REDHOT

(Red Team TTPs)

https://redhot.hackerops.dev
https://slides.com/rvrsh3ll/red-hot

RALPH MAY

@ralphte1

github.com/ralphte

hackerops.dev

Black Hills Information Security

STEVE BOROSH

@424f424f

github.com/rvrsh3ll

medium.com/@rvrsh3ll

futuresec.io

Black Hills Information Security

FUTURESEC TRAINING

https://futuresec.io/

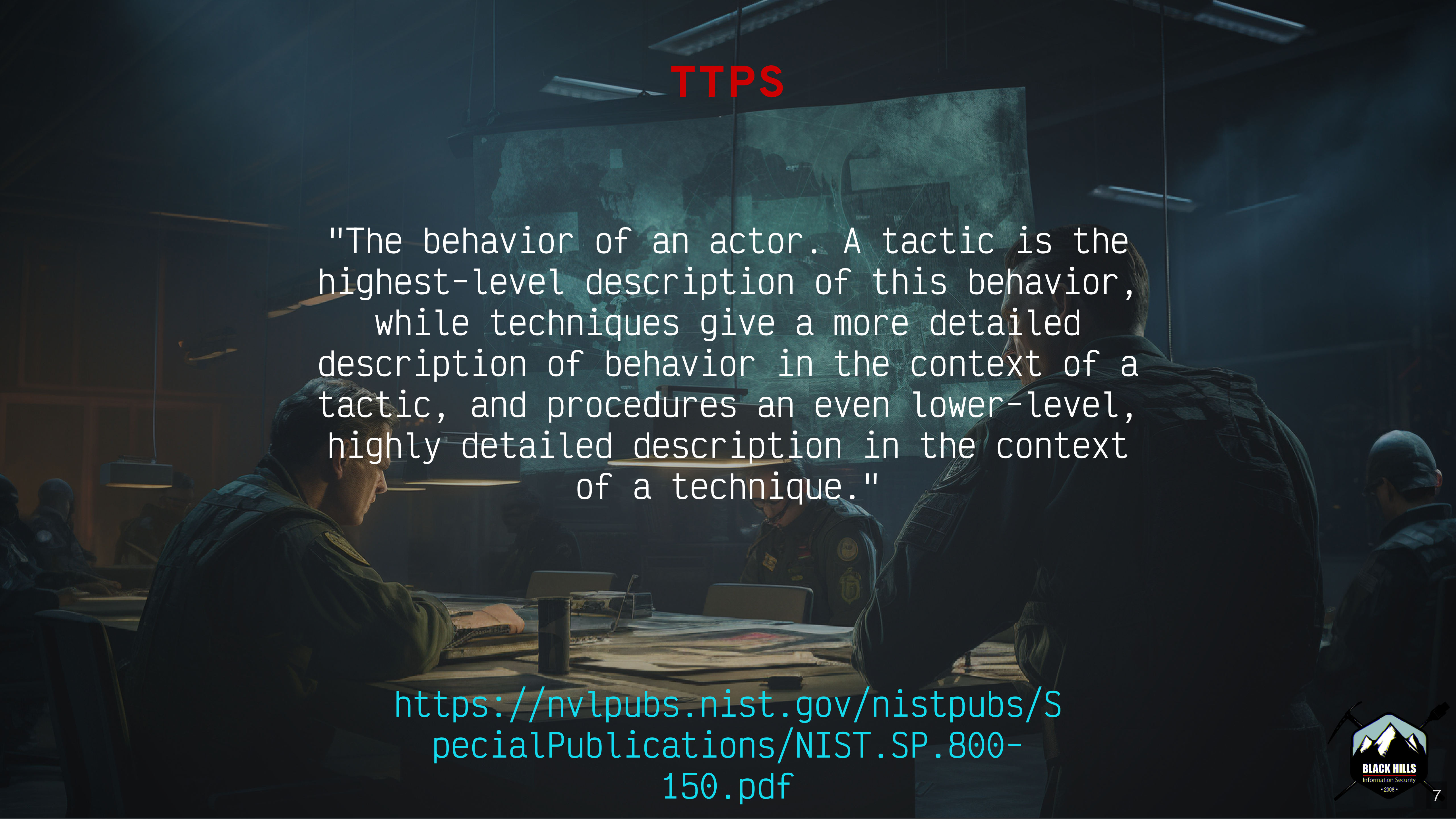
WORKSHOP OVERVIEW

- Enhance red team operators' knowledge of trending TTPs across several MITRE Techniques
- Cross fingers
- Create a custom C2 payload combining several TTPs for remote access to a network.

LAB SETUP

- Ubuntu virtual machine.
- Windows 10/11 with Visual Studio Community Edition installed.

TTPS



"The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique."

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

EXAMPLE TACTICS

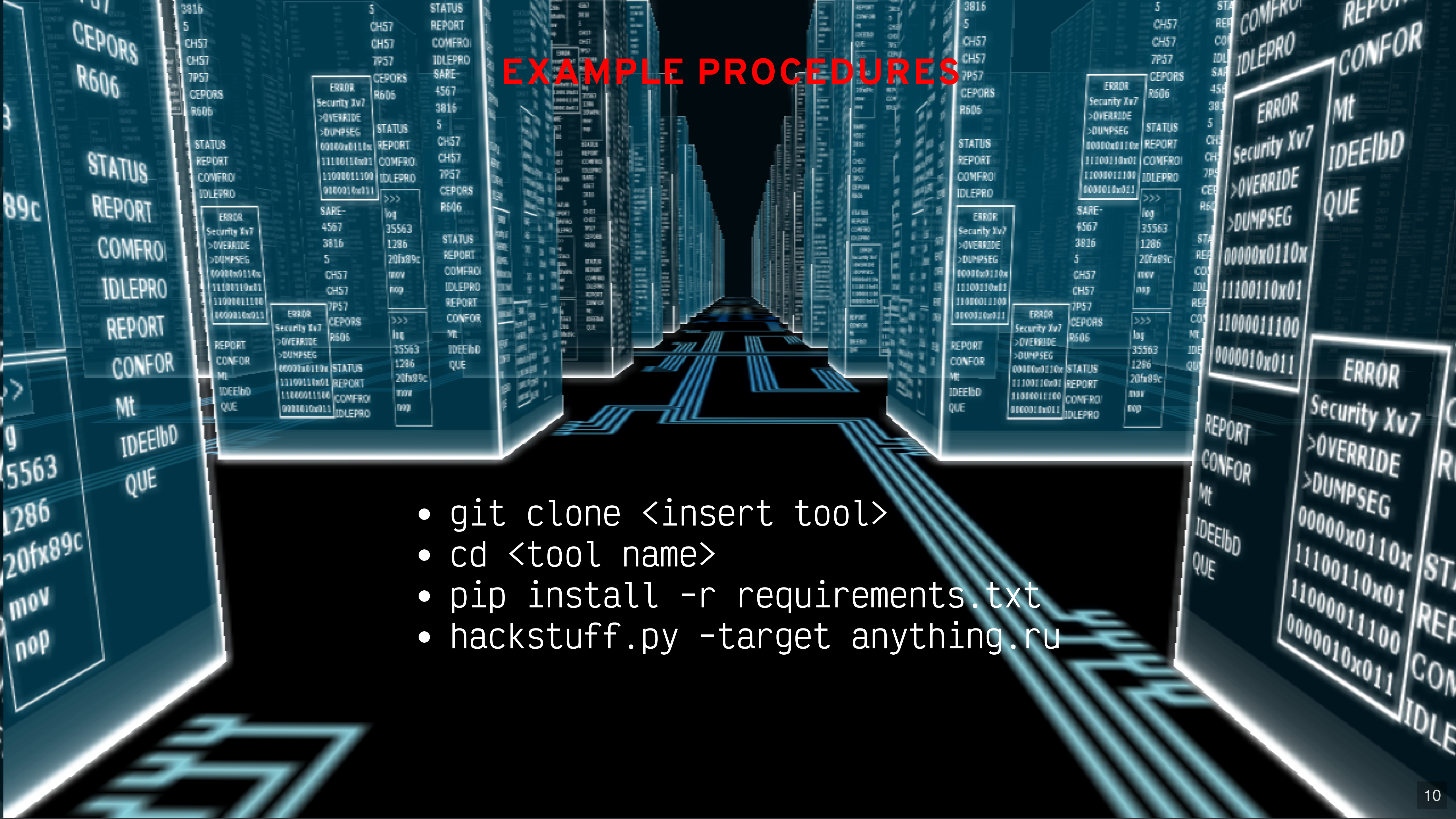
- Reconnaissance
- Execution
- Credential Access

https://attack.mitre.org/tactics/enterprise/

EXAMPLE TECHNIQUES

- Active Scanning
- PowerShell
- LSASS Dumping

https://attack.mitre.org/techniques/enterprise/



EXAMPLE PROCEDURES

- git clone <insert tool>
- cd <tool name>
- pip install -r requirements.txt
- hackstuff.py -target anything.ru

