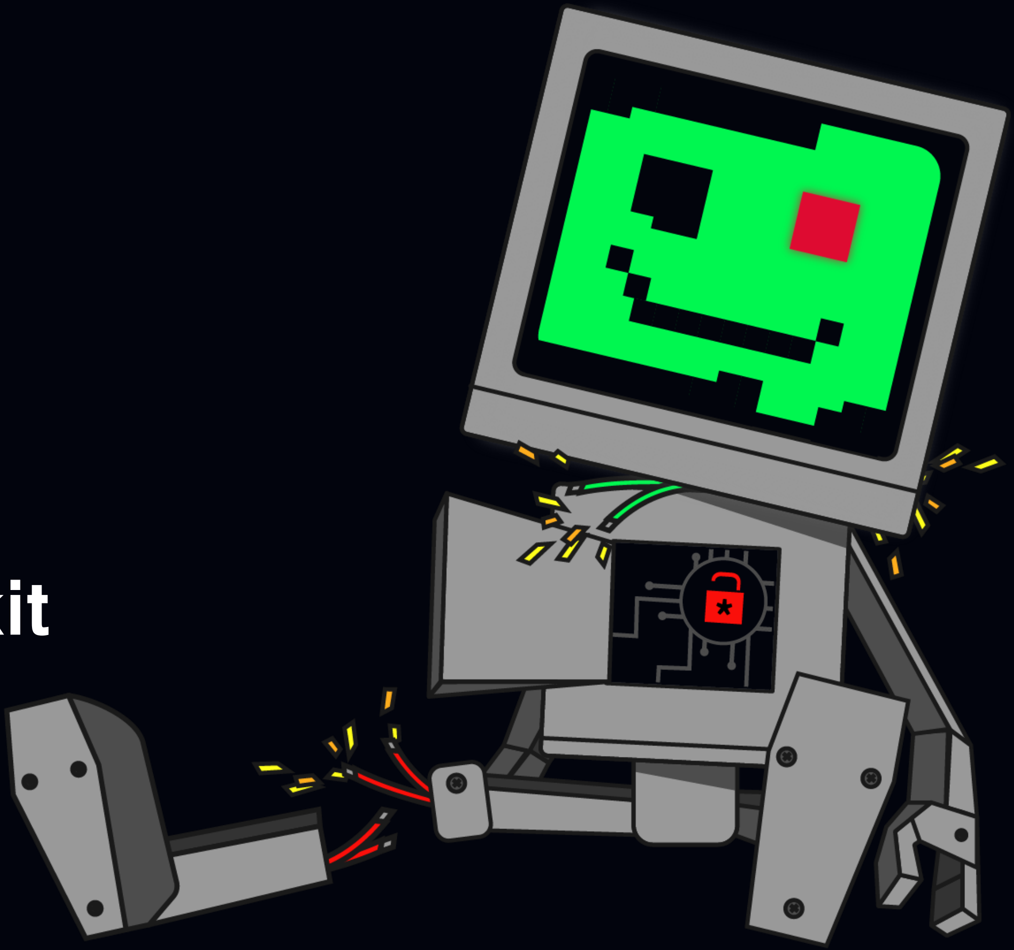
THE H@CK SUMMIT

C:\>

Honeypot vs Red Teaming Toolkit

Piotr Madej

Founder, TrapTech



thehacksummit.com 13-14 października 2022 PGE Narodowy
+ Online

ORGANIZATORZY: AcademicPartners FUNDACJA

DOWÓDZTWO KOMPONENTU WOJSK OBRONY CYBERPRZESTRZENI

Certyfikaty:

CISM

OFFENSIVE security OSCE

CISA

CISSP®

OFFENSIVE security OSCP

CVE:

