Automate Your Internet Security

Frequently Asked Questions

HOW IS QUALYSMAP USEFUL?

QualysMap is a network discovery tool aimed at finding computers of a given domain and providing limited information about them. It detects devices and services running without authorization (placed by a non-authorized user). It also finds weaknesses due to DNS server and firewall misconfigurations. Networks are continually evolving and changes in firewall rules or DNS setups may allow intruders to find more information than they should.

WHAT DOES QUALYSMAP DO?

Only limited information is gathered for each host identified, so as to be the least intrusive as possible.

Information gathered for each device includes:

- Its router
- The operating system it is running
- Open TCP ports (FTP [21], SSH [22], TELNET [23], SMTP [25], DNS [53], HTTP [80], POP [110], NETBIOS [135 and 139] and HTTPS [443])

The results are displayed in graphical and table format. The table format is easier to manage when many hosts are found.

HOW DOES QUALYSMAP WORK?

QualysMap simply takes an Internet domain name, e.g. “yourname.com”. It relies on the domain’s DNS and the netblock information to find as many computers within that domain as it can.

There are many methods QualysMap uses to find hosts:

- AXFR: QualysMap identifies the name server (NS) who has authority on this domain and sends a request to list all the hosts managed by this name server. However, this request is not always allowed and must be forbidden by the administrator.

- FQDN brute force: QualysMap uses a proprietary list of roughly 100 common names (such as www, ftp) to form a list of fully qualified domain names (FQDN). QualysMap then queries the NS to find the IP addresses assigned to the FQDN.

- IP brute force: when QualysMap finds a target, it uses the IP address to determine the netblock and process the result to see if the corresponding FQDN belongs to the domain.

The TCP scan employs technology completely developed by Qualys, and OS fingerprinting is done using “nmap.”

DOES QUALYSMAP PERFORM A PING SCAN?

Yes! If we are sure that the neblock is the property of the customer (we make this test with a whois). In other cases, QualysMap will not perform a ping scan.

I KNOW I HAVE MORE MACHINES THAN ARE SHOWN BY QUALYSMAP. WHY AREN'T THEY DISPLAYED?

Some possible reasons:

- The machines are not recorded in the public DNS.
- They are recorded in the DNS, but no correctly.
- They are aliases, and their IP addresses have already been found (e.g. www.foo.com and foo.foo.com are aliases if both names point to the same IP address). QualysMap will show only one machine per IP address.

SOME MACHINES THAT I DID NOT EXPECT TO SEE ARE ON THE QUALYSMAP. WHY?

The machines are recorded in the name server, which has authority on the subscriber's domain.

HOW DO INTERNALL IP ADDRESSES SHOWS UP?

For each NS found, a module is charged to perform a brute-force on internal IP addresses. It blindly requests the names of servers, which have IP addresses in non routable reserved blocks (basically 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255 and 192.168.0.0-192.168.255.255). Of course, it does not request all the IPs, as these blocks are large, but it makes 20 requests where IPS are most likely to be found.

MY PHYSICAL NETWORK IS DIFFERENT FROM THE ONE MAPPED. WHY?

The map is not intended to represent your entire network. Rather, it presents an "outside-in" view of your network: the same way potential intruders can see it.

WHAT DOES "UNREACHABLE" MEAN FOR QUALYSMAP?

Either the machine was down when QualysMap was running, or the machine is behind a properly configured firewall. Therefore, QualysMap could not determine the router associated with the machine.

HOW DO I KNOW WHEN QUALYSMAP IS DONE?

The text "please wait while discovering" disappears from the screen.

THE JAVA APPLET IS LOADED ON THE BROWSER BUT NOTHING HAPPENS. WHY?

The first thing that QualysMap does is to gather information, most notably by querying the domain name server. QualysMap may appear inactive when the DNS server is down or very slow to respond.

QUALYSMAP APPEARS IN THE WEB BROWSER AND SEEMS TO CONTINUE RUNNING, BUT NO NEW INFORMATION IS DISPLAYED. WHY?

Big domains may take a while to process. QualysMap is still looking for new targets and there is still information remaining to be processed. Note that the activity bar on the bottom left of the QualysMap display indicates whether or not information is being processed. It will disappear when the map is finished.

I ONLY SEE A BLACK OR GRAY PAGE INSTEAD OF THE APPLET. WHY?

Your Java configuration is not correct. Two possibilities:

- Java is deactivated on your browser. Activate it in the browser options menu.
- Java is prohibited at the proxy level. Contact your system administrator.

HOW DOES QUALYSSCAN TEST A NETWORK FOR A DENIAL OF SERVICE (DoS) ATTACK WITHOUT BRINGING DOWN THE WEB SERVER?

When QualysScan tests for a host's DoS vulnerability, it sends special test packets. By analyzing host response, QualysScan can see if the host is vulnerable to a DoS attack without flooding it with traffic.

ALMOST ALL VULNERABILITY ASSESSMENT TOOLS CLAIM TO SCAN FIREWALLS, ROUTERS, AND OTHER HARDWARE IN ONE WAY OR ANOTHER. DOES QUALYSSCAN PERFORM THOSE SCANS IN ANY SPECIAL WAY?

QualysScan not only checks for well-known vulnerabilities, but it also for misconfigurations, which are additional potential security breaches. Thus, exploitable configurations, which were set up by the network administrator, are detected and highlighted for repair.

HOW DOES QUALYSSCAN AUDIT REMOTE DATABASE SERVERS?

QualysScan detects and audits databases (postgres, Oracle, MS Sq1, My Sql, Sybase) without requesting any specific login or configuration. It searches for vulnerabilities or misconfigurations, which lead to information leaks, theft of data or even intrusion and denial of service. Most vulnerability assessment tools require passwords or manual configurations to scan databases.

HOW IS QUALYSGUARD BANDWIDTH- EFFICIENT?

QualysGuard allows for a variable bandwidth load (low, medium, high, or maximum) on the machines it is scanning. Its scanners closely monitor the time-response (through RTT, response-time tests) and dynamically adjust the load according to the setting selected. Furthermore, QualysGuard will only run the scans appropriate to the type of machine scanned (e.g. no test specific to NT will run on a Linux machine).

WHAT ASSURES THE PRIVACY OF CUSTOMER INFORMATION INCLUDING SCAN INFO?

Information from the QualysGuard database is sent to the subscriber's browser via a secured 128 bits SSL connection. All subscriber reports and audit data are strongly encrypted using 64-bit blowfish CBC. The customer key is not stored and is not accessible to Qualys employees.

DOES QUALYS MAKE TAPE BACKUPS OR USE ANY OTHER FORM OF ARCHIVAL MEDIA TO PRESERVE CUSTOMER DATA?

No. For privacy purposes, Qualys does not make copies of the customers' data for archiving or any other purposes, on tape backup or any other form of archival media.

HOW DOES QUALYS ENSURE THE SECURITY OF MY STORED INFORMATION?

Our dedicated database servers are protected from remote attacks by a dedicated firewall and intrusion detection system. In addition, they are located in the center of multiple security rings on a private network that utilizes non-routable addresses.