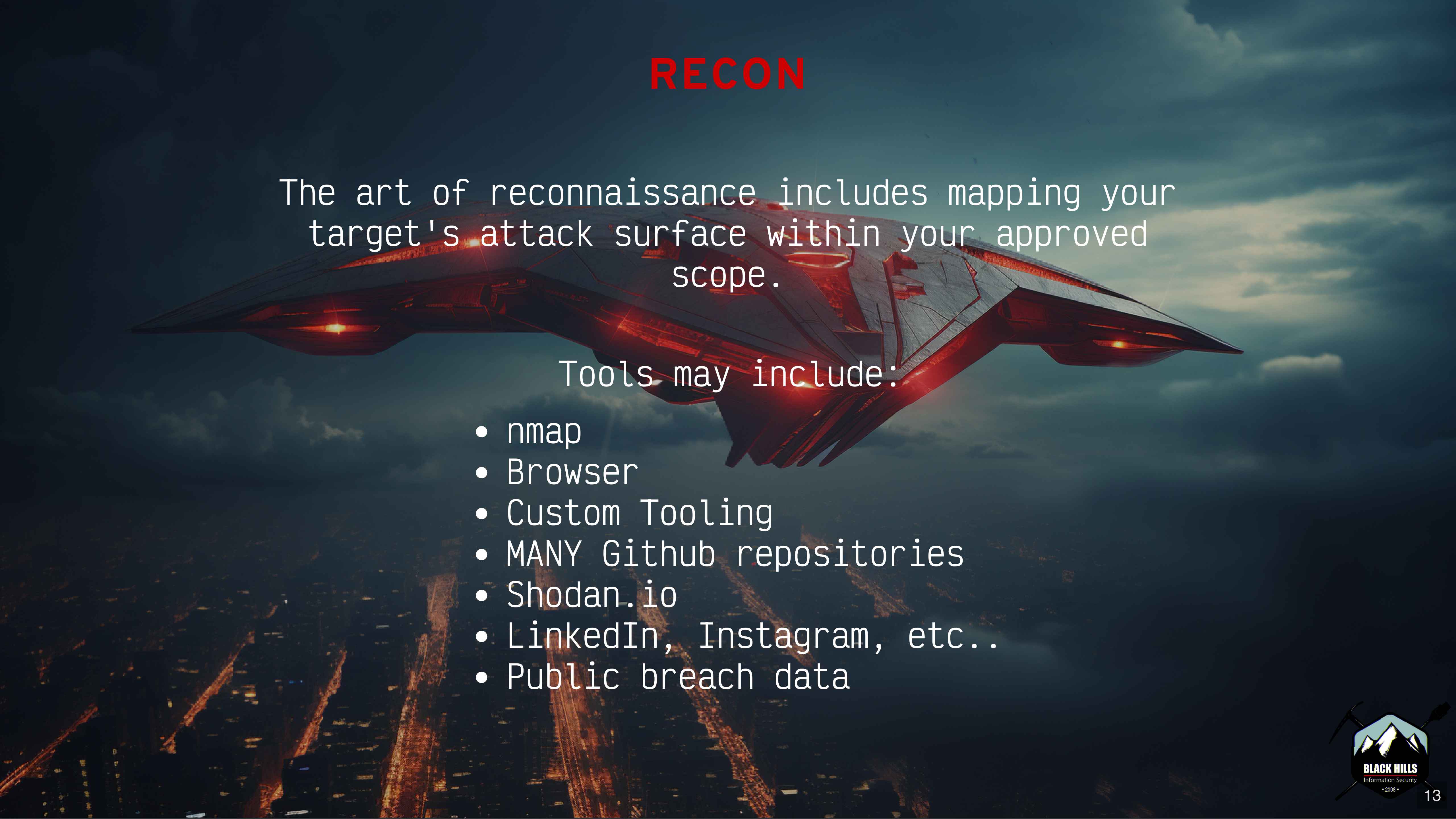
PHASES OF TTPS COVERED

- Recon
- Social Engineering
- Cloud
- Initial Access
- Post Exploitation

RECON TARGETS

Recon targets may include:

- Company Information
  - Usernames
  - Access portals
  - Files
  - Github repositories
- User information
  - Passwords
  - PII
  - Social Media
- Networks
  - By CIDR
  - By domain/subdomain



RECON

The art of reconnaissance includes mapping your target's attack surface within your approved scope.

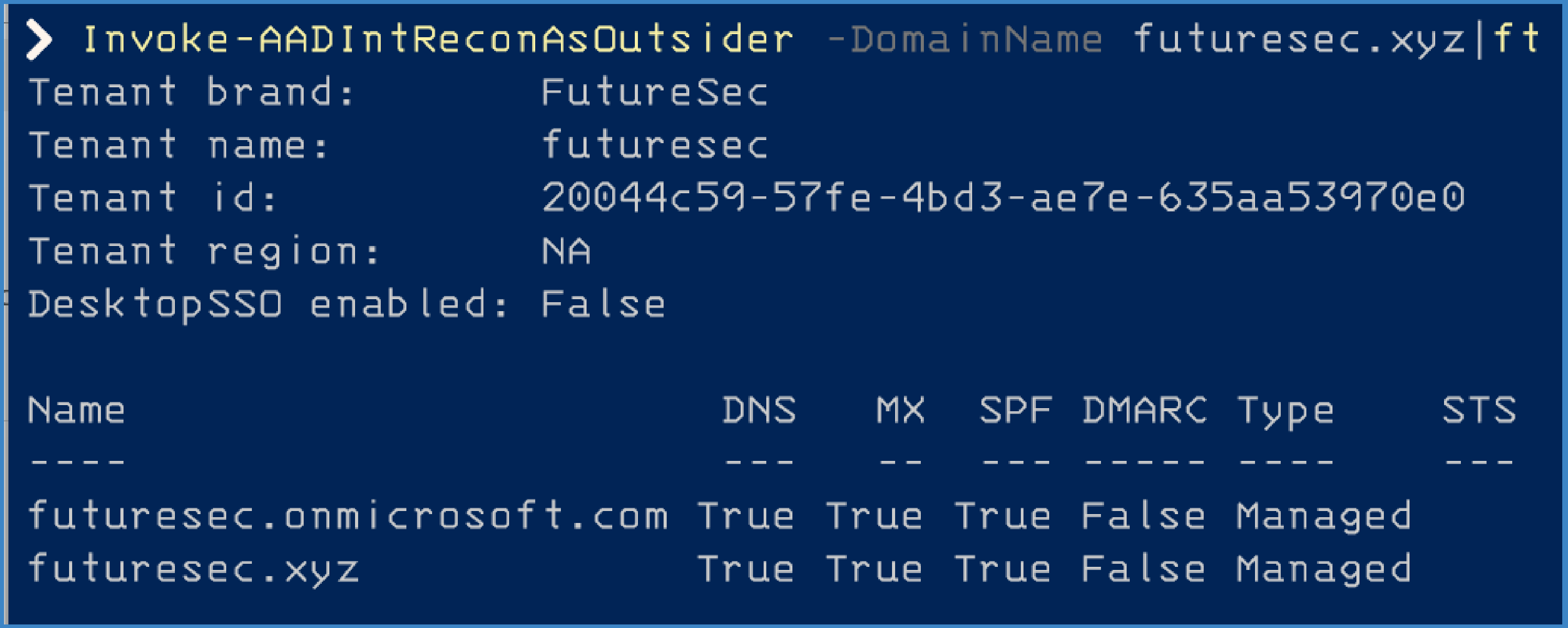
Tools may include:

- nmap
- Browser
- Custom Tooling
- MANY Github repositories
- Shodan.io
- LinkedIn, Instagram, etc..
- Public breach data

MICROSOFT AZURE RECON

AADINTERNALS

```
Invoke-AADIntReconAsOutsider -Domain company.com |ft
```



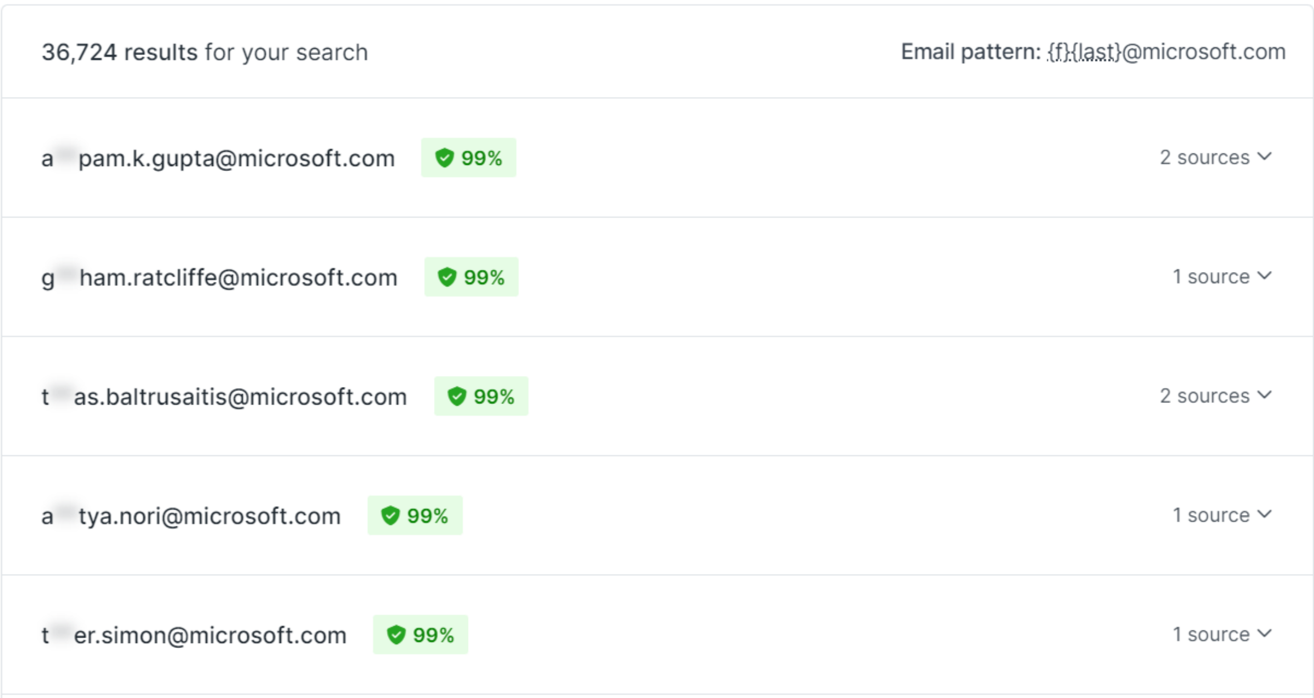
```
> Invoke-AADIntReconAsOutsider -DomainName futuresec.xyz|ft
Tenant brand:       FutureSec
Tenant name:        futuresec
Tenant id:          20044c59-57fe-4bd3-ae7e-635aa53970e0
Tenant region:      NA
DesktopSSO enabled: False

Name                       DNS  MX   SPF  DMARC Type    STS
----                       ---  --   ---  ----- ----    ---
futuresec.onmicrosoft.com True True True False Managed
futuresec.xyz             True True True False Managed
```