HITACHI

Hewlett Packard Enterprise

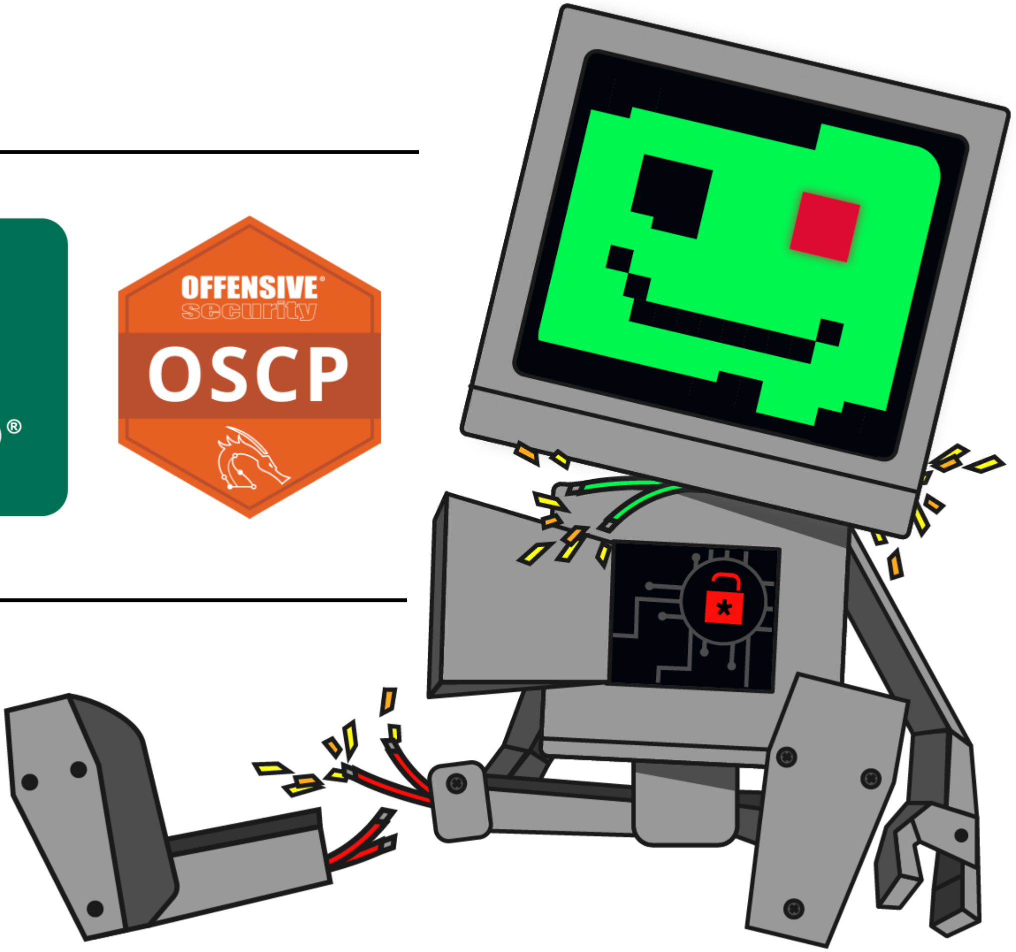
f5®

Microsoft

ORACLE

vmware®

DELL



Deception Technology

Decoy / Przynęta

Cel: zainteresować

- Plik konfiguracyjny
- Wpis w rejestrze
- Event systemowy
- Historia poleceń
- (…)

Przynęta jest łatwa do znalezienia przez atakującego!

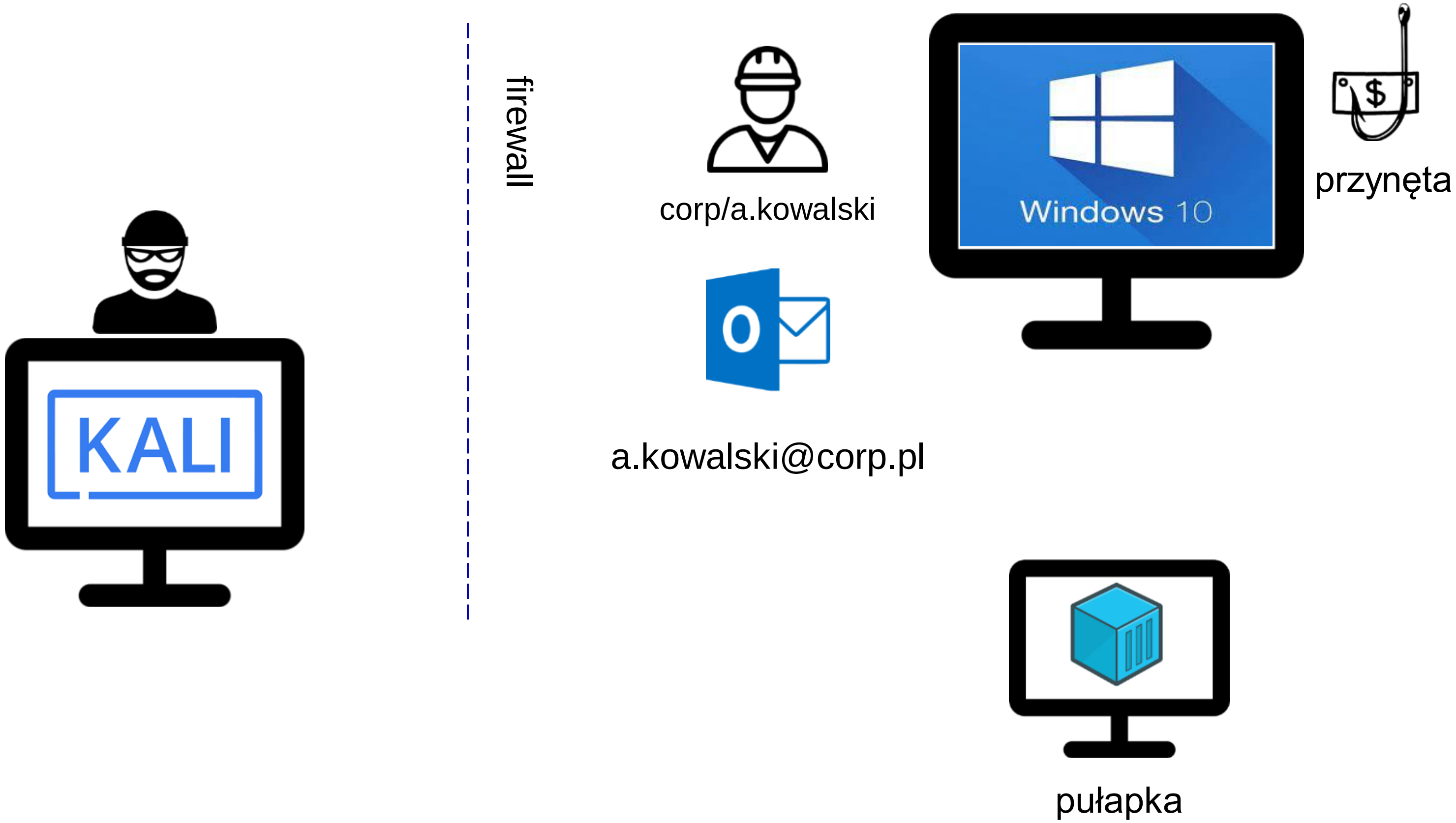
https://www.reddit.com/r/history/comments/m5zhd1/world_war_ii_dummy_tanks/

