Automate Your Internet Security

QualysGuard

API v2.01 Documentation

Document Revision: 2.01

Overview

The QualysGuard API allows Qualys Partners to integrate QualysGuard into their own applications. This document contains instructions for including QualysGuard capabilities in third-party applications; instructions for obtaining working sample code; and a detailed reference section including DTDs, XPaths, and sample output.

Contents

Introduction

The QualysGuard Application Program Interface (API) allows Qualys Partners to integrate QualysGuard into their own applications.

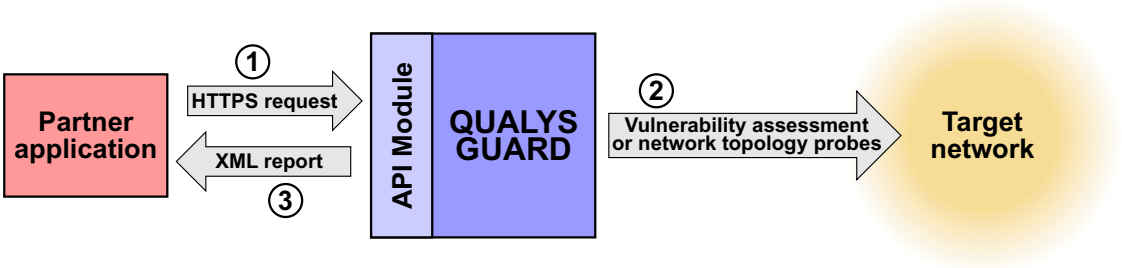
The QualysGuard API Module allows access to two essential functions of QualysGuard:

QualysScan: assesses the vulnerability of a host or a group of hosts.

QualysMap: maps the network topology of all hosts under a domain name.

In addition to providing core QualysGuard capabilities, the API enables partners to automatically create QualysGuard accounts for their customers for full integration with their applications.

How it works



From the Partner's point of view, the system works as follows:

1. Connection:

The partner application establishes a secure HTTP connection (using SSL encryption and "basic" authentication) with QualysGuard's API Module. The HTTP request includes the IP address(es) to be scanned or the domain to be mapped.

2. Scan/Map/Enroll:

The QualysGuard server performs a vulnerability assessment (QualysScan), maps a domain (QualysMap), or creates a new user account (Enrollment).

3. Report:

Upon completion, the QualysGuard server returns a report in XML format.

Using the QualysScan API

To use the QualysScan API, you will need to develop an application that performs the following operations:

1. Send an HTTP request to QualysScan
2. Receive the XML report
3. Decode the XML report

QualysScan has four functions: **scan**; **scan & save**; **list**; and **retrieve**. The first part of this section will cover the basic "scan" functionality.

1. Send an HTTP request

Your application will send an authenticated request to the QualysGuard server using a URL of the following form:

```
https://{server}.qualys.com/msp/scan.php?ip={addresses}
```

where {server} represents the name of the server to which the partner is connected, and {addresses} represents the IP address(es) to be scanned.

Server

Normally, {server} will be "www.fr" or "www.us," as in the following examples:

```
https://www.fr.qualys.com/    for Europe, or
https://www.us.qualys.com/    for the US
```

IP address

If only one IP address will be scanned, then the format is simple. For example:

```
https://www.us.qualys.com/msp/scan.php?ip=1.2.3.4
```

If more than one IP address is to be scanned, the multiple addresses should be in the following format:

```
https://www.us.qualys.com/msp/scan.php?ip=1.2.3.4-1.2.3.9,1.2.3.20
```

Authentication

Along with the URL, your application must send a username and password as part of the HTTP request (see the "Basic Authentication Scheme" section of RFC #2617). The exact method of doing this will vary according to which programming language is used; see the Sample API Code section for details.

2. Receive the XML file

Upon completion of the scan, an XML report is returned. The HTTPS connection, which was opened when the initial request was made, is finally closed after the report is returned.

3. Decode the XML file

There are a number of ways to parse an XML file; it is up to you to decide which is most appropriate. The DTD for QualysScan can be found in Appendix A of this document, or at the following URL:

```
http://{server}.qualys.com/scan-1.dtd
```

Some parts of the XML report may contain HTML tags or other special characters (such as accented letters). Therefore, many elements contain CDATA sections, which allow HTML tags to be included in the report. “High” ASCII and other non-printable characters are escaped using question marks.

Appendix B of this document describes, in detail, the possible attributes of the elements in QualysScan’s DTD.

Other QualysScan functions

Save

If you invoke QualysScan (`scan.php`) with the `save_report` argument set to `yes`, the report will be returned to your application, and it will *also* be saved on the Qualys server. For example:

```
https://{server}.qualys.com/msp/scan.php?ip=1.2.3.4&save_report=yes
```

List

To retrieve a list of previously saved reports, use the following URL:

```
https://{server}.qualys.com/msp/scan_report_list.php
```

You will receive a list of reports in XML format. Each report has a reference code, a date, and a list of the IP addresses that were scanned, as described in the DTD in Appendix C.

There are also two optional arguments to `scan_report_list`, which can be used individually or together:

- If you include `last=yes`, you will only get the information on the *last* scan that was saved.
- If you include `target={address}`, where *address* is an IP address, you will receive a list of all saved reports that include the target IP.
- Finally, if you include *both* an IP address (`target`) *and* `last=yes`, you will get the information on the last saved scan that included the target IP. For example:

```
https://{server}.qualys.com/msp/scan_report_list.php?
  target=1.2.3.4&last=yes
```

Retrieve

To retrieve a previously saved report, use `scan_report.php`, with a reference code (defined in the `ref` argument). For example:

```
https://{server}.qualys.com/msp/scan_report.php?
  ref=scan/987659876.19876
```

The output from the "retrieve" function is functionally identical to that of a simple scan, but it will generally be returned more quickly because the scan has already been performed previously.

There is one optional argument to `scan_report.php`: you can specify an IP address in the `target` argument, and the report will only include the sections that match the IP address you specify. (In technical terms, only one `<IP>` element will be included in the report.)

```
https://{server}.qualys.com/msp/scan_report.php?
  ref=scan/987659876.19876&target=1.2.3.4
```

Using the QualysMap API

To use the QualysMap API, the Partner will need to develop an application that performs the following operations:

1. Send an HTTP request to QualysMap
2. Receive the XML report
3. Decode the XML report

1. Send an HTTP request

Your application will send an authenticated request to the QualysGuard server using a URL of the following form:

```
https://{server}.qualys.com/msp/map.php?domain={target}
```

where {server} represents the name of the server to which the partner is connected, and {target} represents the domain to be mapped.

Server

Normally, {server} will be “www.fr” or “www.us,” as in the following examples:

```
https://www.fr.qualys.com/    for Europe, or
https://www.us.qualys.com/    for the US
```

Target network

Since only one domain name can be mapped at a time, the syntax is very simple. Here’s an example:

```
https://www.us.qualys.com/msp/map.php?domain=targetdomain.com
```

Authentication

Along with the URL, your application must send a username and password as part of the HTTP request (see the “Basic Authentication Scheme” section of RFC #2617). The exact method of doing this will vary according to which programming language is used; see the Sample API Code section for details.

2. Receive the XML file

Upon completion of the scan, an XML file is returned. The HTTPS connection, which was opened when the initial request was made, is finally closed after the report is returned.

