

Name: Cristian Barreno

## Encoding vs Hashing vs Encryption

### EXERCISE 2 - Hashing

#### Task 1

```
echo hello world > file1.txt
```

```
echo hello world > file2.txt
```

A terminal window with a black background and green text. The prompt is 'lynx@lynx: ~'. The user enters 'echo hello world > file1.txt', then 'echo hello world > file2.txt', then 'md5sum file1.txt', and finally 'md5sum file2.txt'. The output for both 'md5sum' commands is '6f5902ac237024bdd0c176cb93063dc4 file1.txt' and '6f5902ac237024bdd0c176cb93063dc4 file2.txt' respectively.

```
lynx@lynx: ~  
lynx@lynx:~$ echo hello world > file1.txt  
lynx@lynx:~$ echo hello world > file2.txt  
lynx@lynx:~$ md5sum file1.txt  
6f5902ac237024bdd0c176cb93063dc4 file1.txt  
lynx@lynx:~$ md5sum file2.txt  
6f5902ac237024bdd0c176cb93063dc4 file2.txt  
lynx@lynx:~$
```

Please note that the MD5 hash of the outputs are identical to each other.

That means when you created the files, they were identical, so were their hashes.

This proves the deterministic nature of using the same hash function, which in this case was md5.

#### Task 2

```
echo hello world! > file3.txt
```

```
md5sum file3.txt
```

A terminal window with a black background and green text. The prompt is 'lynx@lynx: ~'. The user enters 'echo hello world! > file3.txt', then 'md5sum file3.txt'. The output is 'c897d1410af8f2c74fba11b1db511e9e file3.txt'.

```
lynx@lynx: ~  
lynx@lynx:~$ echo hello world! > file3.txt  
lynx@lynx:~$ md5sum file3.txt  
c897d1410af8f2c74fba11b1db511e9e file3.txt  
lynx@lynx:~$
```

Please note that by inputting different text into file3, that the hash is wildly different that the files in Task 1. This is due to the Avalanche effect in Hashing.

### Task 3

```
wget https://github.com/0x00001337/BlackTeamAcademy/blob/main/catpictureess.jpg  
md5sum catpictureess.jpg
```

```
lynx@lynx:~$ wget https://github.com/0x00001337/BlackTeamAcademy/blob/main/catpictureess.jpg  
--2024-03-17 17:19:33-- https://github.com/0x00001337/BlackTeamAcademy/blob/main/catpictureess.jpg  
Resolving github.com (github.com)...  
Connecting to github.com (github.com)|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 4240 (4.1K) [text/plain]  
Saving to: 'catpictureess.jpg'  
  
catpictureess.jpg 100%[=====] 4.14K --.-KB/s in 0s  
2024-03-17 17:19:33 (8.46 MB/s) - 'catpictureess.jpg' saved [4240/4240]  
  
lynx@lynx:~$ md5sum catpictureess.jpg  
01e4e6dbcca17552ae7da38b46b53ba0 catpictureess.jpg  
lynx@lynx:~$
```

