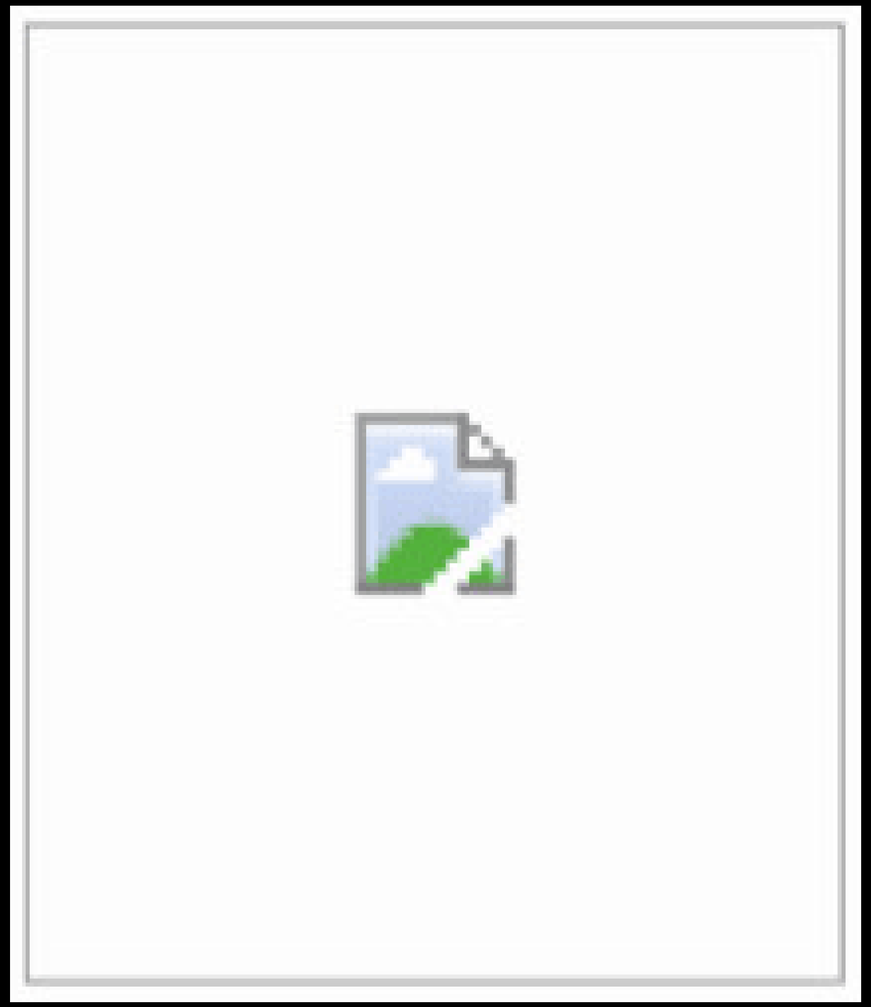
- Required Conditions:
  - **Low-privileged principals** can create **new objects** in **Certificate Templates** container



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

ESC5 + ESC5 = ESC1

- Required Conditions:
  - Low-privileged principals can create new objects in Certificate Templates container
  - Low-privileged principals have Dangerous Rights on an Enrollment Services object
- Attacker Process:
  - **Creates** ESC1 template



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

ESC5 + ESC5 = ESC1

- Required Conditions:
  - Low-privileged principals can create new objects in Certificate Templates container
  - Low-privileged principals have Dangerous Rights on an Enrollment Services object
- Attacker Process:
  - Creates ESC1 template
  - Modifies CA object to enable ESC1 template for enrollment
  - **Requests** certificate as Tier 0 principal and **Authenticates**

```
.\Certify.exe request
/ca:ca.horse.lab\LabRootCA1
/template:Demo1
/altname:Administrator
/sid:[domain RID]-500
```

```
.\Rubeus.exe asktgt
/user:Administrator
/certificate:.\Demo1.pfx
/aes256 /ptt
```