DNS RECON

- Many tools and mostly personal pereference
- Do it for each domain that's in-scope and attached to Azure Tenant
- Feed results to other tools for further enumeration
- Certificate Transparency Searching cert.sh may reveal internal hostnames

LINKEDIN EMAIL GENERATION

{FIRST}.{LAST}@COMPANY.COM



36,724 results for your search Email pattern: {f}{last}@microsoft.com

a[redacted]pam.k.gupta@microsoft.com 99% 2 sources

g[redacted]ham.ratcliffe@microsoft.com 99% 1 source

t[redacted]as.baltrusaitis@microsoft.com 99% 2 sources

a[redacted]tya.nori@microsoft.com 99% 1 source

t[redacted]er.simon@microsoft.com 99% 1 source

GoMapEnum

https://github.com/EatonChips/yalis

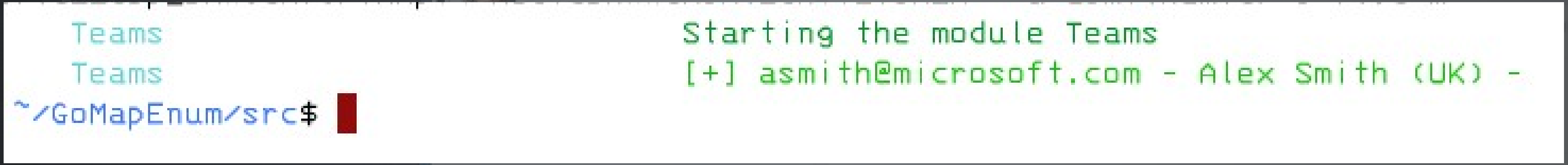
Yalis

https://github.com/nodauf/GoMapEnum

REDHOT TTP

MICROSOFT TEAMS USER ENUMERATION

- Accurate
- Stealthy
- In many cases you may still enumerate users if blocked from sending messages



```
  Teams                              Starting the module Teams
  Teams                              [+] asmith@microsoft.com - Alex Smith (UK) -
~/GoMapEnum/src$ 
```

https://techcommunity.microsoft.com/t5/microsoft-teams-blog/microsoft-teams-users-can-now-chat-with-any-teams-user-outside/ba-p/3070832

SOCIAL ENGINEERING

"Social engineering has become about 75% of an average hacker's toolkit, and for the most successful hackers, it reaches 90% or more." - John McAfee

- Still true if not more so
- Part of our daily lives
- Influence others
- "Would you grab me a cup of coffee while you're in Starbucks?"
- "Hi Jan, I'm Joe from IT and your PC requires an update that we cannot deploy from here. We need you to run this quick patch for your pc. Can you help us real quick after your meeting?"

TYPES OF SE

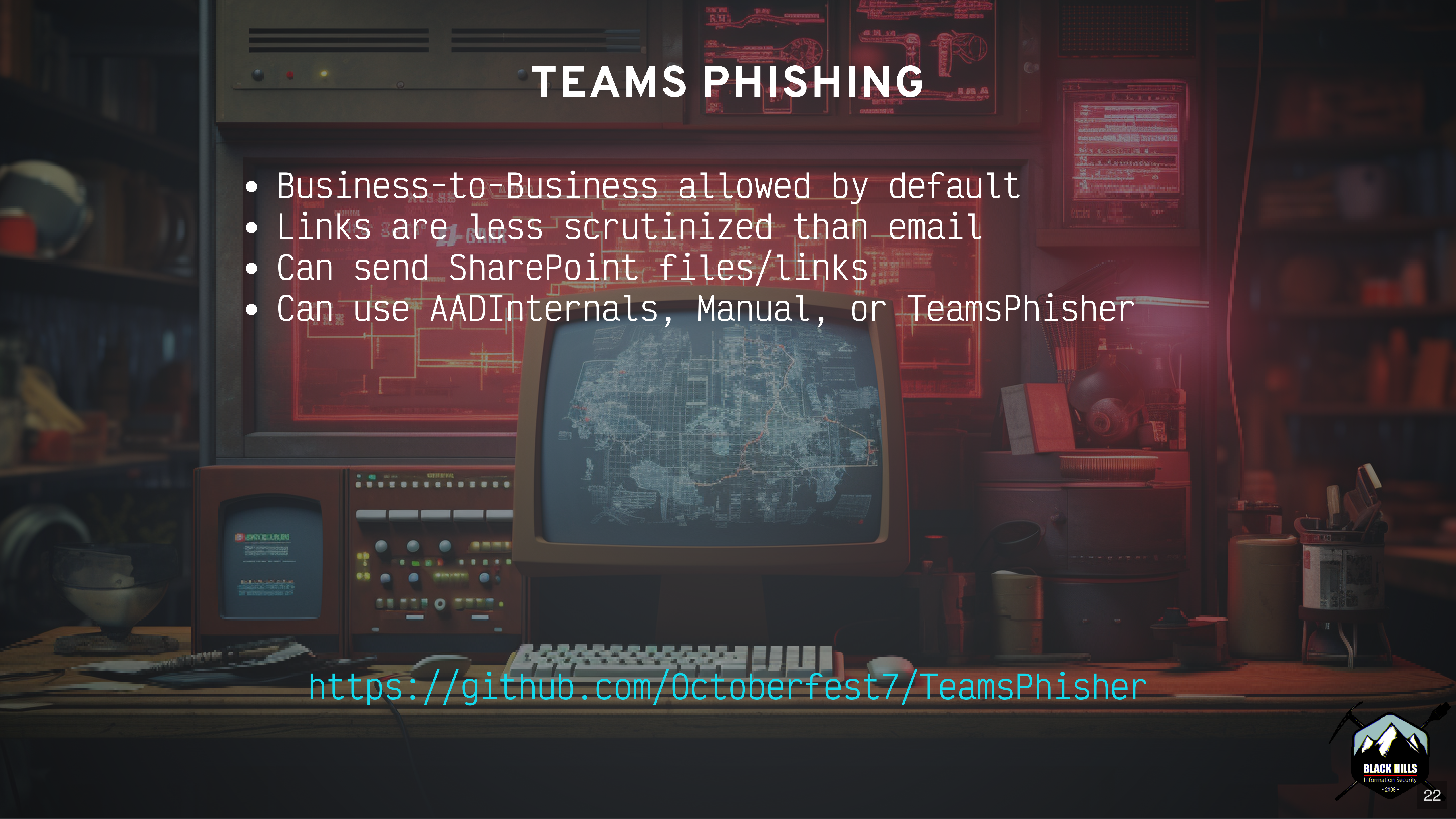
- Face-to-face conversation
- Phishing
- Vishing
- Smishing
- *ishing. (any way to communicate)

OFFICE 365 SPOOFING

- SMTP Smart Host "company-com.mail.protection.outlook.com"
- Send-MailMessage -SMTPServer <insert>
- Default
- May bypass some gateways
- Spoof External to Internal and Internal to Internal

https://www.blackhillsinfosec.com/spoofing-microsoft-365-like-its-1995/

TEAMS PHISHING



- Business-to-Business allowed by default
- Links are less scrutinized than email
- Can send SharePoint files/links
- Can use AADInternals, Manual, or TeamsPhisher

https://github.com/Octoberfest7/TeamsPhisher

REVERSE RDP PHISH

- Send .rdp file
- User connects back to your server
- Capture clipboard, plant files, and steal files