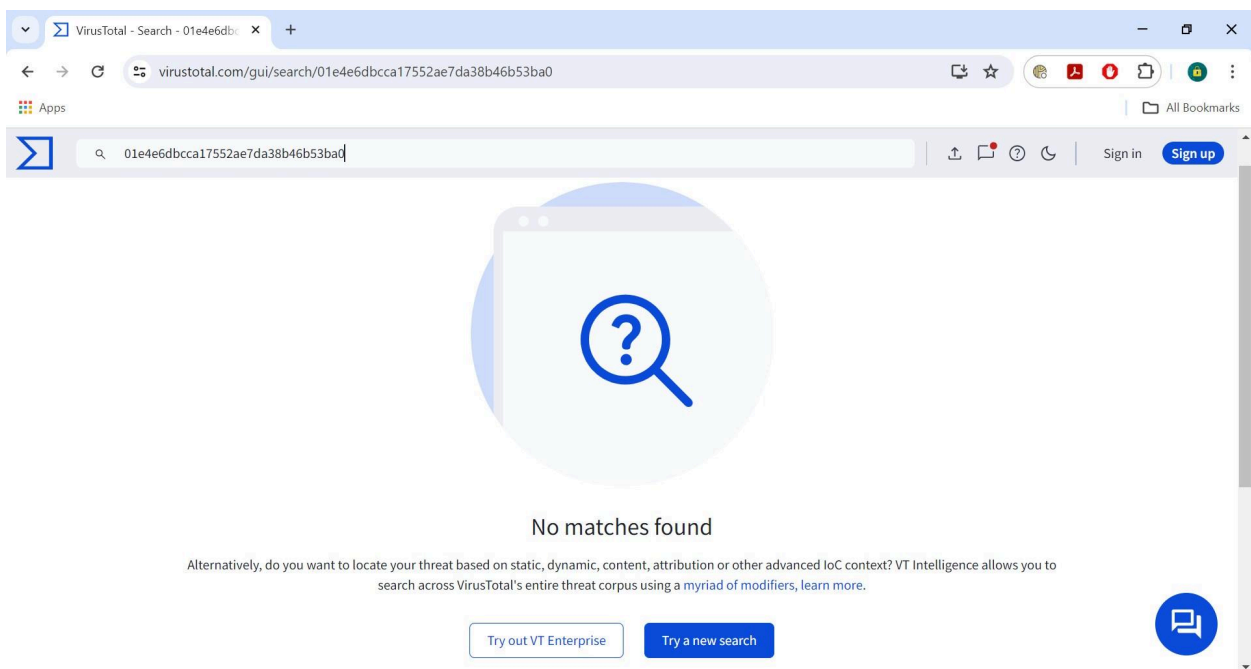
Let's briefly check virustotal

Browse to virus total: <https://www.virustotal.com/gui/home/search>

Copy the above has for catpictureess.jpg and paste it into the search field.

Enter it into the system.

It should return with "No Matches Found" which is GREAT NEWS!

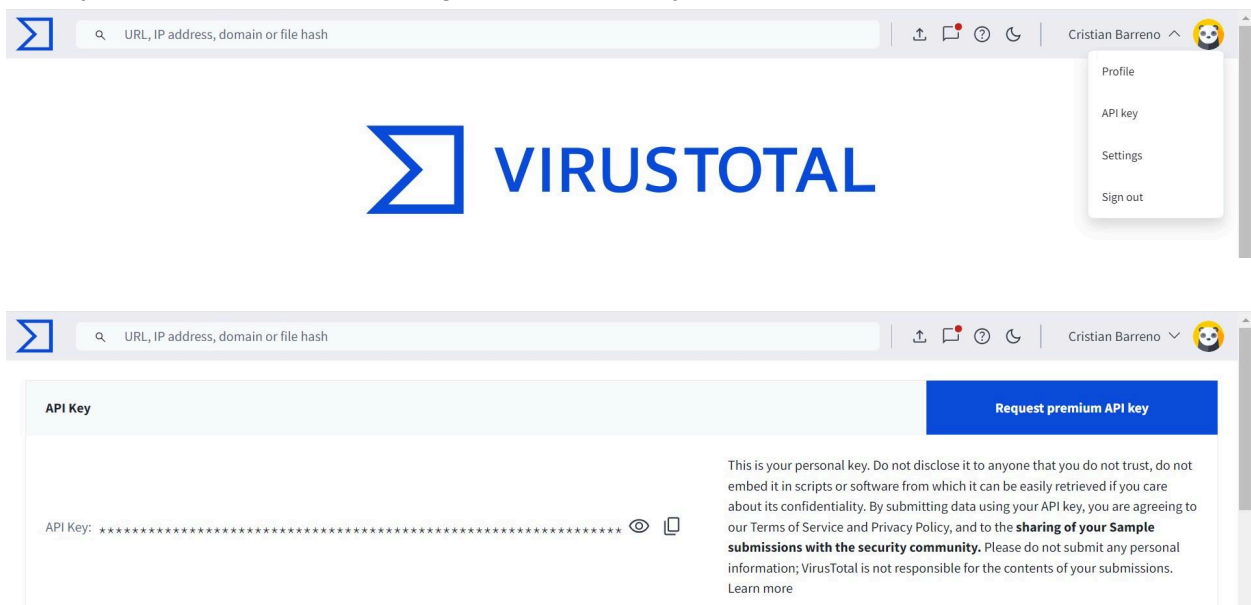


## Task 4

Let's take this up a couple of notches.  
Start in the home folder of your Linux Server

### Step 1

Open a browser to <https://www.virustotal.com>  
Create an Account  
Once you create an account, navigate to the API key



You'll need to copy the API key into the VirusTotal software later, don't navigate away from this page.