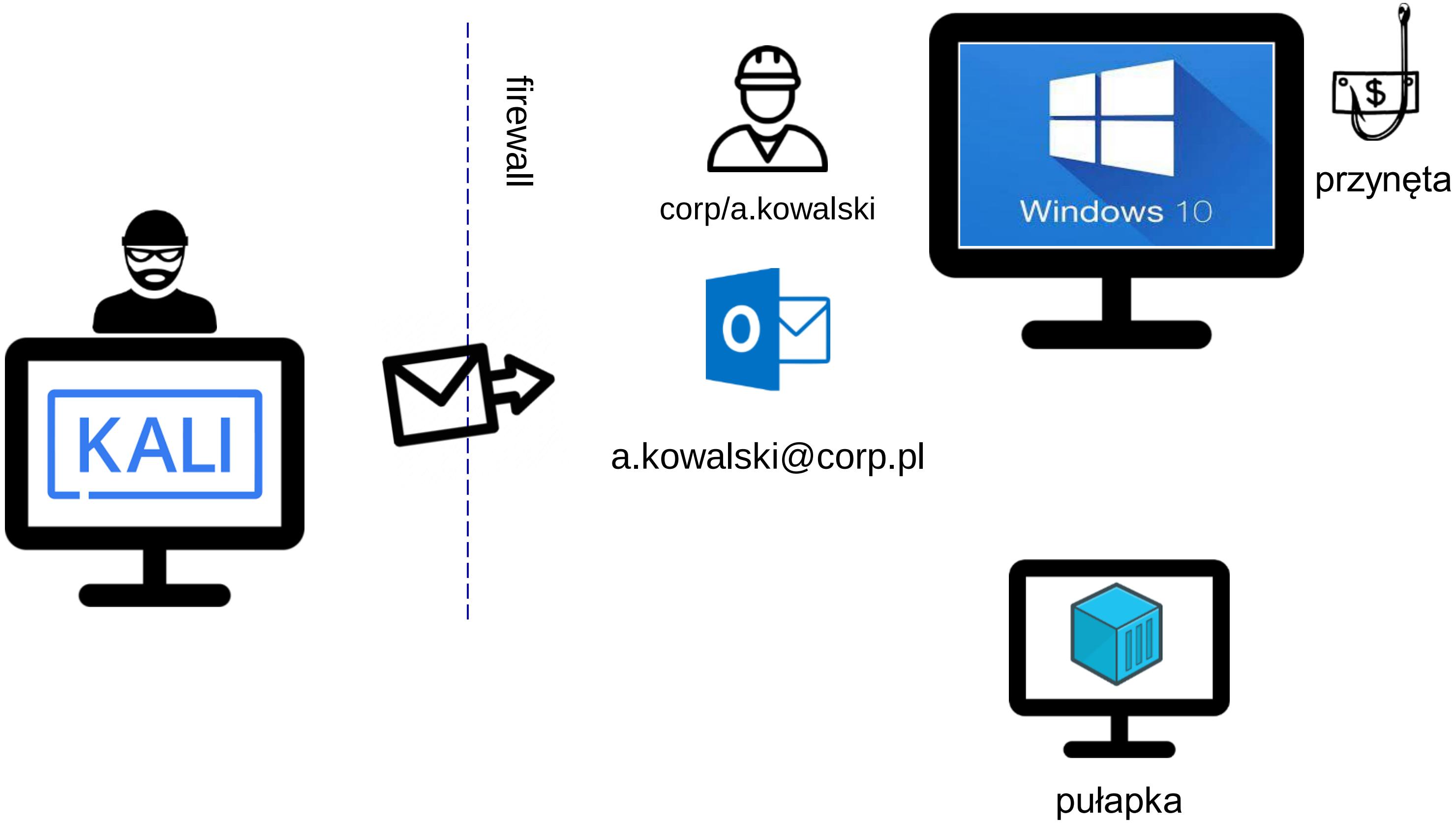
Honeypot / Pułapka

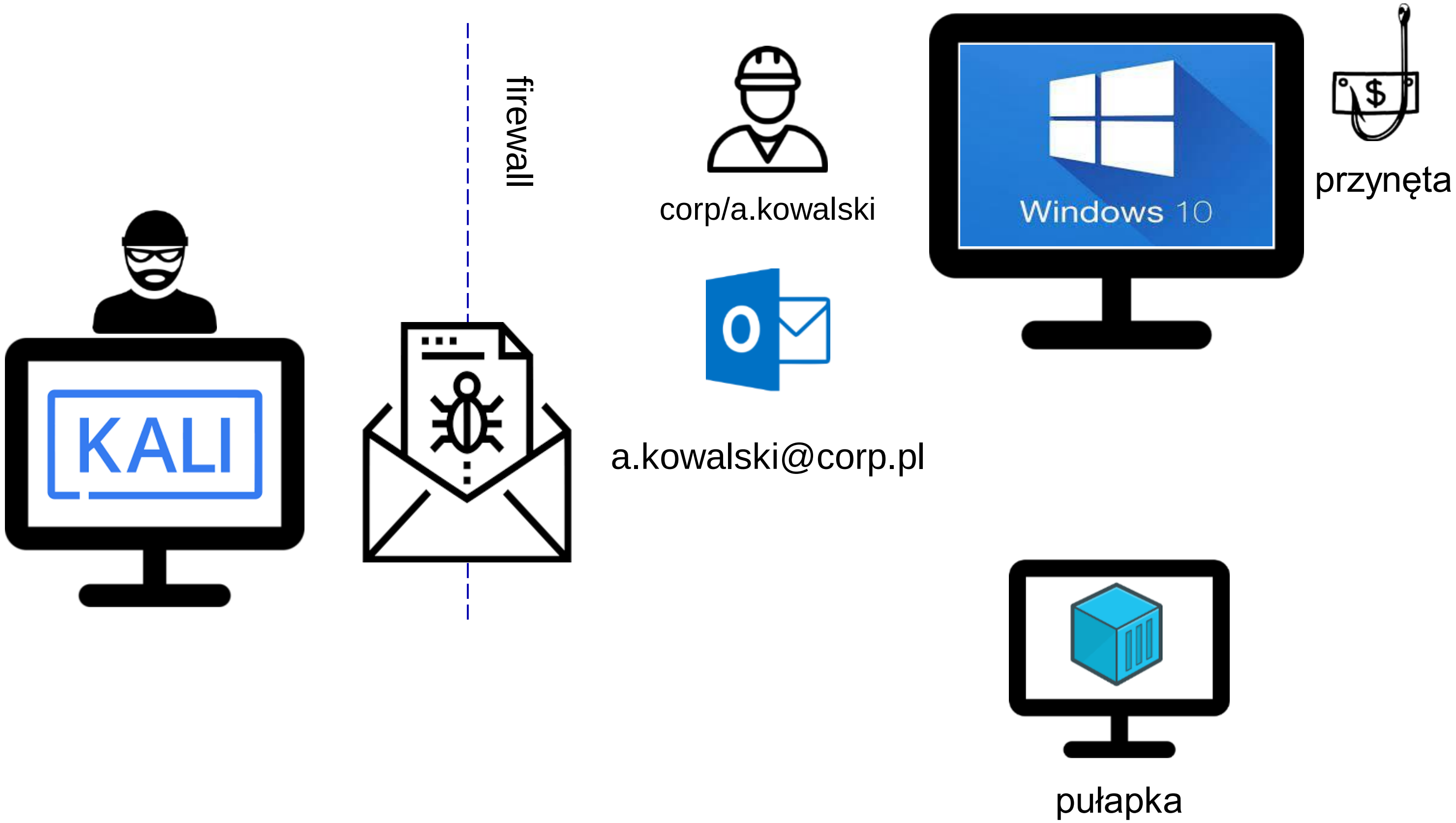
Cel: wykryć