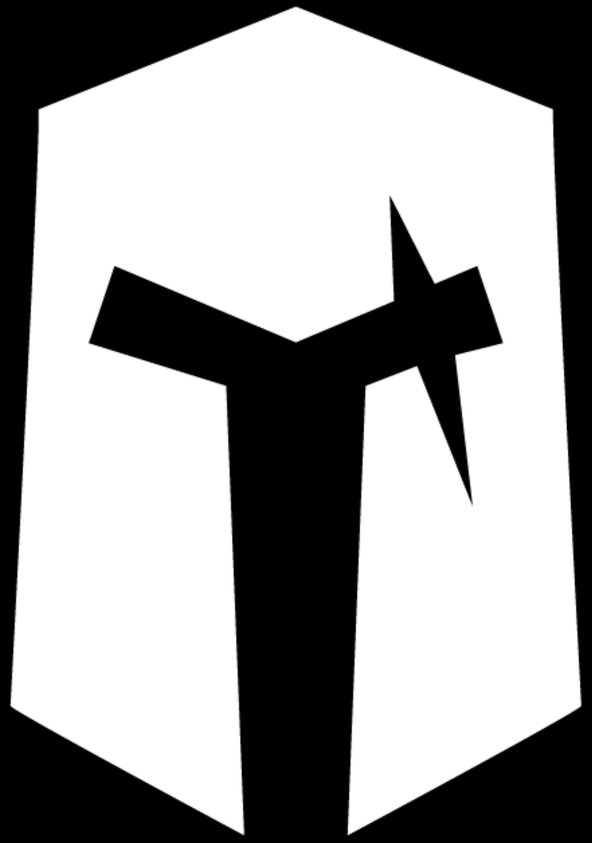
HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Limitations of Popular AD & AD CS Security Tools