### Step 2

In your Linux Server  
We have to download the pre-compiled VirusTotal Application.  
Use the following command to download the zipped file.

```
wget https://github.com/VirusTotal/vt-cli/releases/download/1.0.0/Linux64.zip
```

```
lynx@lynx:~$ wget https://github.com/VirusTotal/vt-cli/releases/download/1.0.0/Linux64.zip
--2024-03-17 17:43:07-- https://github.com/VirusTotal/vt-cli/releases/download/1.0.0/Linux64.zip
Resolving github.com (github.com)... 140.82.112.4
Connecting to github.com (github.com)|140.82.112.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/133561480/bb8bbce9-0ce3-431d-839d-124ec1ecb76f?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVCOYL5A53PQK4ZA%2F20240317%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240317T174307Z&X-Amz-Expires=300&X-Amz-Signature=77f9a20225dfed9e3cc228d2a5ed864cb70739719efc206a84f4de6b806acd248X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=133561480&response-content-disposition=attachment%3B%20filename%3DLinux64.zip&response-content-type=application%2Foctet-stream [following]
--2024-03-17 17:43:07-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/133561480/bb8bbce9-0ce3-431d-839d-124ec1ecb76f?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVCOYL5A53PQK4ZA%2F20240317%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240317T174307Z&X-Amz-Expires=300&X-Amz-Signature=77f9a20225dfed9e3cc228d2a5ed864cb70739719efc206a84f4de6b806acd248X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=133561480&response-content-disposition=attachment%3B%20filename%3DLinux64.zip&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.110.133, 185.199.111.133, 185.199.108.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7120233 (6.8M) [application/octet-stream]
Saving to: 'Linux64.zip'

Linux64.zip           100%[=====] 6.79M  25.6MB/s   in 0.3s

2024-03-17 17:43:08 (25.6 MB/s) - 'Linux64.zip' saved [7120233/7120233]

lynx@lynx:~$
```

List the directory to check.

**ls**

```
lynx@lynx:~$ wget https://github.com/VirusTotal/vt-cli/releases/download/1.0.0/Linux64.zip
--2024-03-17 17:43:07-- https://github.com/VirusTotal/vt-cli/releases/download/1.0.0/Linux64.zip
Resolving github.com (github.com)... 140.82.112.4
Connecting to github.com (github.com)|140.82.112.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/133561480/bb8bbce9-0ce3-431d-839d-124ec1ecb76f?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVCOYL5A53PQK4ZA%2F20240317%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240317T174307Z&X-Amz-Expires=300&X-Amz-Signature=77f9a20225dfed9e3cc228d2a5ed864cb70739719efc206a84f4de6b806acd248X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=133561480&response-content-disposition=attachment%3B%20filename%3DLinux64.zip&response-content-type=application%2Foctet-stream [following]
--2024-03-17 17:43:07-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/133561480/bb8bbce9-0ce3-431d-839d-124ec1ecb76f?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVCOYL5A53PQK4ZA%2F20240317%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240317T174307Z&X-Amz-Expires=300&X-Amz-Signature=77f9a20225dfed9e3cc228d2a5ed864cb70739719efc206a84f4de6b806acd248X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=133561480&response-content-disposition=attachment%3B%20filename%3DLinux64.zip&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.110.133, 185.199.111.133, 185.199.108.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7120233 (6.8M) [application/octet-stream]
Saving to: 'Linux64.zip'

Linux64.zip           100%[=====] 6.79M  25.6MB/s   in 0.3s

2024-03-17 17:43:08 (25.6 MB/s) - 'Linux64.zip' saved [7120233/7120233]

lynx@lynx:~$ ls
catpicturess.jpg  file2.txt  Linux64.zip  log2.txt    notmalwareonreally.txt  windows_activity_logs.txt
file1.txt         file3.txt  log1.txt    malware.txt windows_activity_logs2.txt

lynx@lynx:~$
```

and Linux 64.zip should be there.