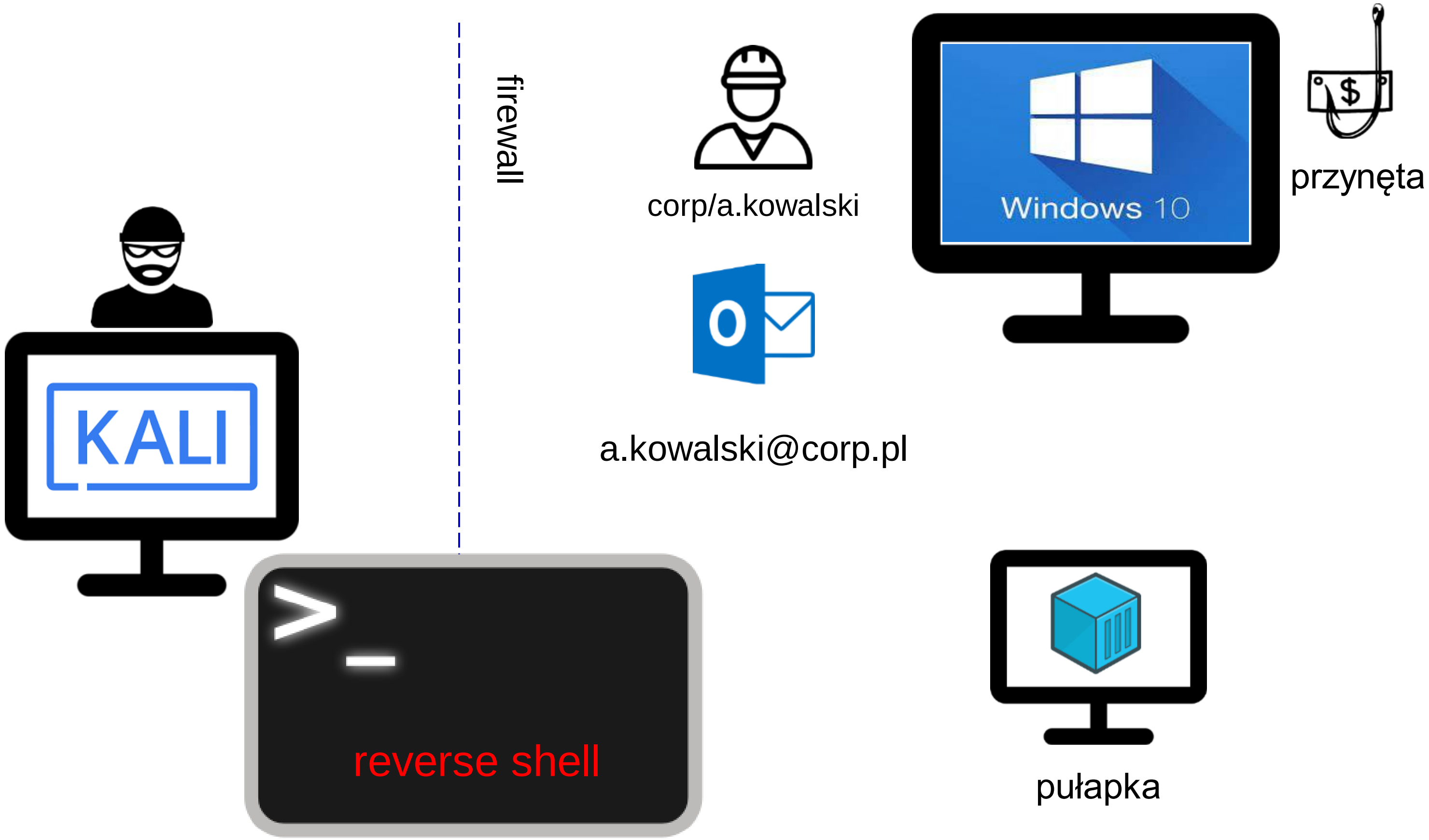
- Aplikacja webowa
- Baza danych
- Zasób sieciowy
- Podatna usługa
- (…)

