7. Custom Reports

Navigation

Defining Reports

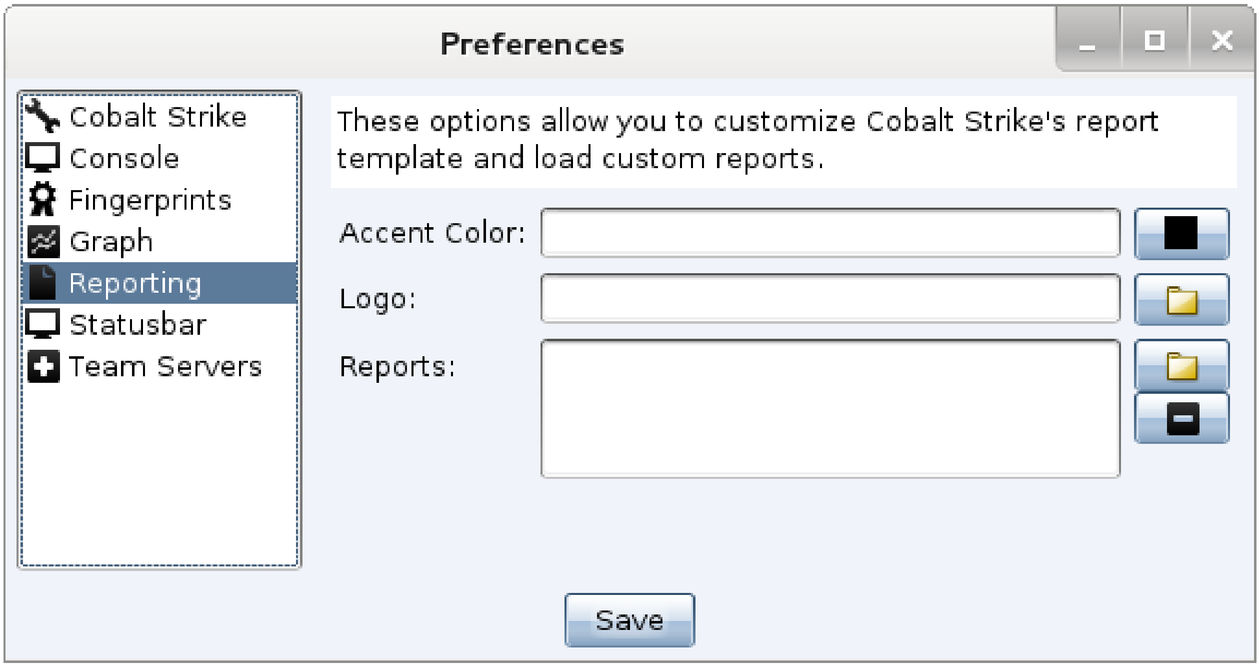
Cobalt Strike uses a domain-specific language to define its reports. This language is similar to Aggressor Script but does not have access to most of its APIs. The report generation process happens in its own script engine isolated from your client.

The report script engine has access to a data aggregation API and a few primitives to specify the structure of a Cobalt Strike report.

The default.rpt (default.rpt) file defines the default reports in Cobalt Strike.

Loading Reports

Go to **Cobalt Strike** -> **Preferences** -> **Reports** to load a custom report. Press the Folder icon and select a .rpt file. Press **Save**. You should now see your custom report under the **Reporting** menu in Cobalt Strike.



These options allow you to customize Cobalt Strike's report template and load custom reports.

Load a report file here.

Report Errors

If Cobalt Strike had trouble with your report (e.g., a syntax error, runtime error, etc.) this will show up in the script console. Go to **View** -> **Script Console** to see these messages.

"Hello World" Report

Here's a simple "Hello World" report. This report doesn't represent anything special. It merely shows how to get started with a custom report.

```
# default description of our report [the user can change this].
describe("Hello Report", "This is a test report.");

# define the Hello Report
report "Hello Report" {
        # the first page is the cover page of our report.
        page "first" {
                # title heading
                h1($1['long']);

                # today's date/time in an italicized format
                ts();

                # a paragraph [could be the default...
                p($1['description']);
        }

        # this is the rest of the report
        page "rest" {
                # hello world paragraph
                p("Hello World!");
        }
}
```

Aggressor Script defines new reports with the **report** keyword followed by a report name and a block of code. Use the **page** keyword within a report block to define which page template to use. Content for a page template may span multiple pages. The first page template is the cover of Cobalt Strike's reports. This example uses &h1 (rfunctions.html#h1) to print a title heading. The &ts (rfunctions.html#ts) function prints a date/time stamp for the report. And the &p (rfunctions.html#p) function prints a paragraph.

The &describe (rfunctions.html#describe) function sets a default description of the report. The user may edit this when they generate the report. This information is passed to the report as part of the report metadata in the **$1** parameter. The **$1** parameter is a dictionary with information about the user's preferences for the report.

Data Aggregation API

Cobalt Strike Reports depend on the Data Aggregation API to source their information. This API provides you a merged view of data from all team server's your client is currently connected to. The Data Aggregation API allows reports to provide a comprehensive report of the assessment activities. These functions begin with the ag prefix (e.g., &agTargets (rfunctions.html#agTargets)). The report engine passes a data aggregate model when it generates a report. This model is the **$3** parameter.