3. Decode the XML file

There are a number of ways to parse an XML file; it is up to you to decide which is most appropriate. The DTD for QualysMap can be found in Appendix G of this document, or at the following URL:

```
http://{server}.qualys.com/map-1.dtd
```

Using the QualysGuard Enrollment API

The QualysGuard Enrollment API module allows you to set up new Qualys accounts. There are three steps in this process:

1. Send an HTTP request to the QualysGuard enrollment system
2. Receive the XML report
3. Decode the XML report

1. Send an HTTP request

Your application will send an authenticated request to the QualysGuard server using a URL of the following form:

```
https://{server}.qualys.com/msp/enrollment.php?{name=value pairs}
```

where {server} represents the name of the server to which the partner is connected. {name=value pairs} are described below.

Server

Normally, {server} will be “www.fr” or “www.us,” as in the following examples:

`https://www.fr.qualys.com/` for Europe, or
`https://www.us.qualys.com/` for the US

Authentication

Along with the URL, your application must send a username and password as part of the HTTP request (see the “Basic Authentication Scheme” section of RFC #2617). The exact method of doing this will vary according to which programming language is used.

NOTE: Enrollment API access is restricted to Back Office accounts only. Use your Back Office login and password to access the Enrollment API.

Name-Value Pairs

To enroll a user, you must submit — using either the POST or GET method — the following name-value pairs to the enrollment URL:

prefix	=	“Mr” | “Ms” | “Mrs”
firstname	=	string; max length 50
lastname	=	string; max length 50
title	=	string; max length 100
phone	=	string; max length 100
email	=	string, properly formatted; max length 80
company	=	string; max length 50
addr1	=	string; max length 80

city	=	string; max length 50
state	=	see Appendix L for acceptable values
zipcode	=	string; max length 20
country	=	see Appendix L for acceptable values
slevel	=	QualysGuard Service Level: varies by partner; contact your account manager for acceptable values
domain	=	domain used by QualysMap: string; must be valid domain; max length 67
targetip	=	IP addresses that may be scanned by the new account; multiple IP addresses may be supplied by delimiting ranges with a dash, and individual IP addresses with a comma (e.g., 1.2.3.4,1.2.3.5.7,1.2.3.9-1.2.3.11); Qualys partners are responsible for validating ownership (or permission) of the IP addresses submitted.
type	=	“Customer” (all partner created accounts are of type “Customer”)

You may optionally include the following name-value pairs when you create an account:

addr2	=	string; max length 80
fax	=	string; max length 100

2. Receive the XML file

Upon completion of the scan, an XML file is returned indicating either success or failure, with supporting information. The HTTPS connection, which was opened when the initial request was made, is finally closed after the report is returned.

3. Decode the XML file

There are a number of ways to parse an XML file; it is up to you to decide which is most appropriate. The DTD for the QualysGuard enrollment API can be found in Appendix J of this document, or at the following URL:

```
http://{server}.qualys.com/enrollment.dtd
```

Account Username And Password Delivery

By default, login credentials for accounts created using the QualysGuard Enrollment API are delivered directly to the end-user by the same process that is in place for accounts created using the Qualys Back Office.

API users may optionally bypass the normal delivery mechanism for login credentials and capture the username and password at account creation time by including the name-value pair “returnpassword” with a “yes” value.

Sample API Code

We have provided four sample programs in Java and in Perl that demonstrate the core concepts of using the QualysGuard API. The sample code is available in a ZIP file at the following URL:

`http://www.qualys.com/documentation/api/sample-code.zip`

Below is a brief description of each sample program.

get.pl / Get.java

The "get" example code demonstrates how to connect to the QualysGuard API (including SSL and basic authentication routines), how to execute the basic QualysScan features, and how to provide arguments to the API. When executed, "get" displays the results of the interaction with the API.

vulnsummary.pl / VulnSummary.java

The "vulnsummary" example code demonstrates how to connect to the QualysGuard API and how to extract vulnerability data from the resulting XML. The sample program returns a list of vulnerabilities, the IP address(es) effected, their severity, and their description. The vulnerabilities are discovered either by executing a scan when the program is run, or by retrieving the results of a previous scan.

score.pl / Score.java

The "score" example code, like "vulnsummary," demonstrates how to connect to the QualysGuard API and extract data from the resulting XML. This program goes a step further and returns a vulnerability "score" that is derived by adding up all of the severity attributes from each vulnerability that is discovered. The vulnerabilities are discovered either by executing a scan when the program is run, or by retrieving the results of a previous scan.

compare.pl / Compare.java

The "compare" example code uses the vulnerability score introduced in the "score" example above. This program calculates a score by running a scan against an IP range. The new calculated score is then compared to the most recent saved score for that same IP address range, and the results are reported.

Appendix A – DTD for scan.php

```
<!-- QUALYS SCAN DTD -->
<!-- $Id: scan-1.dtd,v 1.4 2001/06/22 14:26:00 ben Exp $ -->
<!ELEMENT SCAN ((HEADER,(ERROR|IP+))|ERROR)>
<!ATTLIST SCAN
          value CDATA #REQUIRED>

<!ELEMENT ERROR (#PCDATA)*>

<!-- INFORMATION ABOUT THE SCAN -->
<!ELEMENT HEADER (KEY)+>

<!ELEMENT KEY (#PCDATA)*>
<!ATTLIST KEY
          value CDATA #IMPLIED>

<!-- IP -->
<!ELEMENT IP ((INFOS,SERVICES?,VULNS?,PRACTICES?)|INFOS)>
<!ATTLIST IP
          value CDATA #REQUIRED
          name CDATA #IMPLIED>

<!-- CATEGORIES OF INFO, SERVICE, VULN or PRACTICE -->
<!ELEMENT CAT (INFO+|SERVICE+|VULN+|PRACTICE+)>
<!ATTLIST CAT
          value CDATA #REQUIRED
          fqdn CDATA #IMPLIED
          port CDATA #IMPLIED
          misc CDATA #IMPLIED>

<!-- IP INFORMATIONS -->
<!ELEMENT INFOS (CAT)+>

<!ELEMENT INFO (TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)>
<!ATTLIST INFO
          value CDATA #REQUIRED
          severity CDATA #IMPLIED>

<!-- MAP OF SERVICES -->
<!ELEMENT SERVICES (CAT)+>

<!ELEMENT SERVICE (TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)>
<!ATTLIST SERVICE
          value CDATA #REQUIRED
          severity CDATA #REQUIRED>

<!-- VULNERABILITIES -->
<!ELEMENT VULNS (CAT)+>

<!ELEMENT VULN (TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)>

<!-- vuln is QUALYS ID -->
<!-- severity is QUALYS SEVERITY LEVEL 1 TO 5 -->
<!-- esoid is E-SECURITY-ONLINE ID -->
<!ATTLIST VULN
          value CDATA #REQUIRED
          severity CDATA #REQUIRED
          esoid CDATA #IMPLIED
          cveid CDATA #IMPLIED>
```

```
<!ELEMENT TITLE (#PCDATA)*>

<!ELEMENT DIAGNOSIS (#PCDATA)*>

<!ELEMENT CONSEQUENCE (#PCDATA)*>

<!ELEMENT SOLUTION (#PCDATA)*>

<!-- if format is set to "table" -->
<!-- space is the col separator -->
<!-- and new line '\n' is the end of row -->
<!ELEMENT RESULT (#PCDATA)*>
<!ATTLIST RESULT
          format CDATA #IMPLIED>

<!-- SECURITY TIPS -->
<!ELEMENT PRACTICES (CAT)+>

<!ELEMENT PRACTICE (TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)>

<!ATTLIST PRACTICE
          value CDATA #REQUIRED
          severity CDATA #REQUIRED
          esoid CDATA #IMPLIED
          cveid CDATA #IMPLIED>

<!-- EOF -->
```