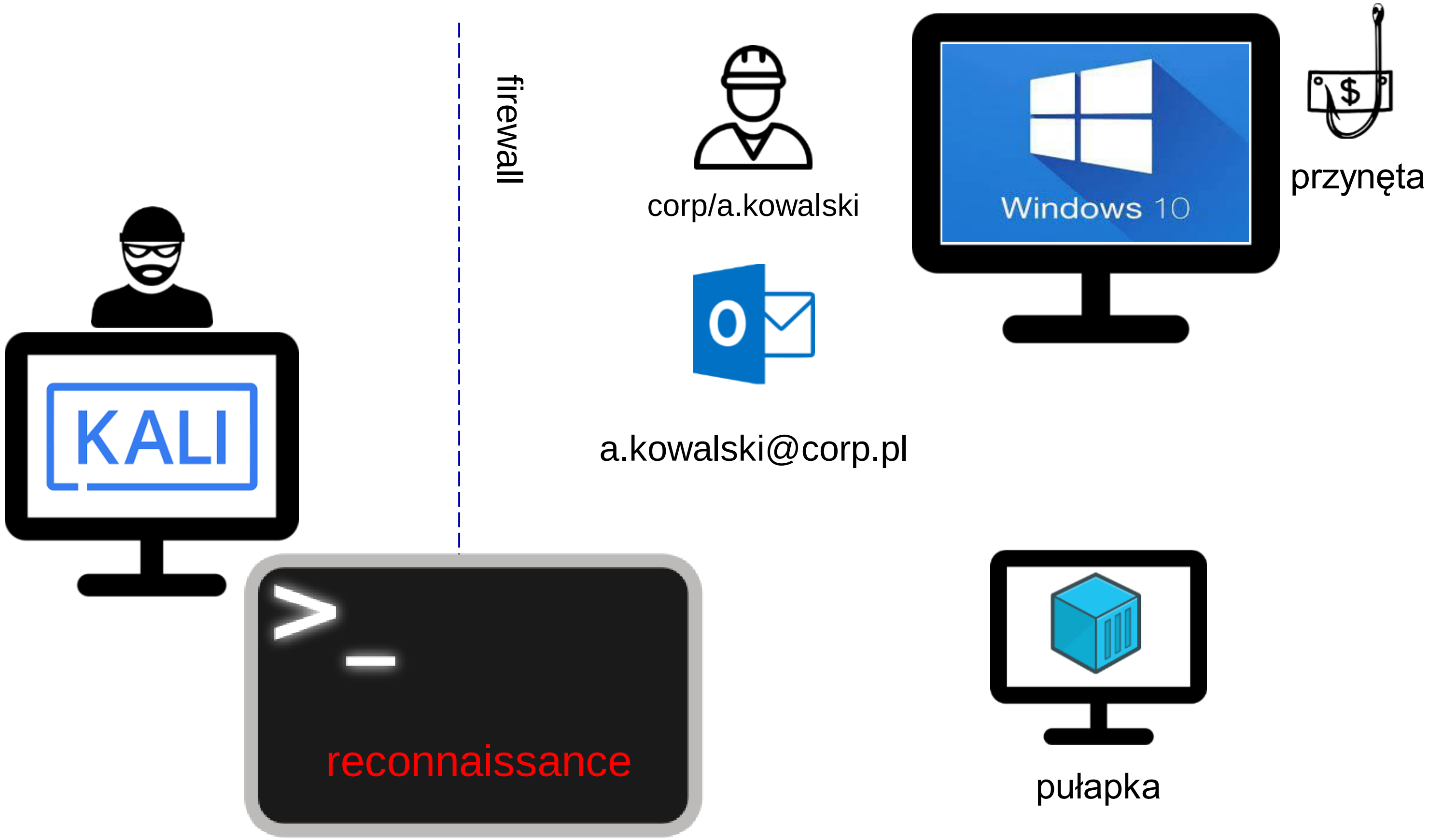
Pułapka nie może okazać się fałszywym zasobem zbyt szybko!


