Pacu Quick Start Guide

Christophe • August 27, 2023

Alright, now that you've downloaded Pacu and set up our credentials, let's run through some simple commands that we have access to.

Commands

`list` or `ls` will list the available modules that we have access to. Since we've not added any custom modules, these are all of the included modules that come with Pacu out of the box.

```
> list

[Category: ESCALATE]

  cfn__resource_injection
  iam__privesc_scan

[Category: EXFIL]

  ebs__download_snapshots
  rds__explore_snapshots
  s3__download_bucket

[Category: ENUM]

  acm__enum
  apigateway__enum
  aws__enum_account
  aws__enum_spend
  cloudformation__download_data
  codebuild__enum
  dynamodb__enum
  ebs__enum_volumes_snapshots
  ec2__check_termination_protection
  ec2__download_userdata
  ec2__enum
  ecr__enum
  ecs__enum
  ecs__enum_task_def
  eks__enum
  enum__secrets
  glue__enum
  guardduty__list_accounts
  guardduty__list_findings
  iam__bruteforce_permissions
  iam__detect_honeytokens
  iam__enum_action_query
  iam__enum_permissions
  iam__enum_users_roles_policies_groups
  iam__get_credential_report
  inspector__get_reports
  lambda__enum
  lightsail__enum
  organizations__enum
  rds__enum
  rds__enum_snapshots
  route53__enum
  systemsmanager__download_parameters
  transfer_family__enum

[Category: PERSIST]

  ec2__backdoor_ec2_sec_groups
  iam__backdoor_assume_role
  iam__backdoor_users_keys
  iam__backdoor_users_password
  lambda__backdoor_new_roles
  lambda__backdoor_new_sec_groups
  lambda__backdoor_new_users

[Category: EXPLOIT]

  api_gateway__create_api_keys
  ebs__explore_snapshots
  ec2__startup_shell_script
  ecs__backdoor_task_def
  lightsail__download_ssh_keys
  lightsail__generate_ssh_keys
  lightsail__generate_temp_access
  systemsmanager__rce_ec2

[Category: RECON_UNAUTH]

  iam__enum_roles
  iam__enum_users

[Category: EVADE]

  cloudtrail__download_event_history
  cloudwatch__download_logs
  detection__disruption
  detection__enum_services
  elb__enum_logging
  guardduty__whitelist_ip
  waf__enum

[Category: LATERAL_MOVE]

  cloudtrail__csv_injection
  organizations__assume_role
  vpc__enum_lateral_movement
```

As you can see, we have modules for:

- ESCALATE (privileges)
- EXFIL(trate)
- ENUM(erate)
- PERSIST
- EXPLOIT
- RECON_UNAUTH(orized)
- EVADE
- LATERAL_MOVE(ment)

Feel free to take your time going through the available modules for each of these categories if you'd like, and by the way, you can use:

`help module_name` to return the help information for that specific module.

For example, if you type:

```
> help waf__enum
```

You'll get all of this information:

```
waf__enum written by Alexander Morgenstern alexander.morgenstern@rhinosecuritylabs.com.

usage: pacu [--regions REGIONS] [--global-region]

This module will enumerate WAF. The enumerated data includes the rule groups, rules and
matching sets for those rules. Global WAF settings are enumerated the same as each
individually-configured region, but they are stored separately in the Pacu database.

options:
  --regions REGIONS  One or more (comma separated) AWS regions in the format "us-east-1".
                     Defaults to all available regions.
  --global-region    Flag to enumerate WAF information for all regions.
```

Which tells you how to use the module, what it will do, and what options you can use with this module.

To actually run the module, you would type:

`run module_name` or,

`run module_name --regions eu-west-1,us-west-1` to run the module against specific regions

I'm not going to run any modules just yet because that's what we'll be doing a lot of throughout the rest of the course.

Instead, let's finally mention and take a quick look at the help menu before moving on:

```
> help
```

Some of the most helpful commands I'll mention are:

- `search [cat[egory]] <search term>` → to search for module either by category or just by search term
- `whoami` → which is super helpful especially when you're switching between users or credentials
- `data` → which lets you display either all data you've stored for this active session or `data <service> [<sub-service>]` to display data related to an AWS service that you've enumerated
- `set_regions <region> [<region>...]` → to set one or more default regions for the current session
- `assume_role <role arn>` → to assume a role's permissions
- `aws <command>` → to run an AWS CLI command directly. I don't typically do this because it can get really messy with keeping track of which credentials you're using, etc... so I'll typically opt to using separate terminals for Pacu and for the CLI, but you can do it if you want to

Alright, that's it for this quick start guide. Let's complete this lesson and let's get started with our first scenario!