Appendix B – XPaths for scan.php

XPath	element specifications / notes
/SCAN	((HEADER,(ERROR | IP+)) | ERROR)
/SCAN/HEADER	(KEY)+
/SCAN/HEADER/KEY	(#PCDATA)*
attribute: **value**	**value** is *implied* and will be one of the following: COMPANY ..... Your company's name DATE ..... Date of scan TITLE ..... A descriptive title TARGET ..... The host(s) being scanned DURATION ..... How long the scan took to complete SCAN_HOST ..... The IP address of the computer doing the scan NBHOST_ALIVE ..... The number of hosts which are "alive" NBHOST_TOTAL ..... The total number of hosts
/SCAN/ERROR	(#PCDATA)*
/SCAN/IP	((INFOS,SERVICES,VULNS,PRACTICES?) | INFOS)
attribute: **value**	**value** is *required* and is an IP address
attribute: **name**	**name** is *implied* and, if present, is an Internet host name
/SCAN/IP/INFOS	(CAT)+
/SCAN/IP/INFOS/CAT	(INFO+ | SERVICE+ | VULN+ | PRACTICE+) *NOTE: When CAT is a child of INFOS, it can only contain INFO elements.*
attribute: **value**	**value** is *required* and will be one of the following: route ..... Information about the route packets cross from the scanner to the host whois ..... ISP & target network WHOIS results
attribute: **fqdn**	**fqdn** is *implied* and, if present, is the fully qualified Internet host name
attribute: **misc**	**misc** is *implied* and, if present, will be "over ssl," indicating that the connection is encrypted using SSL
attribute: **port**	**port** is *implied* and, if present, is the port number of the service being tested
/SCAN/IP/INFOS/CAT[@value="route"]/INFO	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: value	**value** is *required* and will be one of the following: traceroute ..... A traceroute from the scanner to the host
attribute: severity	**severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/INFOS/CAT[@value="whois"]/INFO	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required* and will be one of the following: whois_isp ..... The ISP network handle and info whois_network ..... The network handle and info
attribute: **severity**	**severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/INFOS/CAT/INFO/TITLE	(#PCDATA)*
/SCAN/IP/INFOS/CAT/INFO/DIAGNOSIS	(#PCDATA)*
/SCAN/IP/INFOS/CAT/INFO/CONSEQUENCE	(#PCDATA)*
/SCAN/IP/INFOS/CAT/INFO/SOLUTION	(#PCDATA)*
/SCAN/IP/INFOS/CAT/INFO/RESULT	(#PCDATA)*
attribute: **format**	**format** is *implied* and, if present, will be "table," indicating that the results are a table whose columns will be separated by spaces, and whose rows will be separated by new-line characters

/SCAN/IP/SERVICES	(CAT)+
/SCAN/IP/SERVICES/CAT	(INFO+ | SERVICE+ | VULN+ | PRACTICE+) *NOTE: When CAT is a child of SERVICES, it can only contain SERVICE elements.*
attribute: **value**	**value** is *required* and will be one of the following: darxite ... Darxite Web services detected Firewall ... Firewall detected ftpd ... FTP services detected http ... HTTP services detected irc ... IRC services detected linuxconf ... linuxconf detected mysql ... MySQL services detected netbios ... NetBIOS services detected os ... Operating system information pop2 ... POP2 services detected pop3 ... POP3 services detected PortScan ... Open ports detected Protocols ... Protocols in use rpc ... RPC services detected smb ... SMB services detected smtp ... Mail/SMTP services detected ssh ... SSH services detected telnetd ... Telnet services detected VNC ... VNC services detected X11 ... X-Windows services detected
attribute: **misc**	**misc** is implied and, if present, will contain "over ssl," indicating that the connection is encrypted using SSL
attribute: **fqdn**	**fqdn** is *implied* and, if present, is the fully qualified Internet host name
attribute: **port**	**port** is *implied* and, if present, is the port number of the service being tested
/SCAN/IP/SERVICES/CAT[@value="darxite"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required* and will be: darxite-banner ... Darxite Web server banner
attribute: **severity**	**severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/SERVICES/CAT[@value="Firewall"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required* and will be: fw-check ... Firewall service details
attribute: **severity**	**severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/SERVICES/CAT[@value="ftpd"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required* and will be one of the following: ftpd-banner ... FTP daemon banner ftpd-bounce ... FTP daemon allows relays/bounces ftpd-stat ... FTP daemon supports STAT function
attribute: **severity**	**severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/SERVICES/CAT[@value="http"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required* and will be one of the following: httpd_version ... HTTP daemon version details https_ssl_certificate ... HTTP deamon ssl certificate details https_version ... SSL Web server version
attribute: **severity**	**severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/SERVICES/CAT[@value="irc"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required* and will be: ircd-banner ... IRC daemon banner
attribute: **severity**	**severity** is *implied* and, if present, is an integer between 1 and 5

/SCAN/IP/SERVICES/CAT[@value="linuxconf"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required* and will be: linuxconf-banner.....linuxconf daemon banner
attribute: **severity**	**severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/SERVICES/CAT[@value="mysql"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required* and will be: mysql-banner .....MySQL daemon banner
attribute: **severity**	**severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/SERVICES/CAT[@value="netbios"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required* and will be one of the following: mac_address.....MAC address nbtstat.....NetBIOS name information
attribute: **severity**	**severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/SERVICES/CAT[@value="os"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required* and will be: os.....Operating system information
attribute: **severity**	**severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/SERVICES/CAT[@value="pop2"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required* and will be one of the following: pop2-banner.....POP v2 daemon banner pop3-banner.....POP v3 daemon banner
attribute: **severity**	**severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/SERVICES/CAT[@value="PortScan"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required* and will be one of the following: scan_tcp.....Open TCP services scan_udp.....Open UDP services
attribute: **severity**	**severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/SERVICES/CAT[@value="Protocols"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required* and will be: proto_disco.....Protocols in use
attribute: **severity**	**severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/SERVICES/CAT[@value="rpc"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required* and will be one of the following: rpcinfo.....RPC information scan_rpc.....RPC services scan_hidden_rpc.....Hidden RPC services
attribute: **severity**	**severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/SERVICES/CAT[@value="smb"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required* and will be: scan_smb.....NetBIOS service open
attribute: **severity**	**severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/SERVICES/CAT[@value="smtp"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required* and will be: smtp-banner.....SMTP daemon banner
attribute: **severity**	**severity** is *implied* and, if present, is an integer between 1 and 5