KALI
firewall
corp/a.kowalski
Windows 10
przynęta
a.kowalski@corp.pl
pułapka


firewall
corp/a.kowalski
Windows 10
przynęta
KALI
a.kowalski@corp.pl
pułapka


firewall
corp/a.kowalski
Windows 10
przynęta
KALI
a.kowalski@corp.pl
pułapka


firewall
corp/a.kowalski
Windows 10
przynęta
KALI
a.kowalski@corp.pl
reverse shell
pułapka



firewall

corp/a.kowalski

a.kowalski@corp.pl

przynęta

reconnaissance

pułapka

Find interesting files

```
gci c:\ -Include *pass*.txt, *pass*.xml, *pass*.ini, *pass*.xlsx, *cred*, *vnc*, *.config, *accounts*, -File -Recurse -EA SilentlyContinue
```

Find interesting files

```
gci c:\ -Include *pass*.txt, *pass*.xml, *pass*.ini, *pass*.xlsx, *cred*, *vnc*, *.config, *accounts*, -File -Recurse -EA SilentlyContinue
```

Find config files containing passwords

```
gci c:\ -Include *.txt,*.xml,*.config,*.conf,*.cfg,*.ini -File -Recurse -EA SilentlyContinue | Select-String -Pattern "password"
```

Find interesting files

```
gci c:\ -Include *pass*.txt, *pass*.xml, *pass*.ini, *pass*.xlsx, *cred*, *vnc*, *.config, *accounts*, -File -Recurse -EA SilentlyContinue
```

Find config files containing passwords

```
gci c:\ -Include *.txt,*.xml,*.config,*.conf,*.cfg,*.ini -File -Recurse -EA SilentlyContinue | Select-String -Pattern "password"
```

Find database credentials in configuration files

```
gci c:\ -Include *.config,*.conf,*.xml -File -Recurse -EA SilentlyContinue | Select-String -Pattern "connectionString"
```

Find interesting files

```
gci c:\ -Include *pass*.txt, *pass*.xml, *pass*.ini, *pass*.xlsx, *cred*, *vnc*, *.config, *accounts*, -File -Recurse -EA SilentlyContinue
```

Find config files containing passwords

```
gci c:\ -Include *.txt,*.xml,*.config,*.conf,*.cfg,*.ini -File -Recurse -EA SilentlyContinue | Select-String -Pattern "password"
```

Find database credentials in configuration files

```
gci c:\ -Include *.config,*.conf,*.xml -File -Recurse -EA SilentlyContinue | Select-String -Pattern "connectionString"
```

Locate web server configuration files

```
gci c:\ -Include web.config,applicationHost.config,php.ini,httpd.conf,httpd-xampp.conf,my.ini,my.cnf -File -Recurse -EA SilentlyContinue
```

Find interesting files

```
gci c:\ -Include *pass*.txt, *pass*.xml, *pass*.ini, *pass*.xlsx, *cred*, *vnc*, *.config, *accounts*, -File -Recurse -EA SilentlyContinue
```

Find config files containing passwords

```
gci c:\ -Include *.txt,*.xml,*.config,*.conf,*.cfg,*.ini -File -Recurse -EA SilentlyContinue | Select-String -Pattern "password"
```

Find database credentials in configuration files

```
gci c:\ -Include *.config,*.conf,*.xml -File -Recurse -EA SilentlyContinue | Select-String -Pattern "connectionString"
```

Locate web server configuration files

```
gci c:\ -Include web.config,applicationHost.config,php.ini,httpd.conf,httpd-xampp.conf,my.ini,my.cnf -File -Recurse -EA SilentlyContinue
```

https://github.com/GhostPack/Seatbelt/

```
SELECT System.ItemPathDisplay,System.FileOwner,System.Size,System.DateCreated,System.DateAccessed,System.Search.Autosummary FROM SystemIndex WHERE Contains(*, """"*{0}*"""") AND SCOPE = '{1}' AND (System.FileExtension = '.txt' OR System.FileExtension = '.doc' OR System.FileExtension = '.docx' OR System.FileExtension = '.ppt' OR System.FileExtension = '.pptx' OR System.FileExtension = '.xls' OR System.FileExtension = '.xlsx' OR System.FileExtension = '.ps1' OR System.FileExtension = '.vbs' OR System.FileExtension = '.config' OR System.FileExtension = '.ini')
```

command	Web.config + “password” + “connectionstring”
gci c:\ -Include *pass*.txt, *pass*.xml, *pass*.ini, *pass*.xlsx, *cred*, *vnc*, ***.config**, *accounts*, -File -Recurse -EA SilentlyContinue	OK
gci c:\ -Include *.txt,*.xml,***.config**,*.conf,*.cfg,*.ini -File -Recurse -EA SilentlyContinue | Select-String -Pattern "password"	OK
gci c:\ -Include ***.config**,*.conf,*.xml -File -Recurse -EA SilentlyContinue | Select-String -Pattern "**connectionString**"	OK
gci c:\ -Include **web.config**,applicationHost.config,php.ini,httpd.conf,httpd-xampp.conf,my.ini,my.cnf -File -Recurse -EA SilentlyContinue	OK
(*, """*{0}*""") AND SCOPE = '{1}' AND (System.FileExtension = '.txt' OR System.FileExtension = '.doc' OR System.FileExtension = '.docx' OR System.FileExtension = '.ppt' OR System.FileExtension = '.pptx' OR System.FileExtension = '.xls' OR System.FileExtension = '.xlsx' OR System.FileExtension = '.ps1' OR System.FileExtension = '.vbs' OR System.FileExtension = '**'.config**' OR System.FileExtension = '.ini')	OK

