

TSC Ferret

Cheatsheet & Tips

Basic Usage

Specifying plugin ID/config file name:

```
[-P | -C] [plugin_ID | config_file]
```

E.G.

```
./run.py -P 22869
```

or

```
./run.py -C my_config_file
```

Specifying the output type

TSC Ferret supports four different output types:

```
- html, csv, pdf, or json
```

The default output type is html, but can be changed with the "-o" argument.

E.G.: `./run.py -P 10180 -o csv`

Repository Specification

Use the "-R" argument to specify a file with a list of repository names whose data to return.

Note: Target repositories must be saved to a plaintext file and newline delimited.

E.G.

```
./run.py -P [plugin_ID] -R repofile
```

Host Specification

Use the "-H" argument to specify a host file with a list of hosts whose data to return.

Targets can be in the following formats:

- **IPv4** (192.168.1.1)
- **IPv6** (ABCD:EF01:2345:6789)
- **CIDR** (192.168.0.0/16)

Note: Targets must be saved to a plaintext file and newline delimited.

E.G.

```
./run.py -P [plugin_ID] -H hostfile
```

Column Specification

The "-c" argument allows users to specify the data columns to be returned.

By default, data is split into "Host Info" (IP, DNS, MAC, Repository, and Last Seen) and "Plugin Output" (data returned by plugin).

Columns users can specify:

- IP, DNS, MAC, REPO (Repository), L_SEEN (Last Seen) and CONTENT (Plugin Output)

E.G.

```
./run.py -P [plugin_ID] -c content
```

or

```
./run.py -P [plugin_ID] -c "IP, L_SEEN, CONTENT"
```

Creating a Config File

Run `./config_gen.py` to generate a configuration file from user input.

Search Output

Use the "-s" argument to specify a search query file with strings to query the plugin output.

Lines matching/containing a substring matching the query will be returned in a new column (named after query) and can be returned given the column specification argument with the "CONTENTS" flag.

Note: Queries must be saved to a plaintext file and newline delimited.

E.G.

```
./run.py -P [plugin_ID] -s queryfile
```

Notable Plugins

Ping the remote host	10180
Software enumeration	22869
Unsupported Web Server Detection	34460
TLS Version 1.0 Detection	104743
Red Hat Update Level	14657
Patch Report	66334
SSH Weak Algorithms Supported	90317
SSL Certificate Info	10863
SSL v2/v3 Protocol Detection	20007
SSL Cert Cannot Be Trusted	51192

Note: More information about the plugins @ www.tenable.com/plugins