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

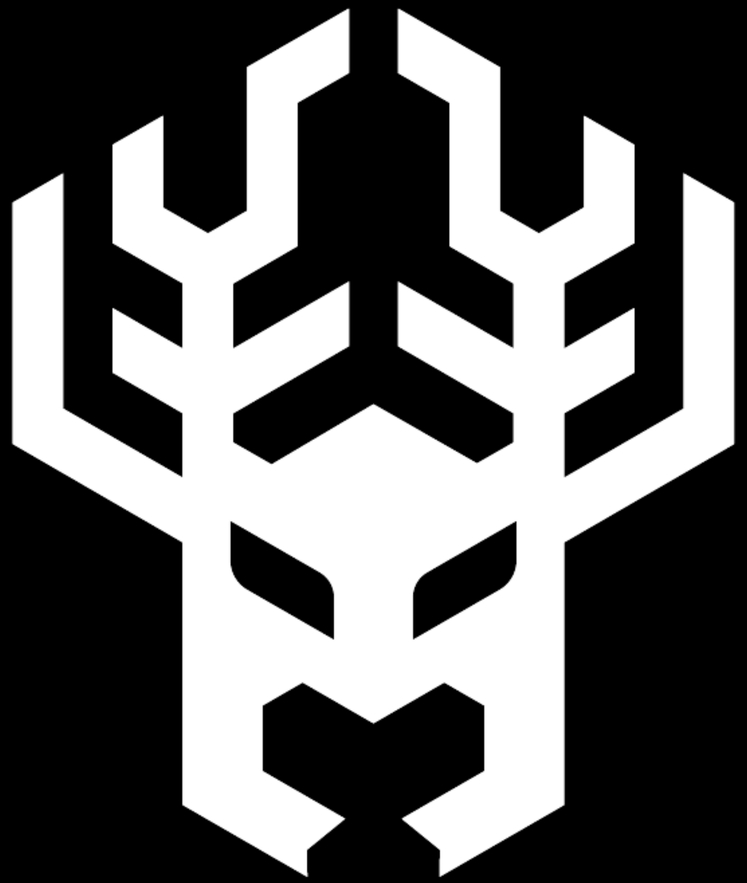
General AD Security Tools



- Purple Knight – Great for AD CS misconfigurations but not for attack paths

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

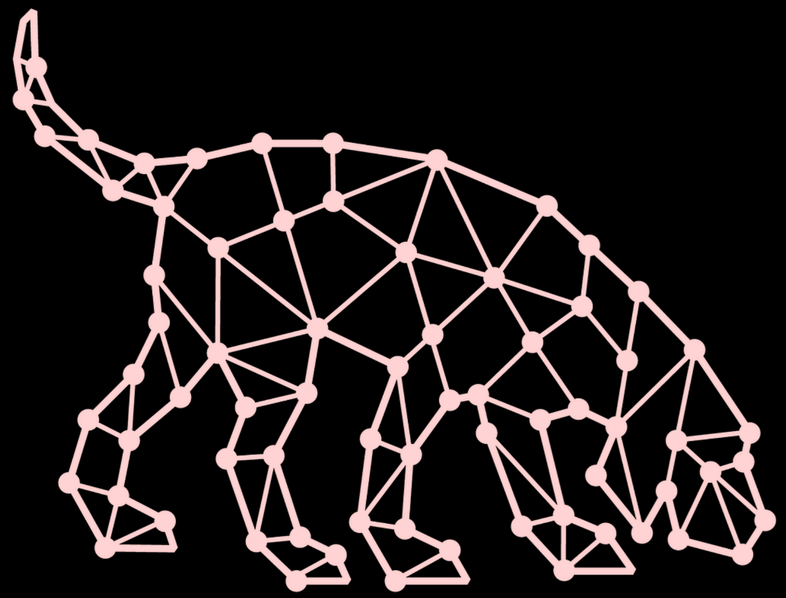
General AD Security Tools



- Purple Knight – Great for AD CS misconfigurations but not for attack paths
- Forest Druid – Great for attack paths but no full AD CS coverage *yet* 😉

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

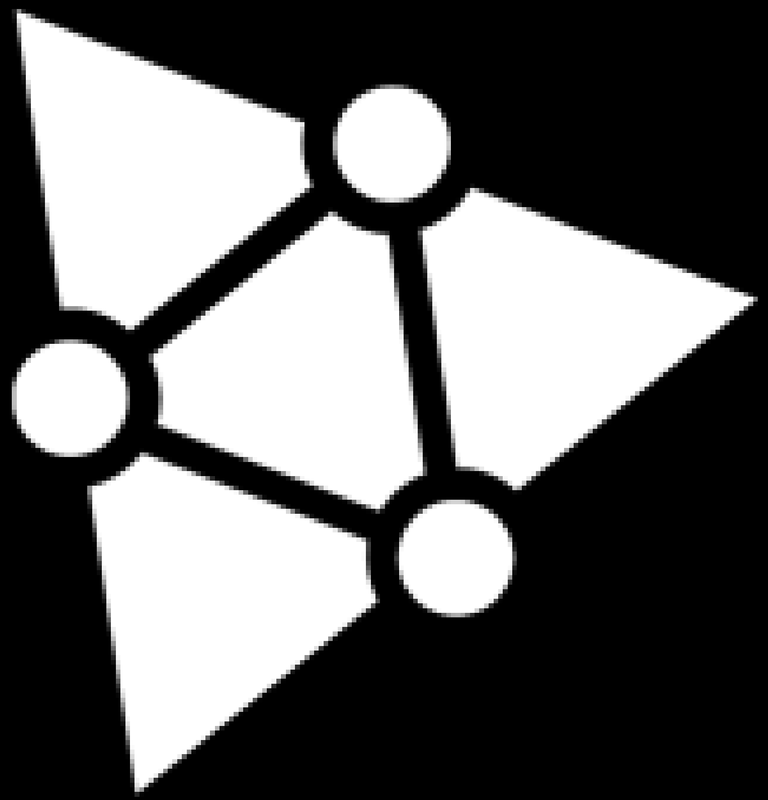
General AD Security Tools



- Purple Knight – Great for AD CS misconfigurations but not for attack paths
- Forest Druid – Great for attack paths but no full AD CS coverage *yet*
- BloodHound – Great for attack paths but can be overwhelming for non-security folks

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

General AD Security Tools



- Purple Knight – Great for AD CS misconfigurations but not for attack paths
- Forest Druid – Great for attack paths but no full AD CS coverage *yet*
- BloodHound – Great for attack paths but can be overwhelming for non-security folks
- PingCastle – Good for AD CS misconfigurations but not for attack paths

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

AD CS-specific Security Tools

- Certify
  - Individual vulnerabilities only
  - No risk/severity ratings
  - Requires manual compilation

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

AD CS-specific Security Tools


```
certipy req \
    -u 'attacker@corp.local' -p 'Passw0rd!' \
    -dc-ip '10.0.0.100' -target 'CA.CORP.LOCAL' \
    -ca 'CORP-CA' -template 'VulnTemplate' \
    -upn 'administrator@corp.local' -sid '...-500'
```