/SCAN/IP/SERVICES/CAT[@value="ssh"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value** attribute: **severity**	**value** is *required* and will be: sshd-banner ..... SSH daemon banner **severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/SERVICES/CAT[@value="telnetd"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value** attribute: **severity**	**value** is *required* and will be one of the following: telnetd-banner ..... Telnet daemon banner **severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/SERVICES/CAT[@value="VNC"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value** attribute: **severity**	**value** is *required* and will be one of the following: vnc-banner ..... VNC daemon banner **severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/SERVICES/CAT[@value="X11"]/SERVICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value** attribute: **severity**	**value** is *required* and will be one of the following: x11-banner ..... X11 server daemon banner **severity** is *implied* and, if present, is an integer between 1 and 5
/SCAN/IP/SERVICES/CAT/SERVICE/TITLE	(#PCDATA)*
/SCAN/IP/SERVICES/CAT/SERVICE/DIAGNOSIS	(#PCDATA)*
/SCAN/IP/SERVICES/CAT/SERVICE/CONSEQUENCE	(#PCDATA)*
/SCAN/IP/SERVICES/CAT/SERVICE/SOLUTION	(#PCDATA)*
/SCAN/IP/SERVICES/CAT/SERVICE/RESULT	(#PCDATA)*
attribute: **format**	**format** is *implied* and, if present, will be "table," indicating that the results are a table whose columns will be separated by spaces, and whose rows will be separated by new-line characters
/SCAN/IP/VULNS	(CAT)+

/SCAN/IP/VULNS/CAT	(INFO+ | SERVICE+ | VULN+ | PRACTICE+) *NOTE: When CAT is a child of VULNS, it can only contain VULN elements.*
attribute: **value**	**value** is *required* and will be one of the following: accounts ..... Irix object server daemon vulnerabilities afp ..... Apple File Protocol vulnerabilities backdoor ..... Back doors and Trojan horses backup ..... Backup system vulnerabilities bordermanager ..... Novell BorderManager vulnerabilities cgi ..... CGI vulnerabilities chat ..... Chat services vulnerabilities chronos ..... Load balancer discovery cisco ..... Cisco vulnerabilities dns ..... DNS vulnerabilities finger ..... Finger vulnerabilities firewall ..... Firewall vulnerabilities ftpd ..... FTP vulnerabilities gopher ..... Gopher vulnerabilities http ..... HTTP vulnerabilities ibmdb2 ..... IBM db2 vulnerabilities icmp ..... ICMP vulnerabilities identd ..... identd vulnerabilities imapd ..... IMAP vulnerabilities innd ..... innd vulnerabilities IRC ..... IRC vulnerabilities lcdproc ..... LCDProc vulnerabilities ldap ..... LDAP vulnerabilities linuxconf ..... linuxconf vulnerabilities lpd ..... lpd vulnerabilities mssql ..... Microsoft SQL server vulnerabilities named ..... named vulnerabilities netbios ..... NetBIOS vulnerabilities netmeeting ..... Microsoft NetMeeting vulnerabilities oracle ..... Oracle vulnerabilities pop3 ..... POP3 vulnerabilities postgresql ..... PostgreSQL vulnerabilities proxy ..... Proxy vulnerabilities remote-administration ..... Remote administration vulnerabilities rexec ..... rexec vulnerabilities rip ..... RIP routing table vulnerabilities rlogin ..... rlogin vulnerabilities rpc ..... RPC vulnerabilities rsh ..... rsh vulnerabilities sendfile ..... sendfile vulnerabilities smtp ..... SMTP vulnerabilities snmp ..... SNMP vulnerabilities ssh ..... SSH vulnerabilities stat ..... systat, netstat and perfcopilot vulnerabilities streaming ..... Streaming media vulnerabilities TCP ..... TCP small services vulnerabilities tcp ..... TCP implementation vulnerabilies telnetd ..... telnetd vulnerabilities tftp ..... tftp vulnerabilities UDP ..... UDP small services vulnerabilities vnc ..... VNC vulnerabilities webanalyzer ..... Web site vulnerabilities windows ..... Microsoft Windows vulnerabilities xfs ..... X-Font Server vulnerabilities X-Windows ..... X-Windows vulnerabilities
attribute: **misc**	**misc** is implied and, if present, will be "over ssl," indicating that the connection is encrypted using SSL
attribute: **fqdn**	**fqdn** is *implied* and, if present, is the fully qualified Internet host name
attribute: **port**	**port** is *implied* and, if present, is the port number of the VULN being tested

/SCAN/IP/VULNS/CAT/VULN	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required*. It will be a description of one of the network vulnerabilities that Qualys has identified. The complete list is far too long to be included here, and moreover, it is constantly being updated.
attribute: **severity**	**severity** is *required* and is an integer between 1 and 5
attribute: **esoid**	**esoid** is *implied* and, if present, is an eSecurityOnline vulnerability ID
attribute: **cveid**	**cveid** is *implied* and, if present, is a CVE ID
/SCAN/IP/VULNS/CAT/VULN/TITLE	(#PCDATA)*
/SCAN/IP/VULNS/CAT/VULN/DIAGNOSIS	(#PCDATA)*
/SCAN/IP/VULNS/CAT/VULN/CONSEQUENCE	(#PCDATA)*
/SCAN/IP/VULNS/CAT/VULN/SOLUTION	(#PCDATA)*
/SCAN/IP/VULNS/CAT/VULN/RESULT	(#PCDATA)*
attribute: **format**	**format** is *implied* and, if present, will be "table," indicating that the results are a table whose columns will be separated by spaces, and whose rows will be separated by new-line characters
/SCAN/IP/PRACTICES	(CAT)+
/SCAN/IP/PRACTICES/CAT	(INFO+ | SERVICE+ | VULN+ | PRACTICE+) *NOTE: When CAT is a child of VULNS, it can only contain VULN elements.*
attribute: **value**	**value** is *required*. For the complete list of possible values, see above under **/SCAN/IP/VULNS/CAT**.
attribute: **fqdn**	**fqdn** is *implied* and, if present, is the fully qualified Internet host name
attribute: **misc**	**misc** is implied and, if present, will be "over ssl," indicating that the connection is encrypted using SSL
attribute: **port**	**port** is *implied* and, if present, is the port number of the VULN being tested
/SCAN/IP/PRACTICES/CAT/PRACTICE	(TITLE,DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,RESULT?)
attribute: **value**	**value** is *required*. It will be a description of one of the "practices" (*potential* vulnerabilities) that Qualys has identified. The complete list is far too long to be included here, and moreover, it is constantly being updated.
attribute: **severity**	**severity** is *required* and is an integer between 1 and 5
attribute: **esoid**	**esoid** is *implied* and, if present, is an eSecurityOnline vulnerability ID
attribute: **cveid**	**cveid** is *implied* and, if present, is a CVE ID
/SCAN/IP/PRACTICES/CAT/PRACTICE/TITLE	(#PCDATA)*
/SCAN/IP/PRACTICES/CAT/PRACTICE/DIAGNOSIS	(#PCDATA)*
/SCAN/IP/PRACTICES/CAT/PRACTICE/CONSEQUENCE	(#PCDATA)*
/SCAN/IP/PRACTICES/CAT/PRACTICE/SOLUTION	(#PCDATA)*
/SCAN/IP/PRACTICES/CAT/PRACTICE/RESULT	(#PCDATA)*
attribute: **format**	**format** is *implied* and, if present, will be "table," indicating that the results are a table whose columns will be separated by spaces, and whose rows will be separated by new-line characters