https://github.com/PowerShellMafia/PowerSploit/

Get-GPPPassword

```
# discover any locally cached GPP .xml files
Write-Verbose '[Get-GPPPassword] Searching local host for any cached GPP files'
$XMLFiles += Get-ChildItem -Path $AllUsers -Recurse -Include 'Groups.xml','Services.xml','Scheduledtasks.xml','DataSources.xml','Printers.xml','Drives.xml' -Force -ErrorAction SilentlyContinue
```

```
# discover potential domain GPP files containing passwords, not complaining in case of denied access to a directory
Write-Verbose "[Get-GPPPassword] Searching \\$Domain\SYSVOL\*\Policies. This could take a while."
$DomainXMLFiles = Get-ChildItem -Force -Path "\\$Domain\SYSVOL\*\Policies" -Recurse -ErrorAction SilentlyContinue -Include @('Groups.xml','Services.xml','Scheduledtasks.xml','DataSources.xml','Printers.xml','Drives.xml')
```

https://github.com/PowerShellMafia/PowerSploit/

Get-GPPAutologon

```
 #discover potential registry.xml containing autologon passwords
 Write-Verbose 'Searching the DC. This could take a while.'
 $XMlFiles = Get-ChildItem -Path "\\$Env:USERDNSDOMAIN\SYSVOL" -Recurse -ErrorAction SilentlyContinue -Include
'Registry.xml’
```

https://github.com/PowerShellMafia/PowerSploit/

Recon Find-InterestingFile

*Default value: @('*password*', '*sensitive*', '*admin*', '*login*', '*secret*', '**unattend*.xml**', '*.vmdk', '*creds*', '*credential*', '*.config')*

https://github.com/PowerShellMafia/PowerSploit/

Get-VaultCredential

```
([Guid] '2F1A6504-0641-44CF-8BB5-3612D865F2E5') = 'Windows Secure Note'
([Guid] '3CCD5499-87A8-4B10-A215-608888DD3B55') = 'Windows Web Password Credential'
([Guid] '154E23D0-C644-4E6F-8CE6-5069272F999F') = 'Windows Credential Picker Protector'
([Guid] '4BF4C442-9B8A-41A0-B380-DD4A704DDB28') = 'Web Credentials'
([Guid] '77BC582B-F0A6-4E15-4E80-61736B6F3B29') = 'Windows Credentials'
([Guid] 'E69D7838-91B5-4FC9-89D5-230D4D4CC2BC') = 'Windows Domain Certificate Credential'
([Guid] '3E0E35BE-1B77-43E7-B873-AED901B6275B') = 'Windows Domain Password Credential'
([Guid] '3C886FF3-2669-4AA2-A8FB-3F6759A77548') = 'Windows Extended Credential'
```

https://github.com/GhostPack/Seatbelt

CloudCredentials

```
string[] azureCredLocations = {     $"{dir}\\.azure\\azureProfile.json",
$"{dir}\\.azure\\TokenCache.dat",
$"{dir}\\.azure\\AzureRMContext.json",
$"{dir}\\AppData\\Roaming\\Windows Azure Powershell\\TokenCache.dat",
$"{dir}\\AppData\\Roaming\\Windows Azure Powershell\\AzureRMContext.json" };

string[] googleCredLocations = {    $"{dir}\\AppData\\Roaming\\gcloud\\credentials.db",
$"{dir}\\AppData\\Roaming\\gcloud\\legacy_credentials",
$"{dir}\\AppData\\Roaming\\gcloud\\access_tokens.db"};
```

https://github.com/GhostPack/Seatbelt

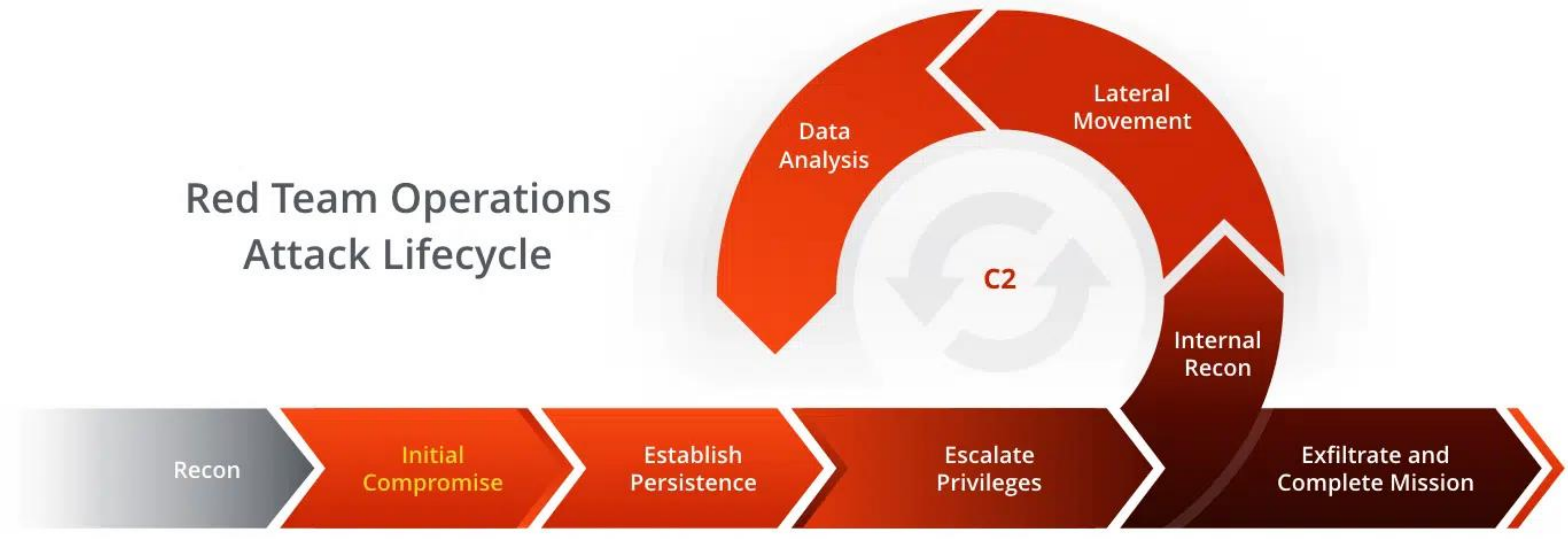
FileZilla

```
if (dir.EndsWith("Public") || dir.EndsWith("Default") || dir.EndsWith("Default User") || dir.EndsWith("All Users"))
continue;

var parts = dir.Split('\\');
var userName = parts[parts.Length - 1];
var configs = new List<FileZillaConfig>();

string[] paths = { $"{dir}\\AppData\\Roaming\\FileZilla\\sitemanager.xml",
$"{dir}\\AppData\\Roaming\\FileZilla\\recentservers.xml" };
```