Mike Felch @ustayready

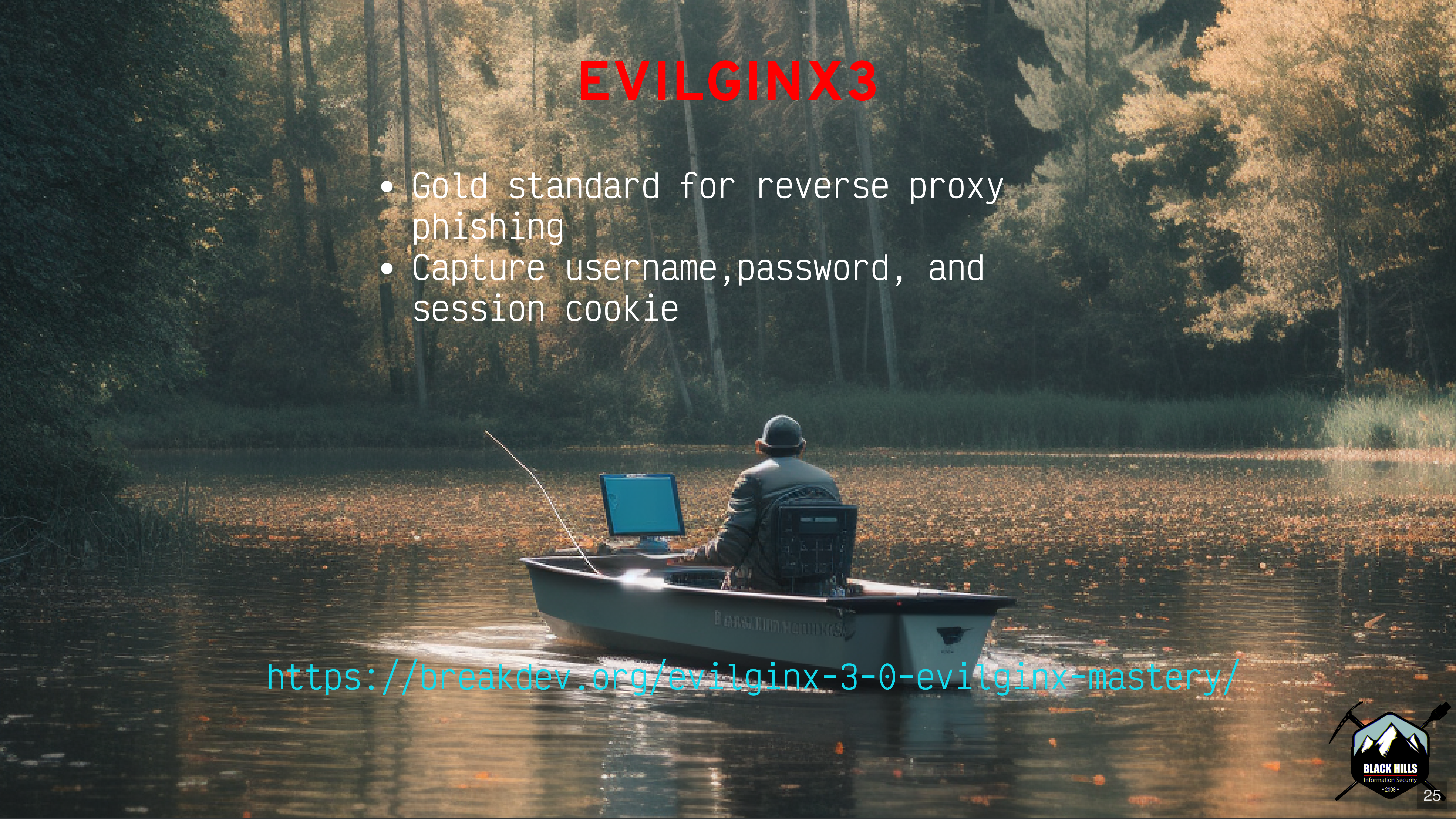
https://www.youtube.com/watch?v=csZ-joDJ1BE

SMISHING

- Cred captures
- Fingerprint devices
- TokenTactics
- Bypass normal Phishing Controls

EVILGINX3

- Gold standard for reverse proxy phishing
- Capture username,password, and session cookie



https://breakdev.org/evilginx-3-0-evilginx-mastery/

REDHOT TTP

AI VISHING

- Using AI to impersonate and fool another person into performing some action.
- Real-Time Voice
- Text to Voice
  - resemble.ai
  - voice.ai
  - speechify.com

John Strand

CLOUD

Targets

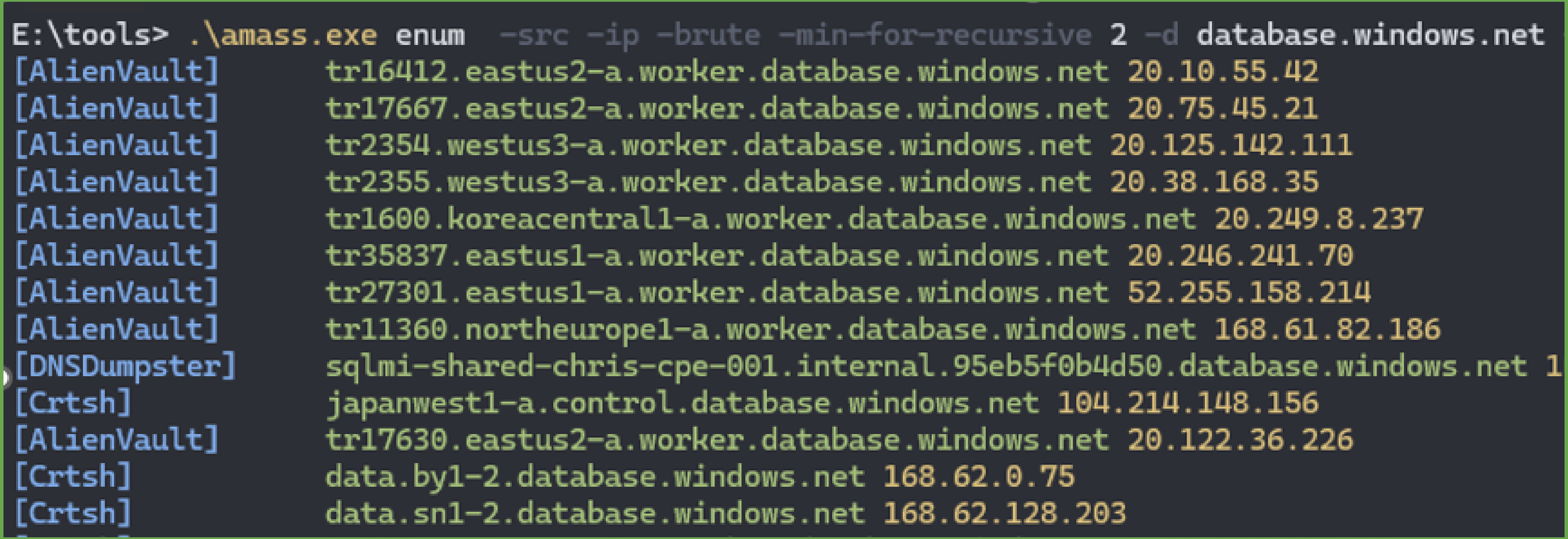
- Azure Passwords
- Azure Databases
- S3 Buckets
- Virtual Machines
- Kubernetes
- Ever growing list

AZURE SQL

- Azure allows other tenants to connect if allowed
- Find credentials in code repositories, Shares, or SharePoint
- Common usernames such as sa are not allowed. sqladmin is however allowed.