- Certify
  - Individual vulnerabilities only
  - No risk/severity ratings
  - Requires manual compilation
- Certipy
  - Individual vulnerabilities only (but with remarks when multiple vulnerabilities could interact)
  - No risk/severity ratings
  - Written in Python 😭

AD CS-specific Security Tools

- PSPKIAudit
  - Individual vulnerabilities only
  - No risk/severity ratings
  - Only covers ESC1-8
  - No longer maintained

AD CS-specific Security Tools

- PSPKIAudit
  - Individual vulnerabilities only
  - No risk/severity ratings
  - Only covers ESC1-8
  - No longer maintained
- Locksmith
  - No visualization of combo attacks
  - Requires AD PowerShell module

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Introducing:

ESCalator

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

“A tiny tool built for **identifying and abusing** AD CS issue combinations that may not be readily obvious”

Demo 1

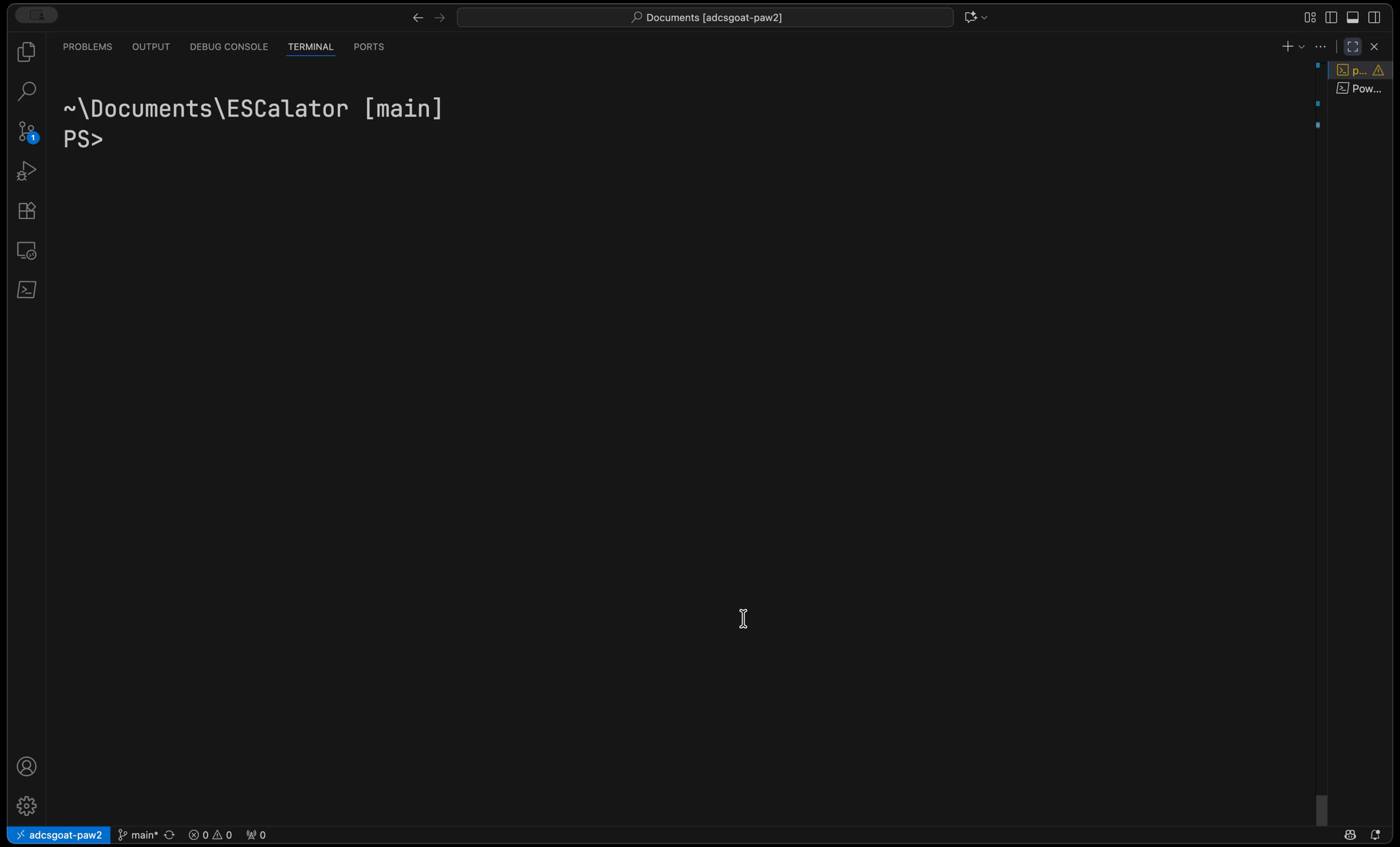
Finding Combinations

+

Attack Planning

HYBRID IDENTITY PROTECTION conf25

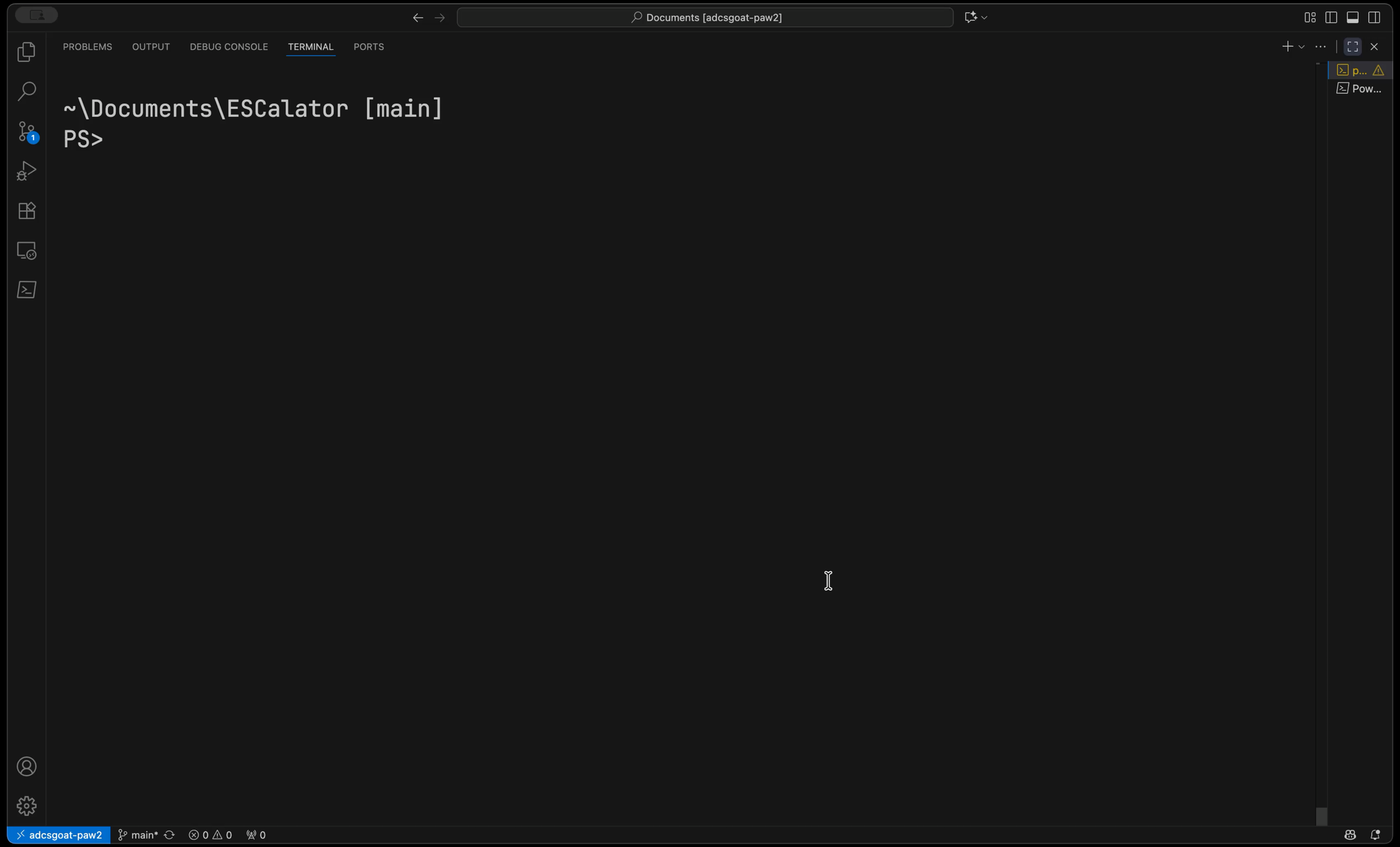
CHARLESTON


Documents [adcsgoat-paw2]
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
~\Documents\ESCalator [main]
PS>
p...
Pow...
adcsgoat-paw2
main*
0 0
0