Now, to unzip this zipped file, we'll need to install unzip.

**sudo apt install unzip -y**

```

lynx@lynx:~$ sudo apt install unzip
[sudo] password for lynx:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  zip
The following NEW packages will be installed:
  unzip
0 upgraded, 1 newly installed, 0 to remove and 61 not upgraded.
Need to get 175 kB of archives.
After this operation, 386 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 unzip amd64 6.0-26ubuntu3.2 [175 kB]
Fetched 175 kB in 31s (5,700 B/s)
Selecting previously unselected package unzip.
(Reading database ... 110818 files and directories currently installed.)
Preparing to unpack .../unzip_6.0-26ubuntu3.2_amd64.deb ...
Unpacking unzip (6.0-26ubuntu3.2) ...
Setting up unzip (6.0-26ubuntu3.2) ...
Processing triggers for man-db (2.10.2-1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
lynx@lynx:~$

```

Time to unzip the VirusTotal application.

**unzip Linux64.zip**

```

lynx@lynx:~$ unzip Linux64.zip
Archive: Linux64.zip
  inflating: vt
lynx@lynx:~$

```

Now run ls and you should see the vt application in your folder. (Hopefully your home folder)

Time to initialize the vt or VirusTotal Application. **Please note you'll need to use dot slash before the application to get it to work.**

**./vt init**

```

lynx@lynx:~$ unzip Linux64.zip
Archive: Linux64.zip
  inflating: vt
lynx@lynx:~$ ls
captures.jpg  file2.txt  Linux64.zip  log2.txt  notmalwareoreally.txt  windows_activity_logs2.txt
file1.txt     file3.txt  log1.txt    malware.txt  vt                    windows_activity_logs.txt
lynx@lynx:~$ ./vt init

```

**VIRUSTOTAL**

VirusTotal Command-Line Interface: Threat Intelligence at your fingertips.

## Enter your API key:

```
lynx@lynx:~  
lynx@lynx:~$ unzip linux64.zip  
Archive: linux64.zip  
  inflating: vt  
lynx@lynx:~$ ls  
catpictureess.jpg  file2.txt  Linux64.zip  log2.txt  notmalwareoreally.txt  windows_activity_logs2.txt  
file1.txt          file3.txt  log1.txt      malware.txt  vt              windows_activity_logs.txt  
lynx@lynx:~$ ./vt init  
  
VIRUSTOTAL  
  
VirusTotal Command-Line Interface: Threat Intelligence at your fingertips.  
Enter your API key:   
Your API key has been written to config file /home/lynx/.vt.toml  
lynx@lynx:~$
```

NOW! We are ready to start using Virus Total from the CLI!

## Step 3

`md5sum catpictureess.jpg`

Now we are going to check this hash in virustotal from the CLI. Please note you'll need to use dot slash before the application to get it to work.

Understand the syntax `./` then `vt` then `file` and then `the hash`.

`./vt file 01e4e6dbcca17552ae7da38b46b53ba0`

```
lynx@lynx:~  
lynx@lynx:~$ unzip linux64.zip  
Archive: linux64.zip  
  inflating: vt  
lynx@lynx:~$ ls  
catpictureess.jpg  file2.txt  Linux64.zip  log2.txt  notmalwareoreally.txt  windows_activity_logs2.txt  
file1.txt          file3.txt  log1.txt      malware.txt  vt              windows_activity_logs.txt  
lynx@lynx:~$ ./vt init  
  
VIRUSTOTAL  
  
VirusTotal Command-Line Interface: Threat Intelligence at your fingertips.  
Enter your API key:   
Your API key has been written to config file /home/lynx/.vt.toml  
lynx@lynx:~$ md5sum catpictureess.jpg  
01e4e6dbcca17552ae7da38b46b53ba0  catpictureess.jpg  
lynx@lynx:~$ ./vt file 01e4e6dbcca17552ae7da38b46b53ba0  
File "01e4e6dbcca17552ae7da38b46b53ba0" not found  
lynx@lynx:~$
```

HURRAY! The cat picture is still not a virus, according to Virus Total.