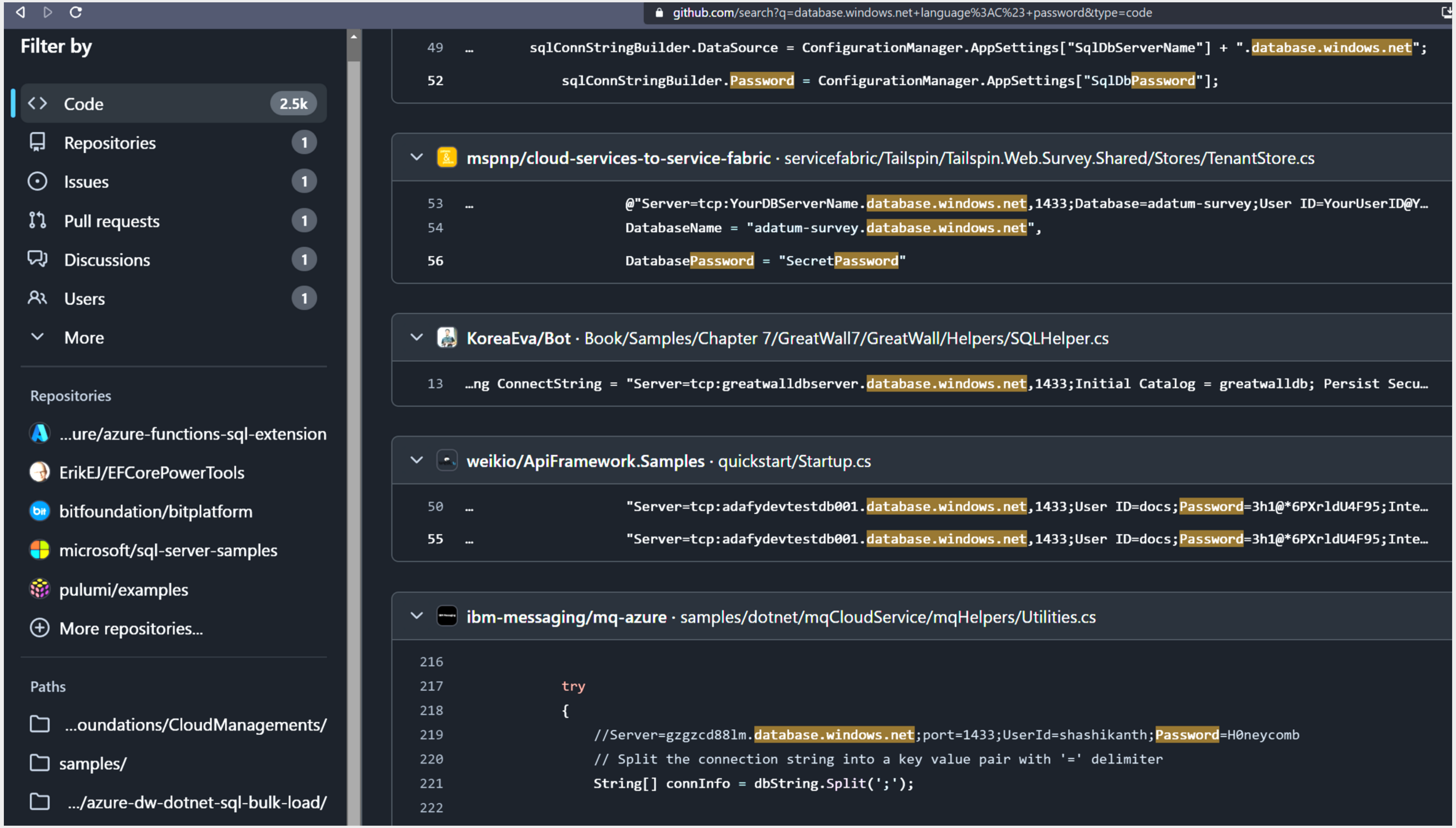
AZURE SQL

FINDING



```
E:\tools> .\amass.exe enum  -src -ip -brute -min-for-recursive 2 -d database.windows.net
[AlienVault]       tr16412.eastus2-a.worker.database.windows.net 20.10.55.42
[AlienVault]       tr17667.eastus2-a.worker.database.windows.net 20.75.45.21
[AlienVault]       tr2354.westus3-a.worker.database.windows.net 20.125.142.111
[AlienVault]       tr2355.westus3-a.worker.database.windows.net 20.38.168.35
[AlienVault]       tr1600.koreacentral1-a.worker.database.windows.net 20.249.8.237
[AlienVault]       tr35837.eastus1-a.worker.database.windows.net 20.246.241.70
[AlienVault]       tr27301.eastus1-a.worker.database.windows.net 52.255.158.214
[AlienVault]       tr11360.northeurope1-a.worker.database.windows.net 168.61.82.186
[DNSDumpster]      sqlmi-shared-chris-cpe-001.internal.95eb5f0b4d50.database.windows.net 1
[Crtsh]            japanwest1-a.control.database.windows.net 104.214.148.156
[AlienVault]       tr17630.eastus2-a.worker.database.windows.net 20.122.36.226
[Crtsh]            data.by1-2.database.windows.net 168.62.0.75
[Crtsh]            data.sn1-2.database.windows.net 168.62.128.203
```

CONNECTION STRINGS



github.com/search?q=database.windows.net+language%3AC%23+password&type=code

```
…       sqlConnStringBuilder.DataSource = ConfigurationManager.AppSettings["SqlDbServerName"] + ".database.windows.net";
            sqlConnStringBuilder.Password = ConfigurationManager.AppSettings["SqlDbPassword"];
```

mspnp/cloud-services-to-service-fabric · servicefabric/Tailspin/Tailspin.Web.Survey.Shared/Stores/TenantStore.cs

```
…                   @"Server=tcp:YourDBServerName.database.windows.net,1433;Database=adatum-survey;User ID=YourUserID@Y…
                    DatabaseName = "adatum-survey.database.windows.net",
                    DatabasePassword = "SecretPassword"
```

KoreaEva/Bot · Book/Samples/Chapter 7/GreatWall7/GreatWall/Helpers/SQLHelper.cs

```
…ng ConnectString = "Server=tcp:greatwalldbserver.database.windows.net,1433;Initial Catalog = greatwalldb; Persist Secu…
```

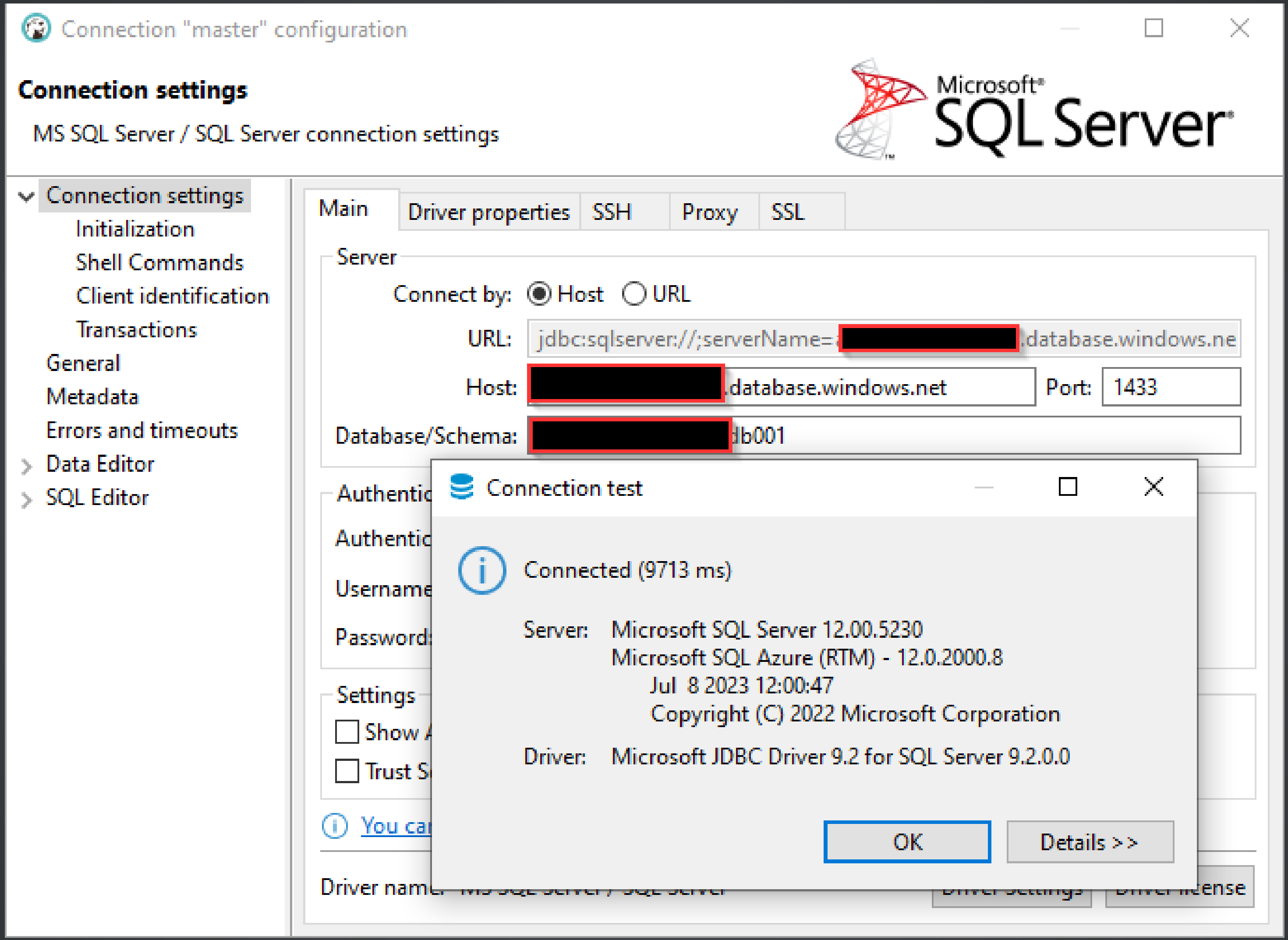
weikio/ApiFramework.Samples · quickstart/Startup.cs

```
…                   "Server=tcp:adafydevtestdb001.database.windows.net,1433;User ID=docs;Password=3h1@*6PXrldU4F95;Inte…
…                   "Server=tcp:adafydevtestdb001.database.windows.net,1433;User ID=docs;Password=3h1@*6PXrldU4F95;Inte…
```

ibm-messaging/mq-azure · samples/dotnet/mqCloudService/mqHelpers/Utilities.cs

```

            try
            {
                //Server=gzgzcd88lm.database.windows.net;port=1433;UserId=shashikanth;Password=H0neycomb
                // Split the connection string into a key value pair with '=' delimiter
                String[] connInfo = dbString.Split(';');

```

CONNECT



Connection "master" configuration

Connection settings

MS SQL Server / SQL Server connection settings

Server

Connect by: ● Host ○ URL

URL: jdbc:sqlserver://;serverName=[redacted].database.windows.ne

Host: [redacted].database.windows.net Port: 1433

Database/Schema: [redacted]db001

Authentic

Authentic

Username

Password:

Settings

□ Show A

□ Trust S

You ca

Driver name: MS SQL Server / SQL Server

Connection test

Connected (9713 ms)

Server: Microsoft SQL Server 12.00.5230
Microsoft SQL Azure (RTM) - 12.0.2000.8
Jul 8 2023 12:00:47
Copyright (C) 2022 Microsoft Corporation

Driver: Microsoft JDBC Driver 9.2 for SQL Server 9.2.0.0

REDHOT TTP

AWS SNS TOPICS

- Amazon Simple Notification Service (SNS)
- Example: SNS topic emails the security team
- Find Vulnerability
- Send spoofed phishing email to the securiy team
  - Use aws cli to send message to topic
- Check SNS policy with cli for "allow *" principal

INITIAL ACCESS

KEY QUESTIONS

- What are your goals?
  - Obtain credentials
  - Obtain sensitive data
  - Obtain a shell
  - Obtain administrator tears

Goals dictate your payload.

