Qualys Scripts

Qualys Scripts provide customers with a set of Perl scripts that allows for automation as well as for the integration of multiple solutions. Customers can leverage and scale their current processes and investments to increase their effectiveness, as well as further automate common tasks and workflows.

All Qualys Scripts are written in Perl. Qualys Scripts use only modules available in CPAN, PPM, and other reliable repositories with documentation on where to find the modules. Please note that Qualys supports the scripts, not the Perl environment. Scripts are supported on Windows and Unix/Linux platforms. Scripts can be automatically scheduled using system utilities.

This document provides a brief description of each of the Qualys Scripts, which have been tested and approved for distribution.

Please Note: Before you begin running scripts, please find your Qualys API server URL. You must supply your API server URL as an input parameter on the command line, in a configuration file or in the script itself. The API server URL to use depends on your account location.

Account Location	**API Server URL**
Qualys US Platform 1	qualysapi.qualys.com
Qualys US Platform 2	qualysapi.qg2.apps.qualys.com
Qualys EU platform	qualysapi.qualys.eu
Qualys Private Cloud Platform	qualysapi.<customerbaseURL>

If you will use client certificates with the Qualys Scripts, there is native support within the Crypt::SSLeay Perl library by just using these environment variables :

```
$ENV{HTTPS_CERT_FILE} = '<certificate path>.pem';
$ENV{HTTPS_KEY_FILE} = '<associated key path>.pem'
```

For information on client certificate support using this Perl library, please visit:
http://search.cpan.org/~dland/Crypt-SSLeay-0.57/SSLeay.pm#CLIENT_CERTIFICATE_SUPPORT

Ag_sc

Ag_sc.pl reads a configuration file with a list of asset groupss, retrieves the data and totals the severities. The output contains 3 sections: a list of severities by asset groups, a list of the most vulnerable hosts, and a list the Top N found vulnerabilities. All lists are filtered by severities and types of vulnerability – All, Confirmed Vulnerabilities (Vuln), Potential Vulnerabilities (Practice), Information Gathered (Ig) – and date range specified in the configuration file.

Ag_tr

Ag_tr.pl provides in csv format a total count of vulnerabilities per asset group organized by asset owner based on a customer defined trend reports list. The Ag_tr.pl script helps customers to reduce the time spent on analyzing multiple trend reports by automatically generating a csv file that includes these details:

- Owner, as defined by the customer in the configuration file
- Asset Group title
- Number of assets in each asset group
- Total number of vulnerabilities per severity level in each asset group
- Total number of vulnerabilities per status in each asset group

AssetGroup_report_card

Assetgroup_report_card.pl calculates scorecards per asset group providing a host count, Windows host count, confirmed vulnerabilities count and potential vulnerabilities count per severity. It also allows identifying up to 4 QIDs for missing software.

The output from this script is a single file. The csv filename has a format similar to “reportcard-2006-05-22-14-08-25-assetgroup_report_card.conf”. The output includes this information:

- Asset Group title
- Total number of hosts in the asset group
- Number of severity level 5 vulnerabilities
- Number of severity level 4 vulnerabilities
- Number of severity level 3 vulnerabilities (optional)
- Total number of hosts in the asset group that have a severity level 3, 4 or 5 vulnerability
- Number of Windows hosts
- Up to 4 QIDs that identify missing software – i.e. AV, Microsoft SMS, Cisco Trust Agent, etc. (optional)

Filterscan

Filterscan.pl automatically downloads scan results and creates Excel files that summarize total vulnerabilities per host, total vulnerabilities per scan, total hosts per scan, and total vulnerabilities across all scans. It groups results by asset group. The output from this script includes two files. The first file, with a name like this %date-time-of-scan%-%title of scan%-data.xls, includes a complete list with the IP address, hostname, QID, severity level and title of the vulnerability provided. The second file, with a name like this %date-time-of-scan%-%title of scan%-report.xls, includes a summary report to show the most vulnerable hosts. Sorting is performed by number of vulnerabilities on each host.

Findports

FindPorts.pl downloads scan results and creates a list of all systems identifying which systems are running specific pre-defined ports and/or services, i.e. systems that have port 80 listening on a network, systems that have http or ftp servers, etc. The Findports.pl script configuration file is used to track account information including the last scan data downloaded so that only new scan results are downloaded and processed.

Map2xls

Map2xls.pl downloads all map data outputs in tab delimited format, which can be easily imported into Excel. Map2xls has a configuration file used to track account information including the last map data downloaded so that only new data is downloaded. It also includes OS filtering capabilities.

Report_filter.pl

Report_filter.pl script uses a Policy_Compliance template file to filter detected vulnerabilities in the PolicyFile output. The Report_filter.pl script can also be run with a find_applications template to create an output that identifies all applications installed on machines based on scan results (QID 90235).

Pull_Tickets

Pull_Tickets.pl script uses the remediation API to download ticket information based on an editable configuration file. It provides a filtering mechanism based on ticket state and status. The output information follows a customizable template.

Scan2xls

Scan2xls.pl creates a list of all systems, identifies which UDP and TCP ports are active for each system, providing and provides OS information. The output tab delimitated file can be imported into Microsoft Excel or other applications. The Scan2xls.pl script has a configuration file used to track account information including the last scan data downloaded so that only new data is downloaded.

Scanlauncher

ScanLauncher.pl launches a scan against a set of IP addresses provided in a flat file, i.e. an IDS writes out a file that includes the IP addresses being attacked, and a scan is then launched against those systems. Scanlauncher.pl doesn’t provide output other than an error log if an error is encountered while trying to launch the scan.

SelectiveQID

SelectiveQIDs.pl created a list of all systems identifying which systems had the user selected QID detected on them. The results can be easily imported into Microsoft Excel or other applications. The SelectiveQIDs.pl script has a configuration file used to track account information including the last scan data downloaded so that only new data is downloaded. This script is most used for compliance, e.g. entering the QID for the discovery of Norton AntiVirus will return a report that shows windows hosts with NAV installed and ones where it is not installed.

TopN

TopN.pl checks your saved scans (or a time-bounded subset of your saved scans) to find the most recent scan for each host, and provides a tab-delimited output file that lists the top N vulnerabilities per asset group, including your All group.