## Step 4

Let's use a known bad hash.

Let's pull up our Virus Total Web page, and paste the following known bad hash:

00434c7dabe90c49dfcb78038e7595e1cfb87851

And let's press the search icon on the right.

Oh my!

65

/71

Community Score

🔴

🟢

🔴 65/71 security vendors and 1 sandbox flagged this file as malicious

Reanalyze

Similar

More

1c5eb6aff2a97fb0c1cca7e497821f0dd6571ece0ce71d1c4833093072df5db4

Size

56.00 KB

Last Modification Date

2 days ago

🔗

EXE

peexe

runtime-modules

checks-network-adapters

spreader

direct-cpu-clock-access

long-sleeps

checks-user-input

detect-debug-environment

DETECTION

DETAILS

RELATIONS

BEHAVIOR

TELEMETRY

COMMUNITY 4

Crowdsourced YARA rules

⚠️ Matches rule win\_brambul\_auto from ruleset win.brambul\_auto at https://malpedia.caad.fkie.fraunhofer.de/ by Felix Bilstein - yara-signator at cocacoding dot com

↳ Detects win.brambul.

Crowdsourced IDS rules

HIGH 0

MEDIUM 4

LOW 5

INFO 0

So... that's really bad.

Lots of detections

But, let's see how this looks like doing it via the command line.

```
./vt file 4e89d194f2575c3a1636bcb1091a0f9f
```

```
lynx@lynx:~$ unzip Linux64.zip
Archive: Linux64.zip
  inflating: vt
lynx@lynx:~$ ls
catpicturess.jpg  file2.txt  Linux64.zip  log2.txt  notmalwarearereally.txt  windows_activity_logs2.txt
file1.txt         file3.txt  log1.txt    malware.txt  vt                windows_activity_logs.txt
lynx@lynx:~$ ./vt init

VIRUSTOTAL

VirusTotal Command-Line Interface: Threat Intelligence at your fingertips.

Enter your API key:
Your API key has been written to config file /home/lynx/.vt.toml
lynx@lynx:~$ md5sum catpicturess.jpg
01e4e6dbccal7552ae7da38b46b53ba0  catpicturess.jpg
lynx@lynx:~$ ./vt file 01e4e6dbccal7552ae7da38b46b53ba0
File "01e4e6dbccal7552ae7da38b46b53ba0" not found
lynx@lynx:~$ ./vt file 4e89d194f2575c3a1636bcb1091a0f9f
File "4e89d194f2575c3a1636bcb1091a0f9f" not found
lynx@lynx:~$ ./vt file 00434c7dabe90c49dfcb78038e7595e1c1fb87851
- id: "1c5eb6aff2a97fb0c1cca7e497821f0dd6571ece0ce71d1c4833093072df5db4"
  _type: "file"
  authenticithash: "fff3530eb0fcd6f36777a9dd5c2fa211b8841ced09736c673645ee803db73eb7e"
  creation_date: 1255524354 # 2009-10-14 12:45:54 +0000 UTC
  crowdsourced_ids_results:
- alert_context:
  - src ip: "93.220.189.23"
```

And it goes on and on and on, wow! That is a huge output! How can we control or manage this?



## Step 5

Let's redirect the output to a file, so we can control what we are seeing.

```
./vt file 00434c7dabe90c49dfcb78038e7595e1cfb87851 > ebil.txt
```

Now, we can use any of the Linux Text READERS to check out the file.