Appendix C – Sample XML report from scan.php

```
<?xml version="1.0" ?>
<!DOCTYPE SCAN SYSTEM "https://www.us.qualys.com/scan-1.dtd">
<SCAN value="scan/993593085.18806">
<HEADER>
    <KEY value="USERNAME">user</KEY>
    <KEY value="COMPANY">Qualys</KEY>
    <KEY value="DATE">20010627000606</KEY>
    <KEY value="TITLE">MSP API Manual vulnerability analysis on 1.2.3.4</KEY>
    <KEY value="TARGET">1.2.3.4</KEY>
    <KEY value="DURATION">00:03:37</KEY>
    <KEY value="SCAN_HOST">195.68.109.142</KEY>
    <KEY value="NBHOST_ALIVE">1</KEY>
    <KEY value="NBHOST_TOTAL">1</KEY>
</HEADER>
<IP value="1.2.3.4" name="host.fqdn">
  <INFOS>
    <CAT value="route">
      <INFO value="traceroute">
        <TITLE>Traceroute</TITLE>
        <RESULT><![CDATA[  1  (195.68.109.129)  2.267 ms
2  (195.68.118.13)  2.993 ms
3  (195.68.85.188)  5.208 ms
4  (213.41.1.233)  3.112 ms
5  (194.250.134.1)  3.621 ms
6  (194.250.136.62)  3.543 ms
7  (212.74.67.25)  3.885 ms
8  (212.74.67.194)  12.379 ms
9  (212.74.64.174)  79.534 ms
10  (1.2.3.4)  83.736 ms]]></RESULT>
      </INFO>
    </CAT>
    <CAT value="whois">
      <INFO value="whois_isp">
        <TITLE>Internet Service Provider</TITLE>
        <RESULT><![CDATA[The ISP network handle is:  NET-SPRINT-INNET5

ISP Network description:
Sprint
Government Systems Division
13221 Woodland Park Road
Herndon, VA  22071
US]]></RESULT>
      </INFO>
      <INFO value="whois_network">
        <TITLE>Target Network Information</TITLE>
        <RESULT><![CDATA[The network handle is:  NETBLK-PBI-NET-5

Network description:
Pacific Bell Internet Services,Inc.
1.2.3.4 - 4.5.6.7
BASIC DSL POOLS (NETBLK-PBI-CUSTNET-8878) PBI-CUSTNET-8878
1.2.3.4 - 4.5.6.7]]></RESULT>
      </INFO>
    </CAT>
  </INFOS>
  <SERVICES>
```

```
    <CAT value="PortScan">
      <SERVICE value="scan_tcp" severity="1">
        <TITLE>Open TCP Services List</TITLE>
        <DIAGNOSIS><![CDATA[The port scanner enables unauthorized users with the appropriate tools to
draw a map of all services on this host that can be accessed from the Internet.  The test was carried
out with a ""stealth"" port scanner so that the server does not log real connections.]]></DIAGNOSIS>
        <CONSEQUENCE><![CDATA[Unauthorized users can exploit this information to test vulnerabilities in
each of the open services.]]></CONSEQUENCE>
        <SOLUTION><![CDATA[Shut down any unknown or unused service on the list.  If you have difficulty
working out which service is provided by which process or program, contact the <A
HREF="mailto:technical-support@qualys.com">Qualys Emergency Response Team</A> or visit the <A
HREF="http://www.cert.org" TARGET="cert-website">CERT website</A> for more information about commercial
and opensource Intrusion Detection Systems available for detecting port scanners of this
kind.]]></SOLUTION>
        <RESULT format="table"><![CDATA[Port  IANA Assigned Ports/Services  Description    Service
Detected
25      smtp    Simple Mail Transfer   smtp
22      ssh     SSH Remote Login Protocol     ssh
110     pop3    Post Office Protocol - Version 3      pop3
6010    x11     X Window System        unknown]]></RESULT>
      </SERVICE>
      <SERVICE value="scan_udp" severity="1">
        <TITLE>Open UDP Services List</TITLE>
        <DIAGNOSIS><![CDATA[A port scanner was used to draw a map of all the UDP services on this host
that can be accessed from the Internet.]]></DIAGNOSIS>
        <CONSEQUENCE><![CDATA[Unauthorized users can exploit this information to test vulnerabilities in
each of the open services.]]></CONSEQUENCE>
        <SOLUTION><![CDATA[Shut down any unknown or unused service on the list.  If you have difficulty
working out which service is provided by which process or program, contact the <A
HREF="mailto:technical-support@qualys.com">Qualys Emergency Response Team</A> or visit the <A
HREF="http://www.cert.org" TARGET="cert-website">CERT website</A> for more information about commercial
and opensource Intrusion Detection Systems available for detecting port scanners of this
kind.]]></SOLUTION>
        <RESULT format="table"><![CDATA[Port  Name    Description
9       discard Discard
67      bootps  Bootstrap Protocol Server
68      bootpc  Bootstrap Protocol Client]]></RESULT>
      </SERVICE>
    </CAT>
    <CAT value="Protocols">
      <SERVICE value="proto_disco" severity="1">
        <TITLE>Open Protocol List</TITLE>
        <DIAGNOSIS><![CDATA[Unauthorized remote users can obtain the list of protocols used on this
host.]]></DIAGNOSIS>
        <CONSEQUENCE><![CDATA[Unauthorized remote users can exploit this information to test
vulnerabilities in each of the available protocols.]]></CONSEQUENCE>
        <SOLUTION><![CDATA[Disable any protocols not required on this host.]]></SOLUTION>
        <RESULT format="table"><![CDATA[1     icmp
4       ipencap
6       tcp
17      udp
39      idpr-cmtp
94      ipip]]></RESULT>
      </SERVICE>
    </CAT>
    <CAT value="os">
      <SERVICE value="os" severity="2">
        <TITLE>Operating System</TITLE>
        <DIAGNOSIS><![CDATA[The Operating System of the host using TCP/IP fingerprinting can be
identified from a remote system. All underlying operating system TCP/IP stacks have subtle differences
that may be identified by sending specially crafted TCP packets.  According to the results of this
""fingerprinting"" technique, the Operating System version is among those listed below.]]></DIAGNOSIS>
        <CONSEQUENCE><![CDATA[Unauthorized remote users can exploit this information to test
vulnerabilities in each of the available protocols.]]></CONSEQUENCE>
        <SOLUTION><![CDATA[Disable any protocols not required on this host.]]></SOLUTION>
        <RESULT><![CDATA[Linux 2.1.19 - 2.2.17,Linux kernel 2.2.13,Linux 2.2.14,Linux 2.2.19 on a DEC
Alpha]]></RESULT>
      </SERVICE>
    </CAT>
```



```
    <CAT value="pop3" port="110">
      <SERVICE value="pop3-banner" severity="2">
        <TITLE>POP3 Banner</TITLE>
        <DIAGNOSIS><![CDATA[The Operating System of the host using TCP/IP fingerprinting can be
identified from a remote system. All underlying operating system TCP/IP stacks have subtle differences
that may be identified by sending specially crafted TCP packets.  According to the results of this
""fingerprinting"" technique, the Operating System version is among those listed below.]]></DIAGNOSIS>
        <CONSEQUENCE><![CDATA[Unauthorized remote users can exploit this information to test
vulnerabilities in each of the available protocols.]]></CONSEQUENCE>
        <SOLUTION><![CDATA[Disable any protocols not required on this host.]]></SOLUTION>
        <RESULT><![CDATA[+OK Qpopper (version 4.0.3) at thats.unpossible.com starting.]]></RESULT>
      </SERVICE>
    </CAT>
    <CAT value="smtp" port="25">
      <SERVICE value="smtp-banner" severity="2">
        <TITLE>SMTP Banner</TITLE>
        <DIAGNOSIS><![CDATA[The Operating System of the host using TCP/IP fingerprinting can be
identified from a remote system. All underlying operating system TCP/IP stacks have subtle differences
that may be identified by sending specially crafted TCP packets.  According to the results of this
""fingerprinting"" technique, the Operating System version is among those listed below.]]></DIAGNOSIS>
        <CONSEQUENCE><![CDATA[Unauthorized remote users can exploit this information to test
vulnerabilities in each of the available protocols.]]></CONSEQUENCE>
        <SOLUTION><![CDATA[Disable any protocols not required on this host.]]></SOLUTION>
        <RESULT><![CDATA[220 unpossible.com ESMTP]]></RESULT>
      </SERVICE>
    </CAT>
    <CAT value="ssh" port="22">
      <SERVICE value="sshd-banner" severity="1">
        <TITLE>SSH Banner</TITLE>
        <DIAGNOSIS><![CDATA[The Operating System of the host using TCP/IP fingerprinting can be
identified from a remote system. All underlying operating system TCP/IP stacks have subtle differences
that may be identified by sending specially crafted TCP packets.  According to the results of this
""fingerprinting"" technique, the Operating System version is among those listed below.]]></DIAGNOSIS>
        <CONSEQUENCE><![CDATA[Unauthorized remote users can exploit this information to test
vulnerabilities in each of the available protocols.]]></CONSEQUENCE>
        <SOLUTION><![CDATA[Disable any protocols not required on this host.]]></SOLUTION>
        <RESULT><![CDATA[SSH-1.99-OpenSSH_2.5.2p2]]></RESULT>
      </SERVICE>
    </CAT>
  </SERVICES>
  <VULNS>
    <CAT value="UDP">
      <VULN value="udp_small_services" severity="2" cveid="CVE-1999-0103">
        <TITLE>UDP Test-Services</TITLE>
        <DIAGNOSIS><![CDATA[This system is running UDP services that are generally used for networking
testing purposes only (7 echo, 9 discard, 13 time, 17 quote of the day, 19 chargen, 37 daytime).  We
would recommend that no information be disclosed (even the current server time).  Moreover, on older
Operating Systems, Echo and chargen or other combinations of UDP services can be used in tandem to flood
the server.  For example, with attacks such as UDP bomb or UDP packet storm.]]></DIAGNOSIS>
        <CONSEQUENCE><![CDATA[Unauthorized users can gather information about the server or cause a
Denial of Service, depending the on TCP/IP stack being run.]]></CONSEQUENCE>
        <SOLUTION><![CDATA[Disable any UDP service which is not required on the server.]]></SOLUTION>
        <RESULT><![CDATA[Port list:
9]]></RESULT>
      </VULN>
    </CAT>
    <CAT value="icmp">
      <VULN value="icmp_time" severity="1" cveid="CAN-1999-0524">
        <TITLE>ICMP Timestamp Request</TITLE>
        <DIAGNOSIS><![CDATA[ICMP ("Internet Control and Error Message Protocol") is a protocol
encapsulated in IP packets. Its principal purpose is to provide a protocol layer able to inform gateways
of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program
for determining if a host is up or down.  It uses ICMP echo packets. ICMP timestamp packets are used to
synchronise clocks between hosts.]]></DIAGNOSIS>
        <CONSEQUENCE><![CDATA[Unauthorized users can obtain information about your network by sending
ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some
internal daemons use this value to calculate ID or sequence numbers (i.e. on SunOS
servers).]]></CONSEQUENCE>
        <SOLUTION><![CDATA[Filter external ICMP queries so that your firewall/router filters out all
types of incoming ICMP packets (You may want to allow ICMP Don't Fragment packets and probably ICMP
echo/reply if you want to allow pinging of hosts). Contact your network consultants for advice since
this issue impact the overall network security.]]></SOLUTION>
        <RESULT><![CDATA[time stamp of host: 21:59:33 GMT]]></RESULT>
      </VULN>
    </CAT>
```



```
    <CAT value="tcp">
      <VULN value="ip_id_pred" severity="1" cveid="GENERIC-MAP-NOMATCH">
        <TITLE>Predictable IP ID field Vulnerability</TITLE>
        <DIAGNOSIS><![CDATA[<DD>The remote host uses non-random IP ID values, that is, it is possible to
predict the next value of the ip_id field of the IP packets sent by this host.]]></DIAGNOSIS>
        <CONSEQUENCE><![CDATA[<DD>An attacker may use this feature to determine if the remote host sent
a packet in reply to another request. When combined with IP source address spoofing this may be used for
anonymous portscanning and other things (where the attacker's real IP address cannot be
determined).]]></CONSEQUENCE>
        <SOLUTION><![CDATA[Contact your vendor for a patch.]]></SOLUTION>
      </VULN>
    </CAT>
  </VULNS>
</IP>
</SCAN>
```