https://github.com/GhostPack/Seatbelt

PowerShellHistory

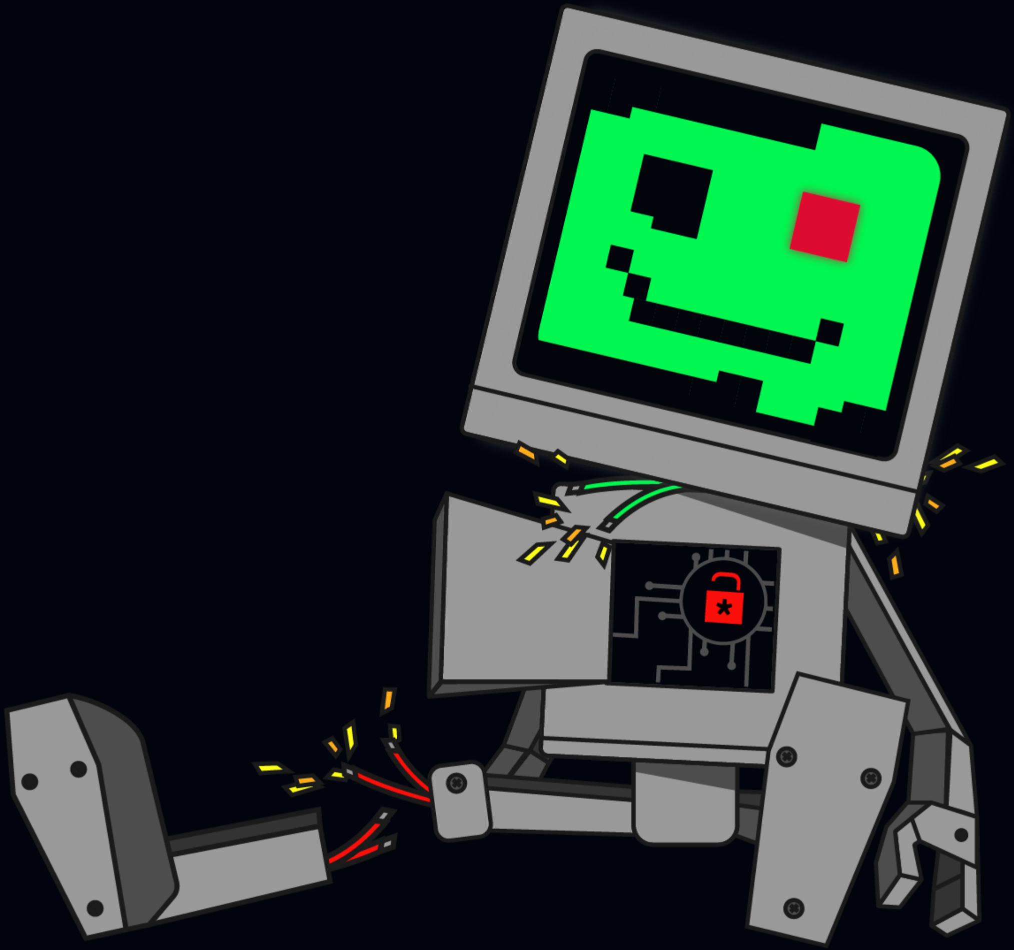
```
if (dir.EndsWith("Public") || dir.EndsWith("Default") || dir.EndsWith("Default User") ||
dir.EndsWith("All Users"))
{
continue;
}

var consoleHistoryPath = $"{dir}\\AppData\\Roaming\\Microsoft\\Windows\\PowerShell\\PSReadline\\ConsoleHost_history.txt";
```



Red Team Operations Attack Lifecycle

https://renatoborbolla.medium.com/red-teaming-adversary-simulation-toolkit-da89b20cb5ea

THE H@CK SUMMIT



Dziękujemy za uwagę!

Zapraszamy do zadawania pytań oraz oceny wystąpienia.

thehacksummit.com 13-14 października 2022 PGE Narodowy
+ Online

ORGANIZATORZY: AcademicPartners FUNDACJA

DOWÓDZTWO KOMPONENTU WOJSK OBRONY CYBERPRZESTRZENI