Less, More, Cat, Head, Tail? What seems like it would be the most useful? The author is going to use less.

```
lynx@lynx: ~  
size: 57344  
ssdeep: "768:9wB+9FisiTZdz4HLCLTRnVuwGiJTPpf16dw6WsyqAgg8RCW+j12wDMrL4C:9sisiTuLCLTRVuwZp5l/lzyqFg8B+RPC"  
tags:  
- "peexe"  
- "runtime-modules"  
- "checks-network-adapters"  
- "spreader"  
- "direct-cpu-clock-access"  
- "long-sleeps"  
- "checks-user-input"  
- "detect-debug-environment"  
times_submitted: 2  
tlsh: "T17B43AE13BCC094F2E45381B161DA9F3AD63720B552AA54C7DFA4CCA76D370B1DA2E18B"  
total_votes:  
  harmless: 0  
  malicious: 0  
trid:  
- file_type: "Petite compressed Win32 executable"  
  probability: 66.7  
- file_type: "Microsoft Visual C++ compiled executable (generic)"  
  probability: 15.4  
- file_type: "Win64 Executable (generic)"  
  probability: 9.8  
- file_type: "Win32 Executable (generic)"  
  probability: 4.2  
- file_type: "Generic Win/DOS Executable"  
  probability: 1.8  
type_description: "Win32 EXE"  
type_extension: "exe"  
type_tag: "peexe"  
type_tags:  
- "executable"  
- "windows"  
- "win32"  
- "pe"  
- "peexe"  
unique_sources: 2  
vhash: "0540465d1d1f70a8z3f061z15zf7z"  
lynx@lynx:~$  
lynx@lynx:~$ ./vt file 00434c7dabe90c49dfcb78038e7595e1cfb87851 > ebil.txt  
lynx@lynx:~$
```



## less ebil.txt

```
lynx@lynx: ~  
- id: "1c5eb6aff2a97fb8c1cca7e497821f0dd6571ece0ce71d1c4833093072df5db4"  
  _type: "file"  
  authenticash: "ff3530eb0fcd6f36777a9dd5c2fa211b8841ced09736c673645ee803db73eb7e"  
  creation_date: 1255524354 # 2009-10-14 12:45:54 +0000 UTC  
  crowdsourced_ids_results:  
- alert_context:  
  - src_ip: "93.220.189.23"  
    alert_severity: "medium"  
    rule_category: "attempted-recon"  
    rule_id: "116:441"  
    rule_msg: "(icmp4) ICMP destination unreachable communication administratively prohibited"  
    rule_raw: "alert ( gid:116; sid:441; rev:2; msg:\"(icmp4) ICMP destination unreachable communication administratively prohibited\"; metadata: rule-type decode; classtype:attempted-recon;)"  
    rule_source: "Snort registered user ruleset"  
    rule_url: "https://www.snort.org/downloads/#rule-downloads"  
- alert_context:  
  - src_ip: "173.44.201.217"  
    alert_severity: "medium"  
    rule_category: "attempted-recon"  
    rule_id: "116:442"  
    rule_msg: "(icmp4) ICMP destination unreachable communication with destination host is administratively prohibited"  
    rule_raw: "alert ( gid:116; sid:442; rev:2; msg:\"(icmp4) ICMP destination unreachable communication with destination host is administratively prohibited\"; metadata: rule-type decode; classtype:attempted-recon;)"  
    rule_source: "Snort registered user ruleset"  
    rule_url: "https://www.snort.org/downloads/#rule-downloads"  
- alert_context:  
  - dest_ip: "210.172.74.97"  
    dest_port: 445  
    alert_severity: "medium"  
    rule_category: "attempted-recon"  
    rule_id: "122:7"  
    rule_msg: "(port_scan) TCP filtered portsweep"  
    rule_raw: "alert ( gid:122; sid:7; rev:2; msg:\"(port_scan) TCP filtered portsweep\"; metadata: rule-type preproc; classtype:attempted-recon;)"  
    rule_source: "Snort registered user ruleset"  
    rule_url: "https://www.snort.org/downloads/#rule-downloads"  
- alert_context:  
  - src_ip: "91.188.6.134"  
    src_port: 445  
    alert_severity: "medium"  
    rule_category: "bad-unknown"
```

Now by using the command line interface text connection to virus total, I can bring in automatable log enrichment and information that can be used with other code to provide good threat intelligence and a way to populate cybersecurity systems.