Appendix D – DTD for scan_report_list.php

```
<!-- QUALYS SCAN_REPORT_LIST DTD -->
<!-- $Id: scan_report_list.dtd,v 1.2 2001/06/22 14:26:27 ben Exp $ -->
<!ELEMENT SCAN_REPORT_LIST (SCAN_REPORT*)>
<!ATTLIST SCAN_REPORT_LIST
          user CDATA #REQUIRED
          from CDATA #REQUIRED
          to CDATA #REQUIRED
          with_target CDATA #IMPLIED>

<!ELEMENT SCAN_REPORT EMPTY>
<!ATTLIST SCAN_REPORT
          ref CDATA #REQUIRED
          date CDATA #REQUIRED
          target CDATA #REQUIRED>

<!-- EOF -->
```

Appendix E – XPaths for scan_report_list.php

XPath	element specifications / notes
/SCAN_REPORT_LIST	(SCAN_REPORT*)
attribute: **user**	**user** is *required* and is the Qualys username
attribute: **from**	**from** is *required* and is the oldest date (in YYYYMMDDHHMMSS format) in the range of available scans
attribute: **to**	**to** is *required* and is the newest date (in YYYYMMDDHHMMSS format) in the range of available scans
attribute: **with_target**	**with_target** is *implied* and, if present, is an IP address that will be found in each of the reports in the list
/SCAN_REPORT_LIST/SCAN_REPORT	EMPTY
attribute: **ref**	**ref** is *required* and is the reference, or key, for the scan
attribute: **date**	**date** is *required* and is the date when the scan was performed (in YYYYMMDDHHMMSS format)
attribute: **target**	**target** is *required* and is the IP address (or range of IP addresses) upon which the scan was performed