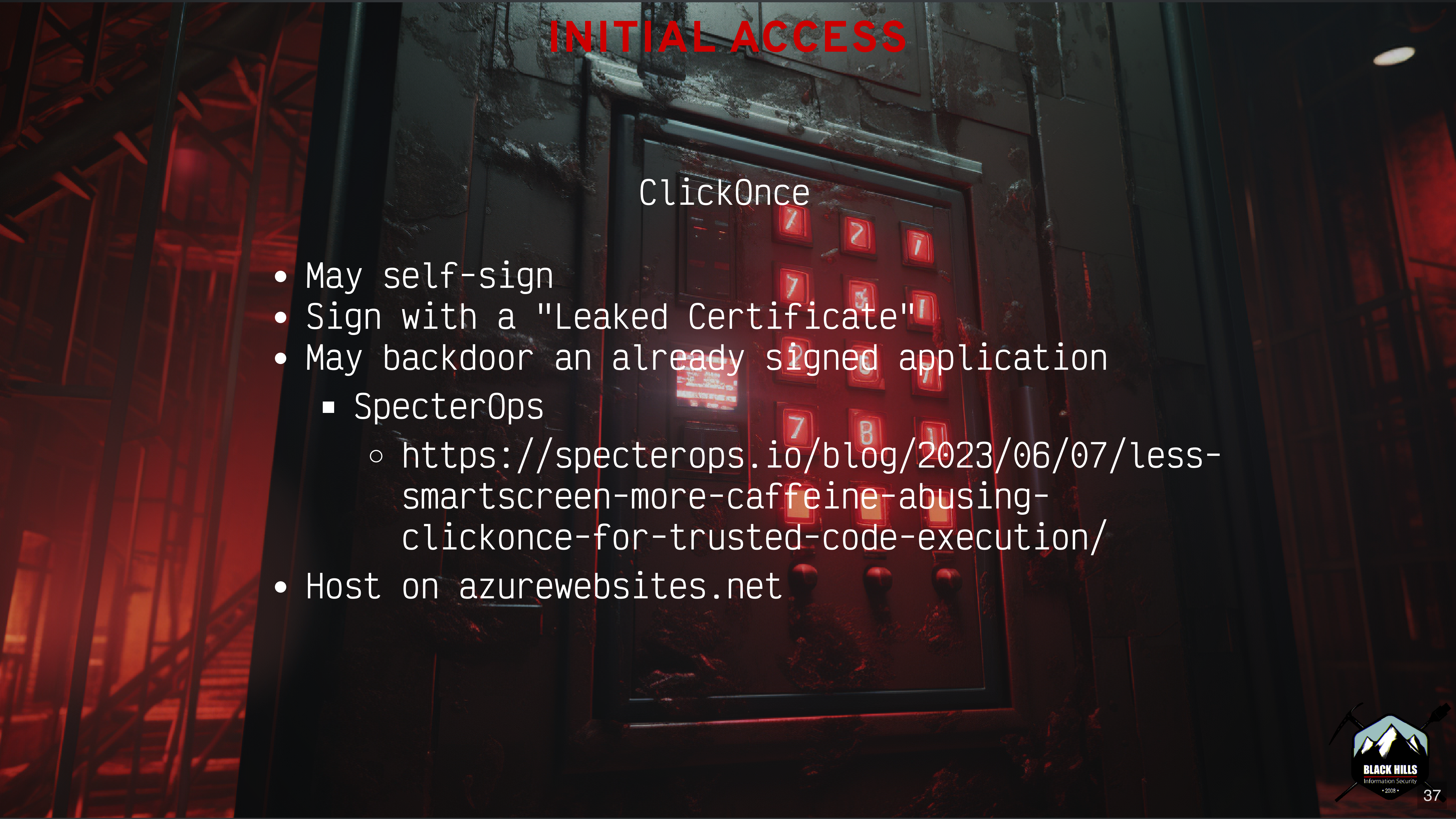
Custom (JWT,Browser Secrets,access keys, files) stealer anyone?

INITIAL ACCESS

TARGETS

- User Workstation
- Web Shell
- SQL Injection
- Windows/RDP
- Linux/SSH

INITIAL ACCESS



ClickOnce

- May self-sign
- Sign with a "Leaked Certificate"
- May backdoor an already signed application
    - SpecterOps
        - https://specterops.io/blog/2023/06/07/less-smartscreen-more-caffeine-abusing-clickonce-for-trusted-code-execution/
- Host on azurewebsites.net

REVERSE SSH TUNNELS

- May not be allowed out over standard SSH
- Try other ports
- Just works better than C2 SOCKS

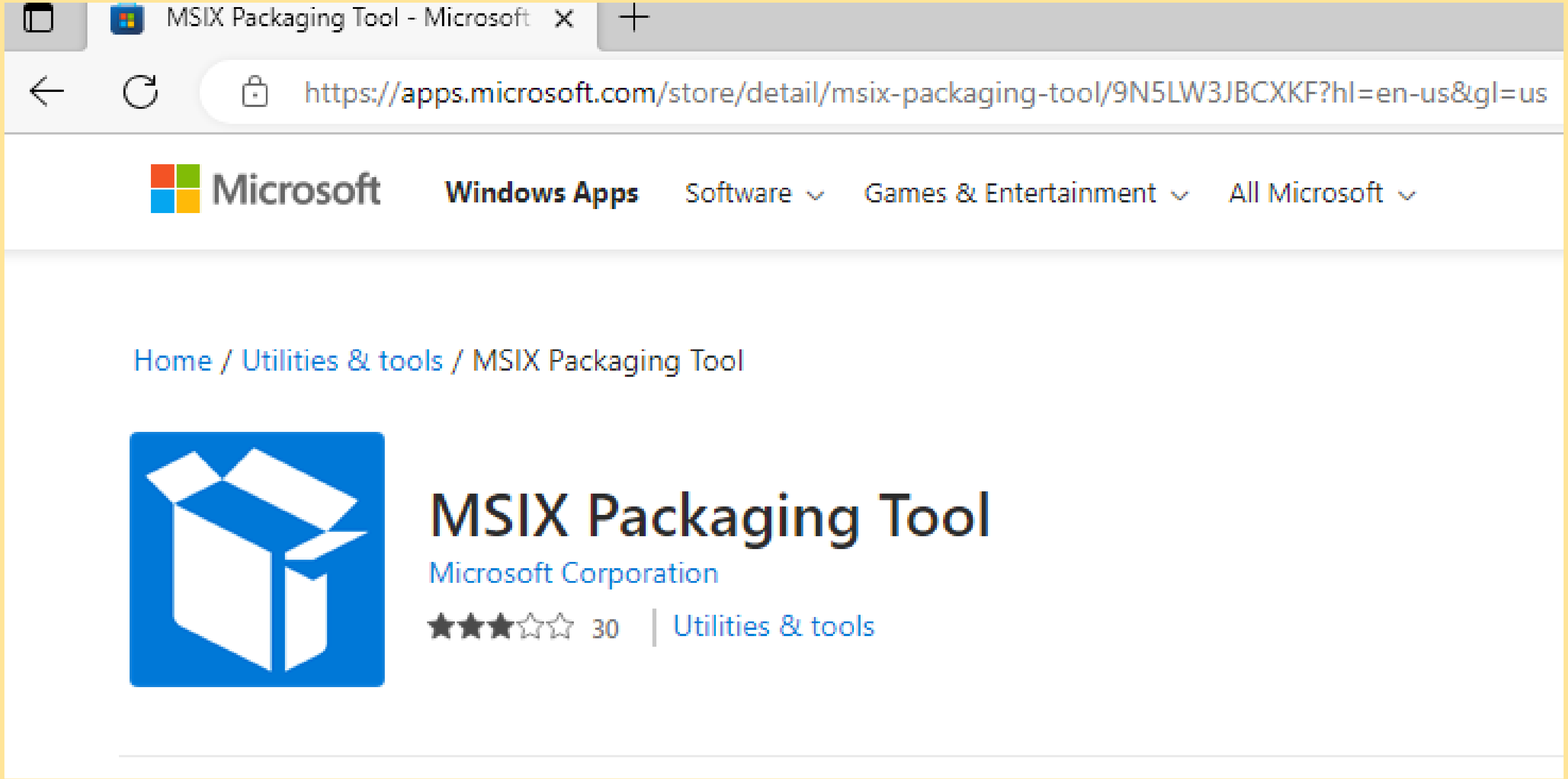
REDHOT TTP

MSIX

LEAKED SIGNATURE + APP DOMAIN INJECTION

- Find Leaked CertificatesCavaet to C# app domain injection:
  - https://tij.me/blog/finding-and-utilising-leaked-code-signing-certificates/
  - It works ;)
- You cannot install an MSIX package if it is not signed
- Cannot execute-assembly/sharpinline in the same agent due to the app domain.