Demo 2

ESC4 → ESC1

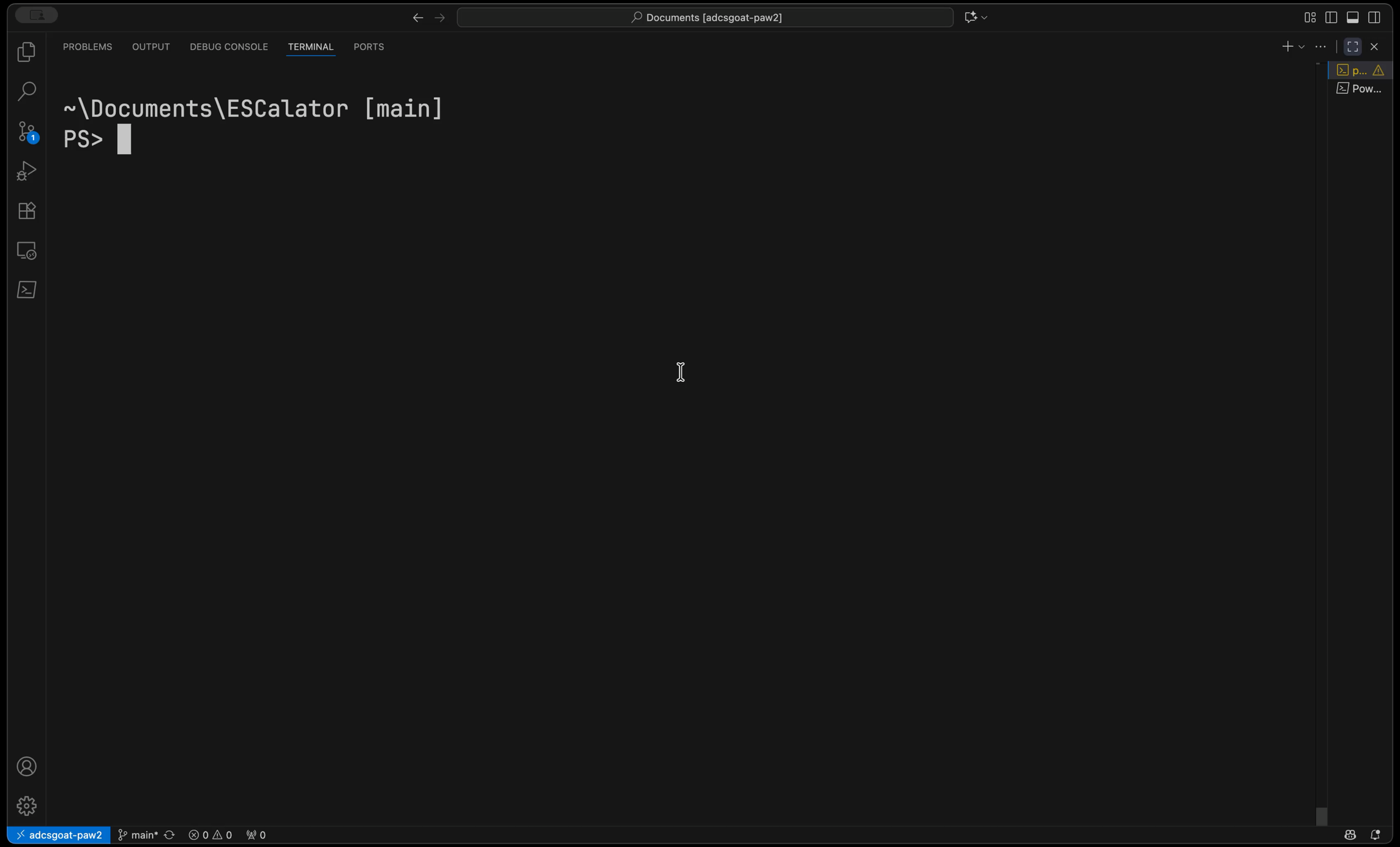
HYBRID IDENTITY PROTECTION conf25 CHARLESTON