Appendix F – Sample XML report from scan_report_list.php

```
<?xml version="1.0" ?>
<!DOCTYPE SCAN_REPORT_LIST SYSTEM "https://www.us.qualys.com/scan_report_list.dtd">
<SCAN_REPORT_LIST user="some_user" from="20010320012752" to="20010628022752">
<SCAN_REPORT ref="scan/993593085.18806" date="20010628022752" target="1.2.3.4"  />
<SCAN_REPORT ref="scan/993593085.18777" date="20010320012752" target="1.2.3.4"  />
</SCAN_REPORT_LIST>
```

Appendix G – DTD for map.php

```
<!-- QUALYS MAP DTD -->
<!-- $Id: map.dtd,v 1.1 2001/02/09 12:38:06 pes Exp $ -->

<!ELEMENT MAP (IP+)>
<!ATTLIST MAP
        value CDATA #REQUIRED>

<!ELEMENT IP ((PORT+,LINK*)|LINK+)?>
<!ATTLIST IP
        value CDATA #REQUIRED
        name CDATA #IMPLIED
        type CDATA #IMPLIED
        os CDATA #IMPLIED>

<!ELEMENT PORT (#PCDATA)*>
<!ATTLIST PORT
        value CDATA #REQUIRED>

<!ELEMENT LINK EMPTY>
<!ATTLIST LINK
        value CDATA #REQUIRED>
```

Appendix H – XPaths for map.php

XPath	element specifications / notes
/MAP	(IP+)
/MAP/IP	((PORT+,LINK*) | LINK+)?
attribute: **value**	**value** is *required* and is an IP address
attribute: **name**	**name** is *implied* and, if present, is an Internet host name
attribute: **type**	**type** is *implied* and, if present, will be "router," indicating that the device is a router
attribute: **os**	**os** is *implied* and, if present, is a string indicating the device's operating system
/MAP/IP/PORT	(#PCDATA)*
attribute: **value**	**value** is *required* and will be one of the following: 21 ..... FTP 22 ..... SSH 23 ..... Telnet 25 ..... SMTP 53 ..... DNS 80 ..... HTTP 110 ..... POP3 135 ..... NetBIOS 139 ..... NetBIOS 443 ..... HTTPS
/MAP/IP/LINK	EMPTY
attribute: **value**	**value** is *required*. If /MAP/IP[@type="router"] then there will be one /MAP/IP/LINK per host found in the domain that is served by that router. In this case, **value** will be the IP address of the host that this router serves. Otherwise, **value** is the IP address of the router that serves this host; if **value** is empty in this case, it means that the router was protected by a firewall or otherwise shielded from discovery.

Appendix I – Sample XML report from map.php

```
<?xml version="1.0" ?>
<!DOCTYPE MAP SYSTEM "https://www.us.qualys.com/map.dtd">

<MAP value="user_account/map/2001.06.28.02:13:20">
<IP value="194.55.109.12" name="gw.qualys-test.com" os="Cisco IOS 11.3">
<LINK value="194.55.110.6"></LINK>
</IP>
<IP value="194.55.109.13" name="ntproxyhost.qualys-test.com" os="Linux 2.0.38">
<LINK value="194.55.110.6"></LINK>
</IP>
<IP value="194.55.109.14" name="trip.qualys-test.com" os="Solaris 8">
<LINK value="194.55.110.6"></LINK>
</IP>
<IP value="194.55.109.15" name="retrieval.qualys-test.com" os="SunOS 4.1.4U">
<LINK value="194.55.110.6"></LINK>
</IP>
<IP value="194.55.109.16" name="sales1.qualys-test.com" os="Irix 6.4">
<LINK value="194.55.110.6"></LINK>
</IP>
<IP value="194.55.110.6" type="router">
<LINK value="194.55.109.12"></LINK>
<LINK value="194.55.109.13"></LINK>
<LINK value="194.55.109.14"></LINK>
<LINK value="194.55.109.15"></LINK>
<LINK value="194.55.109.16"></LINK>
</IP>
<IP value="212.85.128.51" name="www.qualys.com" os="Linux">
<PORT value="80"></PORT>
<LINK value="212.85.128.254"></LINK>
</IP>
<IP value="212.85.128.254" type="router">
<LINK value="212.85.128.51"></LINK>
</IP>
</MAP>
```

Appendix J – DTD for enrollment.php

```
<!ELEMENT REGISTRATION (USERINFO|ERROR)>

<!ELEMENT USERINFO (USERNAME,SERVICE_LEVEL,PASSWORD?)>

<!ELEMENT USERNAME (#PCDATA)>

<!ELEMENT SERVICELEVEL (#PCDATA)>

<!--PASSWORD element optional; it is only included if “returnpassword” name-value pair set to “yes” -->
<!ELEMENT PASSWORD (#PCDATA)>

<!ELEMENT ERROR (FIELD+,SUMMARY)>

<!ELEMENT FIELD (#PCDATA)*>
<!ATTLIST FIELD
        name (prefix|firstname|lastname|title|phone|email|company|addr1|
              city|zipcode|country|state|sleve1|type|domain|targetip|addr2|fax) #REQUIRED
        error_type (invalid|missing) #REQUIRED>

<!ELEMENT SUMMARY (#PCDATA)>
```

Appendix K – XPaths for enrollment.php

XPath	element specifications / notes
/REGISTRATION	(USERINFO|ERROR)
/REGISTRATION/USERINFO	(USERNAME,SERVICE_LEVEL,PASSWORD?)
/REGISTRATION/USERINFO/USERNAME	(#PCDATA)
/REGISTRATION/USERINFO/PASSWORD	(#PCDATA) *NOTE: only returned if "returnpassword" value is set to "yes"*
/REGISTRATION/USERINFO/SERVICE_LEVEL	(#PCDATA)
/REGISTRATION/ERROR	(FIELD+,SUMMARY)
/REGISTRATION/ERROR/FIELD	(#PCDATA)*
attribute: **name** attribute: **error_type**	**name** is *required* and is the field that is in error. **error_type** is *required* and will be one of the following: missing ..... A required field was missing invalid ..... The value given for a field does not meet the specification
/REGISTRATION/ERROR/SUMMARY	(#PCDATA)

Appendix L – Acceptable “state” and “country” values for enrollment.php

Acceptable values for “state”

"No State" | "Alabama" | "Alaska" | "Arizona" | "Arkansas" | "Armed Forces Asia" | "Armed Forces Europe" | "Armed Forces Pacific" | "California" | "Colorado" | "Connecticut" | "Delaware" | "District of Columbia" | "Florida" | "Georgia" | "Hawaii" | "Idaho" | "Illinois" | "Indiana" | "Iowa" | "Kansas" | "Kentucky" | "Louisiana" | "Maine" | "Maryland" | "Massachusetts" | "Michigan" | "Minnesota" | "Mississippi" | "Missouri" | "Montana" | "Nebraska" | "Nevada" | "New Hampshire" | "New Jersey" | "New Mexico" | "New York" | "North Carolina" | "North Dakota" | "Ohio" | "Oklahoma" | "Oregon" | "Pennsylvania" | "Rhode Island" | "South Carolina" | "South Dakota" | "Tennessee" | "Texas" | "Utah" | "Vermont" | "Virginia" | "Washington" | "West Virginia" | "Wisconsin" | "Wyoming"