MSIX PACKAGING TOOL



MSIX Packaging Tool - Microsoft

https://apps.microsoft.com/store/detail/msix-packaging-tool/9N5LW3JBCXKF?hl=en-us&gl=us

Home / Utilities & tools / MSIX Packaging Tool

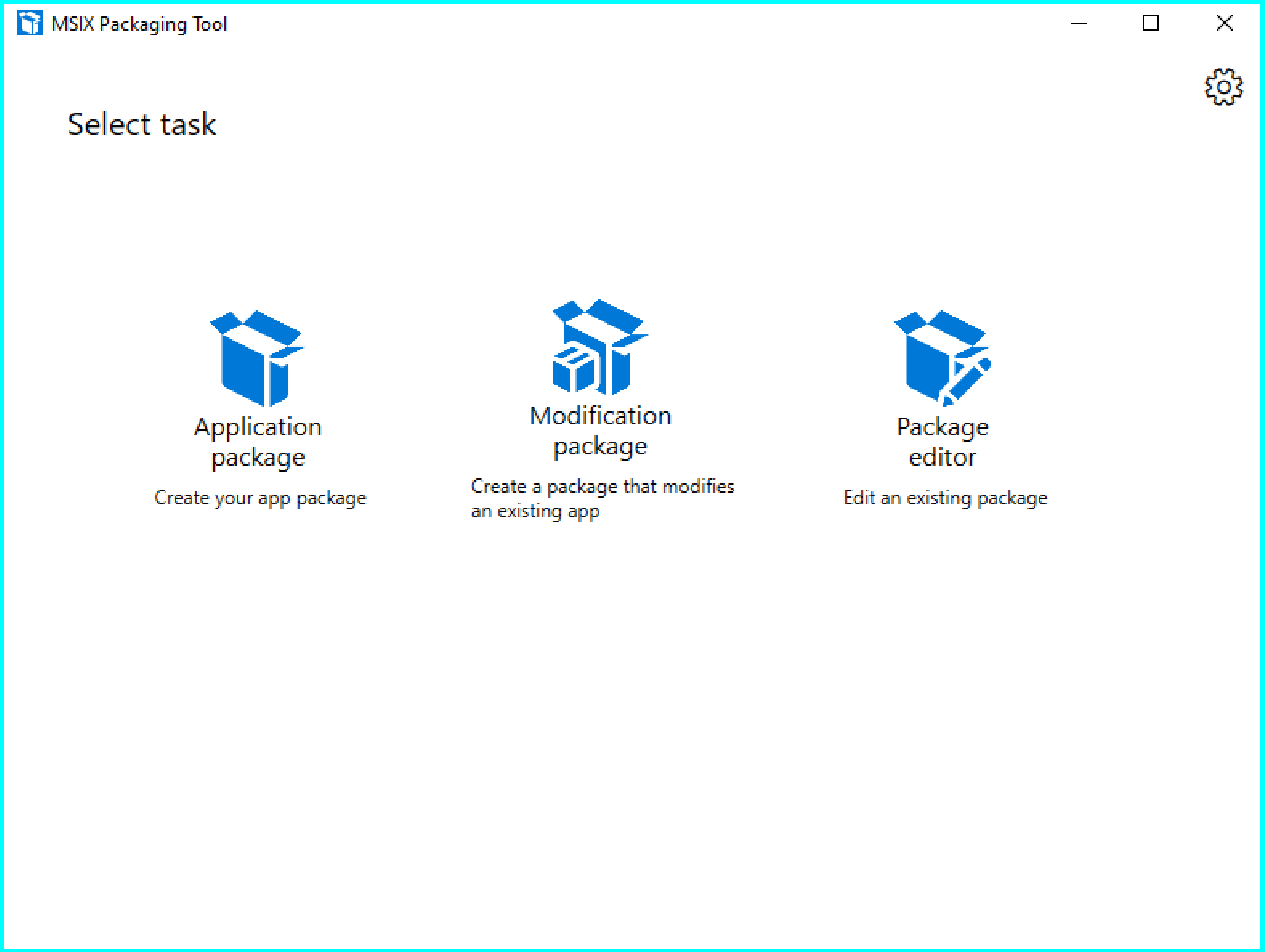
MSIX Packaging Tool

Microsoft Corporation

★★★☆☆ 30 | Utilities & tools

https://learn.microsoft.com/en-us/windows/msix/packaging-tool/create-app-package

MSIX SELECT TASK



Select task

Application package

Create your app package

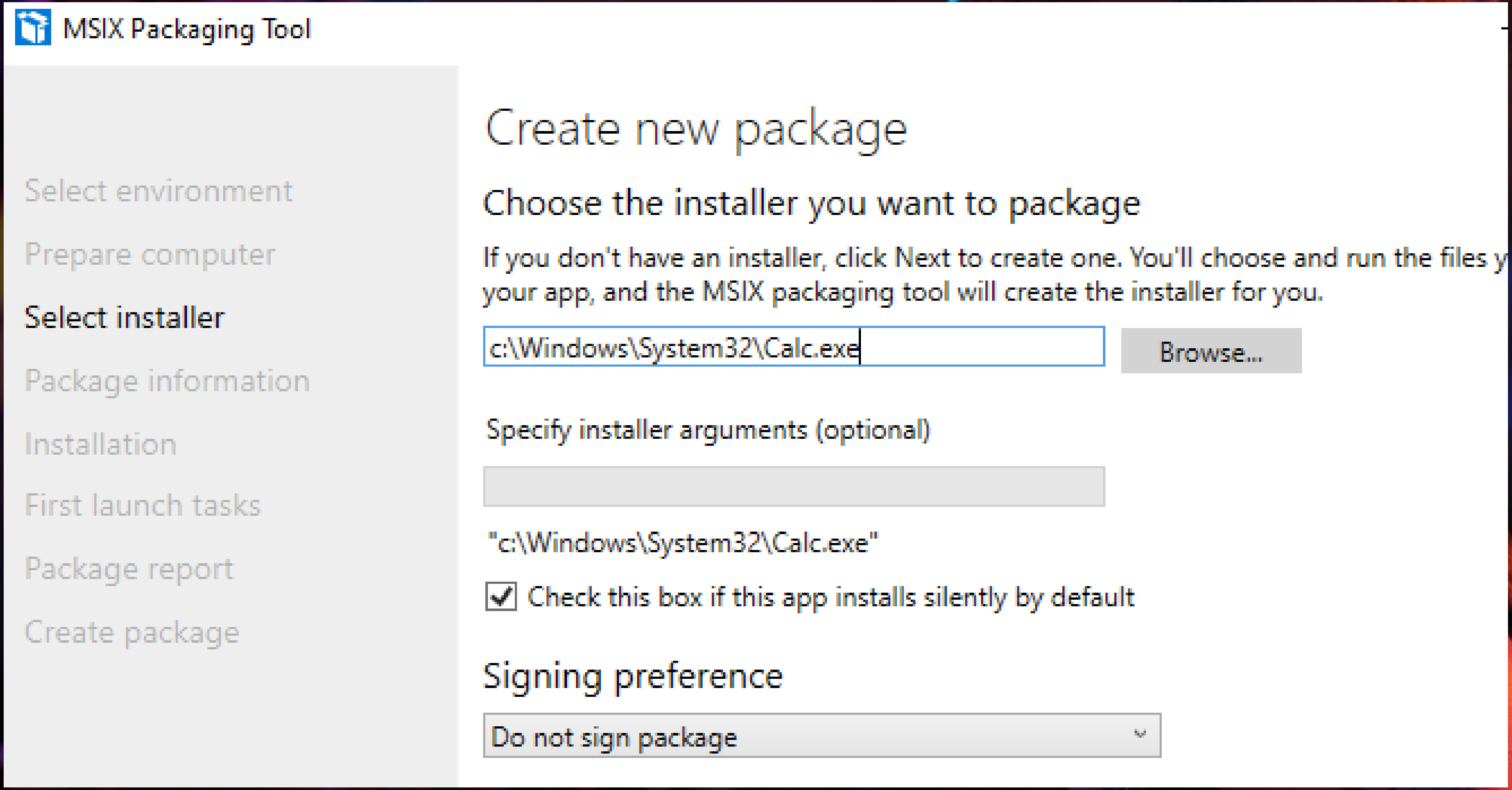
Modification package

Create a package that modifies an existing app

Package editor

Edit an existing package

MSIX CREATE PACKAGE



Create new package

Choose the installer you want to package

If you don't have an installer, click Next to create one. You'll choose and run the files y your app, and the MSIX packaging tool will create the installer for you.

c:\Windows\System32\Calc.exe

Specify installer arguments (optional)

