Rhynorater Update README.md ae8cb41 · 6 years ago 23 Commits

Dockerfile	Add dockerfile	6 years ago
README.md	Update README.md	6 years ago
exampleInput.txt	Adding the code.	6 years ago
exampleOutput.csv	Adding the code.	6 years ago
exampleOutput.json	Adding the code.	6 years ago
exampleOutput.txt	Test before your commit...	6 years ago
requirements.txt	Add requirements.txt	6 years ago
sshUsernameEnumExploit.py	Added simple test to check if target is ...	6 years ago

README

CVE-2018-15473-Exploit

On August 15th, 2018, the following advisory was posted on the OSS-Security list:
http://openwall.com/lists/oss-security/2018/08/15/5

The ShellIntel team decided to invest some time and write an exploit for this vulnerability. The exploit below has the following features:

- Threading - default 5
  - If more than 10 are used, often the OpenSSH service gets overwhelmed and causes retries
- Single username evaluation via `username` parameter
- Multiple username evaluation via `userList` parameter
- Multiple username evaluation file output via `outputFile` parameter
- Multiple output formats (list, json, csv) via `outputFormat` parameter

An example username input file is given in `exampleInput.txt`
An example results output file in List format is given in `exampleOutput.txt`
An example results output file in JSON format is given in `exampleOutput.json`
An example results output file in CSV format is given in `exampleOutput.csv`

Install the dependencies by running `pip install -r requirements.txt`

=======

Build the image:

docker build -t cve-2018-15473 .

Run the exploit:

docker run cve-2018-15473 -h

Delete containers and image:

docker ps -a | awk '$2 == "cve-2018-15473" {print $1}' | xargs docker rm docker rmi cve-2018-15473