Acceptable values for “country”

"Afghanistan" | "Albania" | "Algeria" | "Andorra" | "Angola" | "Anguilla" | "Antartica" | "Antigua and Barbuda" | "Argentina" | "Armenia" | "Aruba" | "Australia" | "Austria" | "Azerbaijan" | "Bahamas" | "Bahrain" | "Bangladesh" | "Barbados" | "Belarus" | "Belgium" | "Belize" | "Benin" | "Bermuda" | "Bhutan" | "Bolivia" | "Bosnia-Herzegovina" | "Botswana" | "Bouvet Island" | "Brazil" | "British Indian Ocean Territory" | "Brunei Darussalam" | "Bulgaria" | "Burkina Faso" | "Burundi" | "Cambodia" | "Cameroon" | "Canada" | "Cape Verde" | "Cayman Islands" | "Central African Republic" | "Chad" | "Chile" | "China" | "Christmas Island" | "Cocos (Keeling) Islands" | "Colombia" | "Comoros" | "Congo" | "Cook Islands" | "Costa Rica" | "Cote D'Ivoire" | "Croatia" | "Cuba" | "Cyprus" | "Czech Republic" | "Denmark" | "Djibouti" | "Dominica" | "Dominican Republic" | "East Timor" | "Ecuador" | "Egypt" | "El Salvador" | "Equatorial Guinea" | "Estonia" | "Ethiopia" | "Faeroe Islands" | "Falkland Islands (Malvinas)" | "Fiji" | "Finland" | "France" | "French Guiana" | "French Polynesia" | "French Southern Territories" | "Gabon" | "Gambia" | "Georgia" | "Germany" | "Ghana" | "Gibraltar" | "Greece" | "Greenland" | "Grenada" | "Guadeloupe" | "Guatemala" | "Guernsey" | "Guinea" | "Guinea-Bissau" | "Guyana" | "Haiti" | "Heard and McDonald Islands" | "Honduras" | "Hong Kong" | "Hungary" | "Iceland" | "India" | "Indonesia" | "Iran (Islamic Republic of)" | "Iraq" | "Ireland" | "Isle of Man" | "Israel" | "Italy" | "Jamaica" | "Japan" | "Jersey" | "Jordan" | "Kazakhstan" | "Kenya" | "Kiribati" | "Korea" | "Korea" | "Kuwait" | "Kyrgyzstan" | "Lao Peoples Democratic Republi" | "Latvia" | "Lebanon" | "Lesotho" | "Liberia" | "Libyan Arab Jamahiriya" | "Liechtenstein" | "Lithuania" | "Luxembourg" | "Macau" | "Madagascar" | "Malawi" | "Malaysia" | "Maldives" | "Mali" | "Malta" | "Marshall Islands" | "Martinique" | "Mauritania" | "Mauritius" | "Mexico" | "Micronesia" | "Moldova" | "Monaco" | "Mongolia" | "Montserrat" | "Morocco" | "Mozambique" | "Myanmar" | "Namibia" | "Nauru" | "Nepal" | "Netherland Antilles" | "Netherlands" | "Neutral Zone (Saudi/Iraq)" | "New Caledonia" | "New Zealand" | "Nicaragua" | "Niger" | "Nigeria" | "Niue" | "Norfolk Island" | "Northern Mariana Islands" | "Norway" | "Oman" | "Pakistan" | "Palau" | "Panama Canal Zone" | "Panama" | "Papua New Guinea" | "Paraguay" | "Peru" | "Philippines" | "Pitcairn" | "Poland" | "Portugal" | "Puerto Rico" | "Qatar" | "Reunion" | "Romania" | "Russia" | "Rwanda" | "Saint Kitts and Nevis" | "Saint Lucia" | "Samoa" | "San Marino" | "Sao Tome and Principe" | "Saudi Arabia" | "Senegal" | "Seychelles" | "Sierra Leone" | "Singapore" | "Slovak Republic" | "Slovenia" | "Solomon Islands" | "Somalia" | "South Africa" | "Spain" | "Sri Lanka" | "St. Helena" | "St. Pierre and Miquelon" | "St. Vincent and the Grenadines" | "Sudan" | "Suriname" | "Svalbard and Jan Mayen Islands" | "Swaziland" | "Sweden" | "Switzerland" | "Syrian Arab Republic" | "Taiwan" | "Tajikistan" | "Tanzania" | "Thailand" | "Togo" | "Tokelau" | "Tonga" | "Trinidad and Tobago" | "Tunisia" | "Turkey" | "Turkmenistan" | "Turks and Caicos Islands" | "Tuvalu" | "U.S. Minor Outlying Islands" | "Uganda" | "Ukraine" | "United Arab Emirates" | "United Kingdom" | "United States of America" | "Uruguay" | "Uzbekistan" | "Vanuatu" | "Vatican City State" | "Venezuela" | "Vietnam" | "Virgin Islands (British)" | "Wallis and Futuna Islands" | "Western Sahara" | "Yemen" | "Yugoslavia" | "Zaire" | "Zambia" | "Zimbabwe"

Appendix M – Sample XML reports from enrollment.php

Sample XML report for a successful registration:

```
<?xml version="1.0" ?>
<REGISTRATION>
<USERINFO>
<USERNAME>somelogin</USERNAME>
<SERVICE_LEVEL>qualys_full</SERVICE_LEVEL>
</USERINFO>
</REGISTRATION>
```

Sample XML report for a successful registration with returnpassword=yes:

```
<?xml version="1.0" ?>
<REGISTRATION>
<USERINFO>
<USERNAME>somelogin</USERNAME>
<PASSWORD>somepassword</PASSWORD>
<SERVICE_LEVEL>qualys_full</SERVICE_LEVEL>
</USERINFO>
</REGISTRATION>
```

Sample XML report for an unsuccessful registration:

```
<?xml version="1.0" ?>
<REGISTRATION>
<ERROR>
<FIELD name="domain" error_type="invalid">invalid domain: www.baddomain.com</FIELD>
<FIELD name="email" error_type="missing"/>
<FIELD name="addr1" error_type="missing"/>
<SUMMARY>invalid domain name, missing email address, missing first address line</SUMMARY>
</ERROR>
</REGISTRATION>
```

About Qualys

Qualys, Inc. is a leading provider of network assessment and monitoring solutions, enabling Managed Security Providers, security professionals and corporate customers to remotely and automatically audit Internet-connected networks for security vulnerabilities. Where traditional security monitoring products require customers to buy, develop and manage solutions internally, Qualys' service platform approach enables immediate, transparent and continuous security auditing and risk assessment of global networks, inside and outside the firewall. Founded in 1999 by a team of Internet security experts, Qualys is headquartered in Sunnyvale, California, with offices in France, Germany and the U.K. The company is privately financed by ABS Ventures, Bessemer Venture Partners, Trident Capital, and VeriSign, the leading provider of Internet trust services. For more information about Qualys, please visit www.qualys.com.

QUALYS, Inc.
1326 Chesapeake Terrace
Sunnyvale, CA 94089

To contact us:	
E-mail:	info@qualys.com
U.S. phone:	1-800-745-4355
International phone:	1-408-747-6000
On the Web:	www.qualys.com
For technical support:	
E-mail:	apisupport@qualys.com