Documents [adcsgoat-paw2]
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
~\Documents\ESCalator [main]
PS>
p...
Pow...
adcsgoat-paw2
main*
0 0
0

Demo 3

ESC4 + ESC5 = ESC1

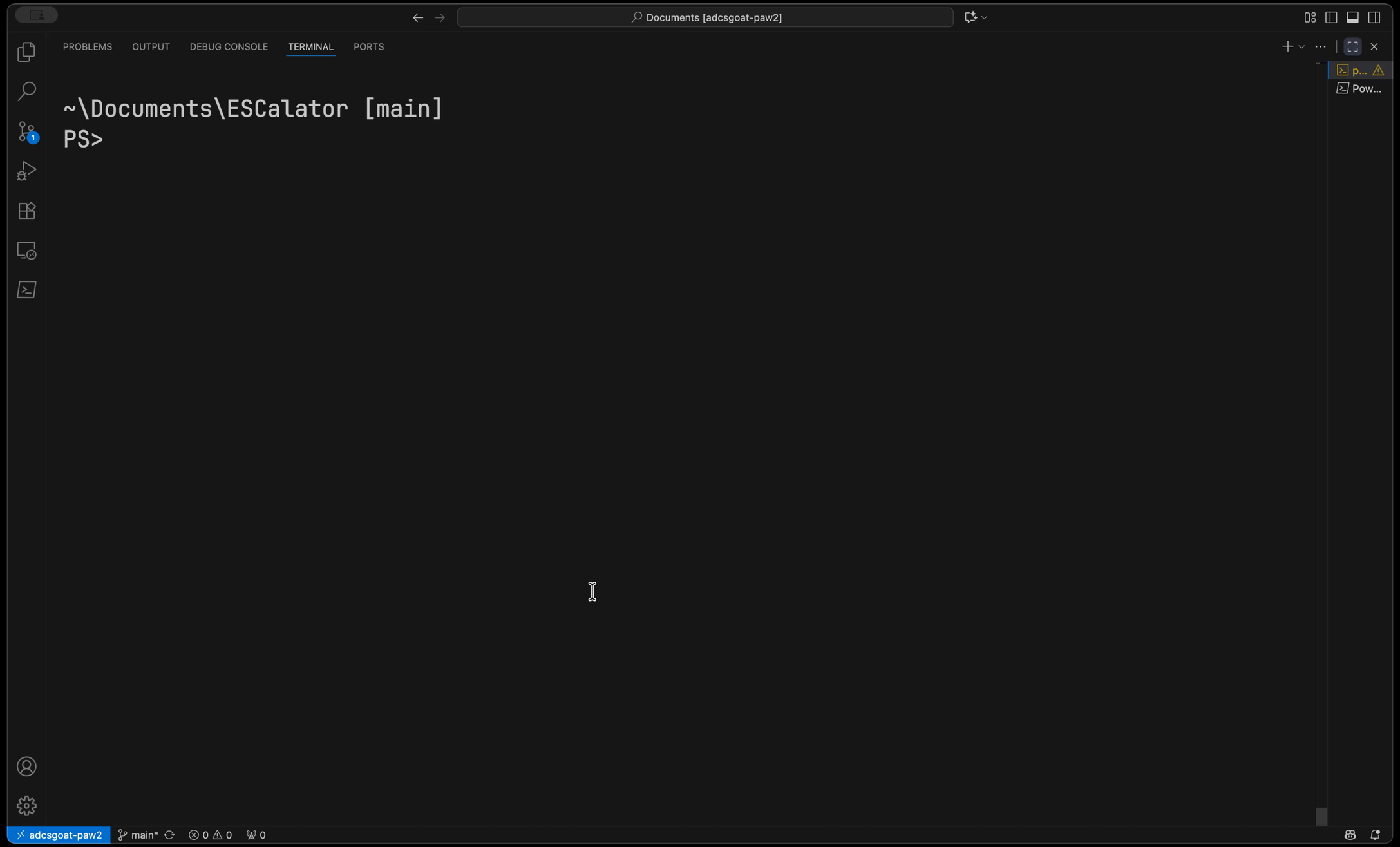
HYBRID IDENTITY PROTECTION conf25 CHARLESTON