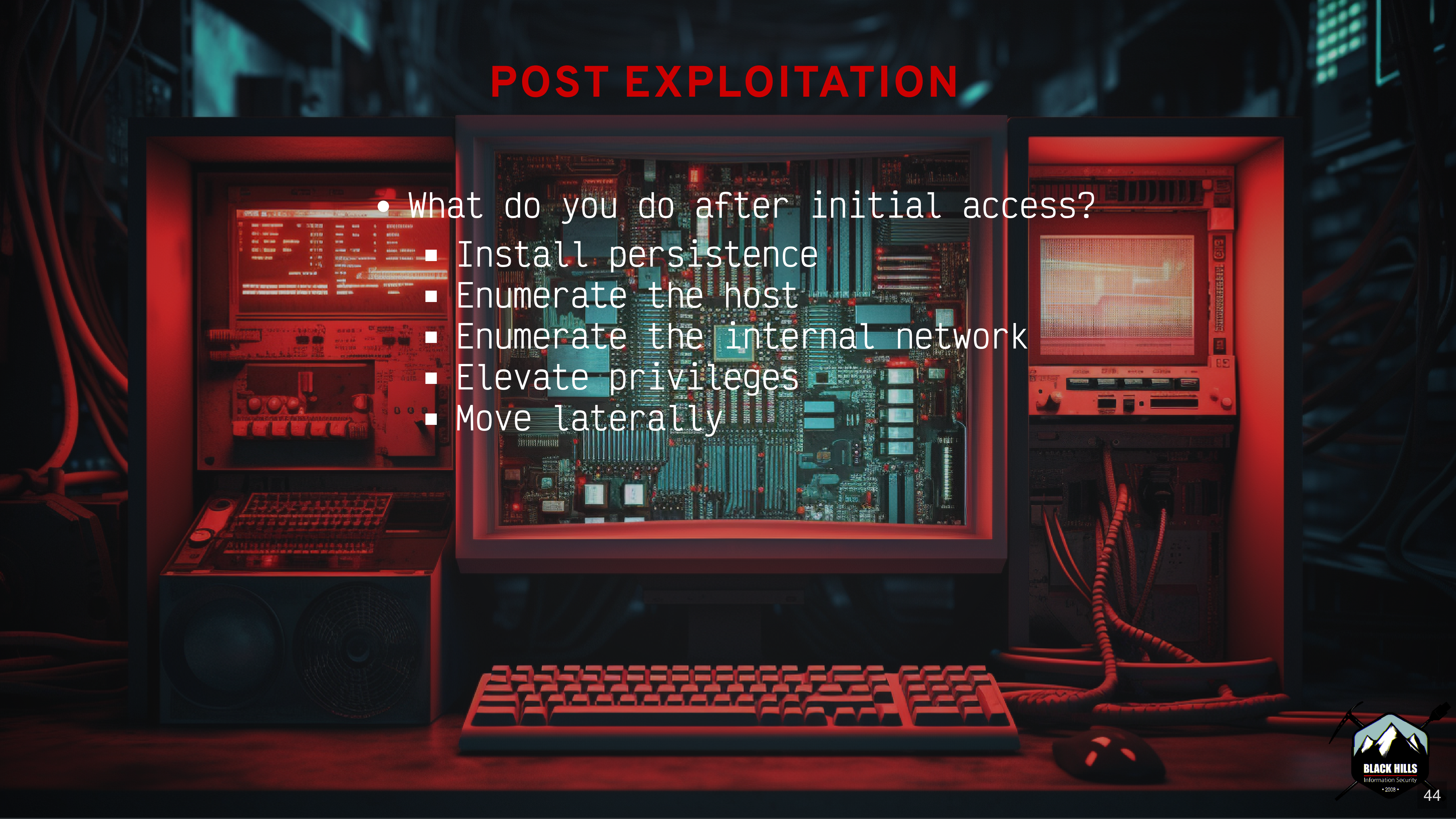
"c:\Windows\System32\Calc.exe"

☑ Check this box if this app installs silently by default

Signing preference

Do not sign package

POST EXPLOITATION



- What do you do after initial access?
  - Install persistence
  - Enumerate the host
  - Enumerate the internal network
  - Elevate privileges
  - Move laterally

ACTIVE DIRECTORY CERTIFICATE SERVICES

- Most cases, user to DA
- Multiple abuse paths
- Easy win
- Certipy - https://github.com/ly4k/Certipy

https://posts.specterops.io/certified-pre-owned-d95910965cd2

TOOL PROXYING

Why run on host/disk when you can tunnel your traffic and enhance your EDR evasion potential?

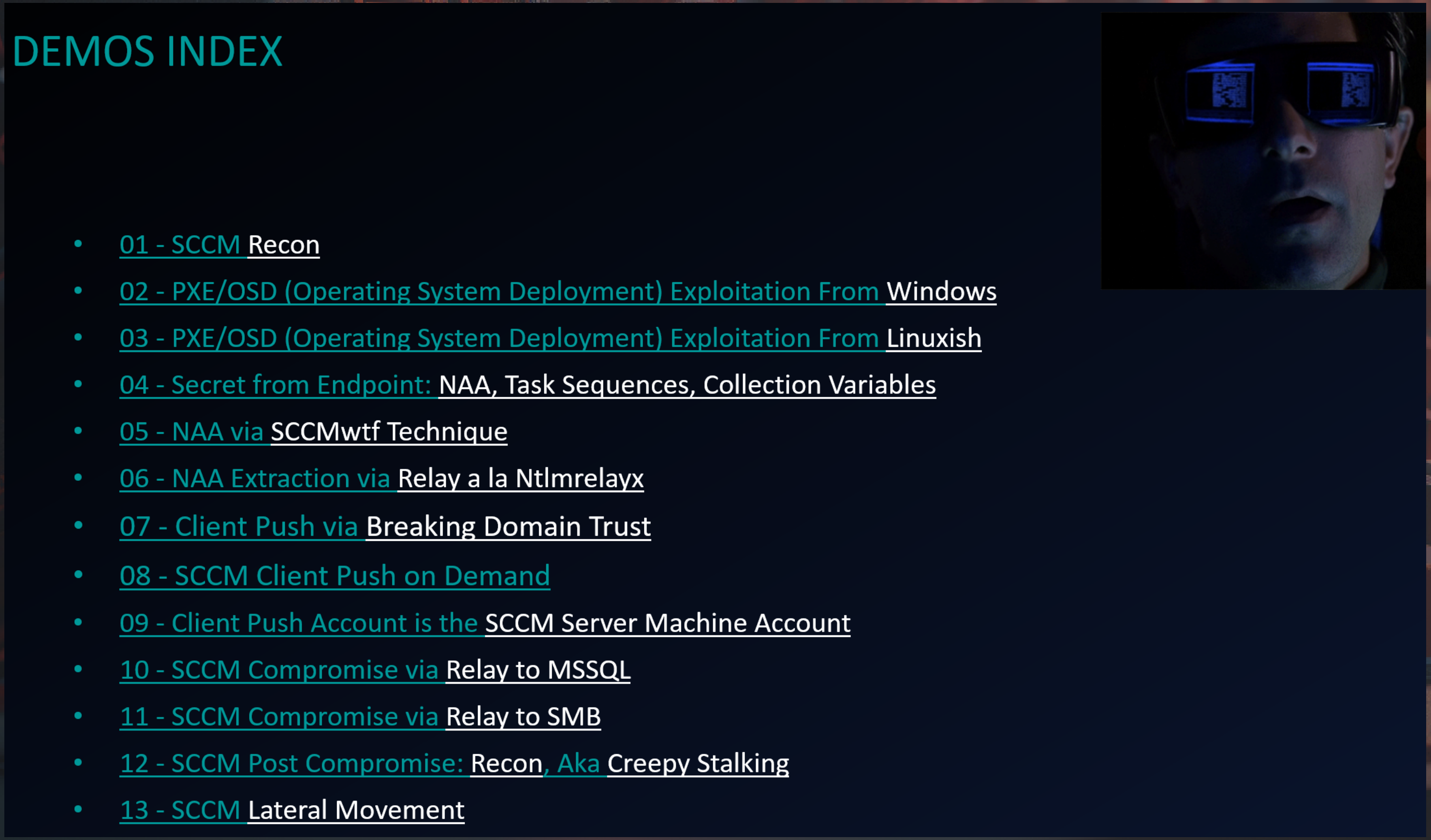
- C2/SSH SOCKS Proxy
- ProxyCap
- Proxifier

REDHOT TTP

POST EXPLOITATION

SCCM/MECM Abuse

https://www.youtube.com/watch?v=W9PC9erm_pI



DEMOS INDEX

- 01 - SCCM Recon
- 02 - PXE/OSD (Operating System Deployment) Exploitation From Windows
- 03 - PXE/OSD (Operating System Deployment) Exploitation From Linuxish
- 04 - Secret from Endpoint: NAA, Task Sequences, Collection Variables
- 05 - NAA via SCCMwtf Technique
- 06 - NAA Extraction via Relay a la Ntlmrelayx
- 07 - Client Push via Breaking Domain Trust
- 08 - SCCM Client Push on Demand
- 09 - Client Push Account is the SCCM Server Machine Account
- 10 - SCCM Compromise via Relay to MSSQL
- 11 - SCCM Compromise via Relay to SMB
- 12 - SCCM Post Compromise: Recon, Aka Creepy Stalking
- 13 - SCCM Lateral Movement

@vendetce

SCCM ABUSE TOOL LIST

- SharpSCCM
  - https://github.com/Mayyhem/SharpSCCM
- SCCMHunter
  - https://github.com/garrettfoster13/sccmhunter
- PXEThief
  - https://github.com/MWR-CyberSec/PXEThief
- SeatBelt
  - https://github.com/GhostPack/Seatbelt

LAB

REDHOT

BE BACK SOON

REDHOT

DEFCON 31