Documents [adcsgoat-paw2]
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
~\Documents\ESCalator [main]
PS>
p...
Pow...
adcsgoat-paw2
main*
0 0
0

Demo 4

ESC5 + ESC5 = ESC1

HYBRID IDENTITY PROTECTION conf25 CHARLESTON


Documents [adcsgoat-paw2]
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
~\Documents\ESCalator [main]
PS>
p...
Pow...
adcsgoat-paw2
main*
0 0
0

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Key Takeaways

- New AD CS attacks are continually being developed
- AD CS is **still** very easy to misconfigure 😭
- Low- and Medium-priority issues can stack quickly and go unnoticed and undefended when automated

Thanks!

- Andrew Pla
- Arnim Rupp
- Benjamin Delpy
- Brandon Colley
- Carl Sörqvist
- Christoph Falta
- Elkement
- Emmanuel Ferdman
- Hans-Joachim Knobloch
- Hermon Kidane
- Huy Kha
- Jim Sykora
- Jonas Bülow Knudsen
- Jonathan Colon
- Justin Bollinger
- Justin Connors
- Justin Palk
- Lars Karlslund
- Lee Chagolla-Christensen
- Lenoardo Nuñez
- Maciej Kosz
- Martin Plattner
- Mike Jankowski-Lorek
- Mike Saunders
- Oliver Lyak
- Przemysław Kłys
- Sam Erde
- Sean Metcalf
- Spencer Alessi
- Sylvain Heineger
- Tim Medin
- Uwe Gradenegger
- Will Schroeder

Questions?

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Have identity security and resiliency concerns? Visit semperis.com

For references, resources, and other projects, visit jakehildreth.com

Let's Connect!

References and Educational Materials

- https://blog.chrisse.se/?p=1162
- https://blog.qdsecurity.se/author/carlsorqvist/
- https://cqureacademy.com/blog/enhanced-key-usage
- https://elkement.art/2019/06/01/sizzle-hackthebox-unintended-getting-a-logon-smartcard-for-the-domain-admin-2/
- https://elkement.art/2020/06/21/impersonating-a-windows-enterprise-admin-with-a-certificate-kerberos-pkinit-from-linux/
- https://ethicalchaos.dev/2020/10/04/attacking-smart-card-based-active-directory-networks/
- https://gist.github.com/jakehildreth/13c7d615adc905d317fc4379026ad28e
- https://github.com/CarlSorqvist/PsCertTools/tree/main/NTAuthGuard
- https://github.com/cfalta/PoshADCS
- https://github.com/gentilkiwi/kekeo
- https://github.com/gentilkiwi/mimikatz
- https://github.com/GhostPack/Certify
- https://github.com/GhostPack/PSPKIAudit
- https://github.com/jakehildreth/Locksmith
- https://github.com/ly4k/Certipy
- https://github.com/Sleepw4lker/TameMyCerts
- https://github.com/SpecterOps/BloodHound
- https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc732443(v=ws.11)?redirectedfrom=MSDN
- https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/active-directory-certificate-services-overview
- https://m365xazure.de/security/watch-out-for-certificate-theft/
- https://mcselles.wordpress.com/2016/02/22/certutil-examples-for-managing-active-directory-certificate-services-ad-cs-from-the-command-line/
- https://research.ifcr.dk/certifried-active-directory-domain-privilege-escalation-cve-2022-26923-9e098fe298f4
- https://research.ifcr.dk/certipy-4-0-esc9-esc10-bloodhound-gui-new-authentication-and-request-methods-and-more-7237d88061f7
- https://www.semperis.com/forest-druid/
- https://www.semperis.com/purple-knight/
- https://virot.eu/pretty-list-of-certificate-authorities-that-ad-trusts-for-auth/
- https://www.gradenegger.eu/en/configuration-of-security-event-monitoring-auditing-settings-for-certification-bodies/
- https://www.keyfactor.com/blog/hidden-dangers-certificate-subject-alternative-names-sans/
- https://www.pingcastle.com
- https://www.sysadmins.lv/blog-en/how-to-read-adcs-enrollment-agentcertificate-manager-rights-in-powershell.aspx
- https://www.sysadmins.lv/blog-en/understanding-active-directory-certificate-services-containers-in-active-directory.aspx