GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Leadership Essentials for Managers (Cybersecurity Leadership 512)"
at http://www.giac.org/registration/gslc

Creating a Comprehensive Vulnerability Assessment Program for a Large Company Using QualysGuard

GSLC Gold Certification

Author: Tim Proffitt, tim@timproffitt.com

Adviser: Jeff Turner

Accepted:

© SANS Institute 2008, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

Creating a Comprehensive Vulnerability Assessment Program for a Large Company Using QualysGuard

What is Vulnerability Assessment? 3
Introduction to QualysGuard 4
Creating Security Policies and Controls 6
Categorization of Assets 8
Discovery of Assets 9
Host and Asset Configuration 10
Configuring Scanning Details 12
Report on Your Results 16
Rank Your Risks and Remediate 20
Handling Verification and False Positives 22
Compliance and Life Cycles 25
In Conclusion 27

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

What is Vulnerability Assessment?

Vulnerability Assessment, according to wikipedia.org, is the process of identifying and quantifying vulnerabilities in a system. Vulnerability assessment can be used against many different types of systems such as a home security alarm, the protection of a nuclear power plant or a military outpost. Note that vulnerability assessment is different from risk assessments even though they share some of the same commonalities. Vulnerability Assessment concerns itself with the identification of vulnerabilities, the possibilities of reducing those vulnerabilities and improving the capacity to manage future incidents. This paper will focus primarily on vulnerability assessment as it pertains to information technology infrastructure and how utilizing QualysGuard can ease the burden on your technology staff.

With today's global marketplace, companies cannot afford to tarnish their reputation with a public security incident. Corporations can suffer major financial losses if a security incident is encountered in the business. The fear of revenue loss should motivate companies to begin taking proactive measures against vulnerabilities in their infrastructure. The concept of vulnerability assessment is a critical process that should be followed in any organizations as a way to identify, assess and respond to new vulnerabilities before those vulnerabilities become a threat.

So how does a company initiate a vulnerability assessment project? There are generally a few common steps to vulnerability assessment:

- Create and obtain approval for vulnerability assessment.
- Find and inventory your systems
- Manage the collected information

© SANS Institute 2008, Author retains full rights.

- Assess the information by risk or vulnerability
- Plan to remediate.

Introduction to QualysGuard

Qualys is a security vendor (www.qualys.com) that has created a vulnerability assessment solution based on a true ASP model delivered over the Internet. The Qualys service provides hardware based IP scanning devices to be placed throughout your environment. Additionally, external Internet scanners can be used from Qualys' operations centers. Each of these hardware based scanners contact the Qualys service over SSLv3 to obtain their scanning instructions, update vulnerability detection details and transfer the raw assessment data back up to your Qualys portal.

The advantages for using Qualys are many:

- First, the tremendous amount of assessment data you will collect does not need to be retained, secured, or correlated on your disks. Qualys currently keeps assessment data for two years before rolling the data to make room for your next assessment scan. As of the writing of this document, Qualys does not place a limit on the amount of data you store in your repository. However, there is a two year retention limit from the time of the assessment scan.
- Second, Qualys provides hardware scanning appliances that are specifically crafted to perform network scanning. Your team will not need to provide, configure, secure or maintain workstations to facilitate your scanning. In larger environments where companies are using their own manual scanners, it can take considerable time patching and updating and troubleshooting each of those scanners.

© SANS Institute 2008, Author retains full rights.

Qualys removes this activity by providing a simple hardware based scanner whose only setup configuration is IP information and credentials to connect to Qualys.

- Third, all assessment data collected from any number of the appliance scanners is contained in your single portal database. Your team would not need to pull assessment data from various scanners to report on the larger picture. All of your detailed data is correlated in one location to report on as you wish.

- Fourth, Qualys maintains vulnerability signatures and automatically updates your scanning appliances. Since you can report on only those vulnerabilities that your scanner knows about, it is important to have a current and extensive vulnerability database to query against.

- Reporting off the correlated data has been streamlined from generation one type vulnerability services. The reporting options are vast and allow for any type of filtering you can request. Extracting reports has been made easy by offering PDF, XML, MHT or HTML versions.

If you are worried about the security of your assessment data leaving your premises, fear not. Data is encrypted per customer and can only be read by the accounts assigned to your team. Qualys will declare they are not able to review your assessment data. Understanding that vulnerability data requires heightened confidentiality, integrity and availability, Qualys takes several steps to secure your data. When data is transmitted to Qualys from your scanning appliances, SSLv3 is used and vulnerability data stored in the Qualys repository is encrypted using AES 256.

© SANS Institute 2008, Author retains full rights.

Creating Security Policies and Controls

In most cases, assessing vulnerabilities in the technology world requires verbal interviews with your system administrators and scanning your networks for devices. Network scanning, usually starting at the network layer of the OSI model and moving up to the application layer, will open several connection types to the target of your assessment. Typically, there are a common set of TCP and UDP ports that if successful connections are made, the device can be fingerprinted.

It is in this phase of vulnerability assessment that has the potential to cause harm. There are systems in the market today that can be rendered inoperable if targeted by a vulnerability assessment scan. In one example that I have seen, successive TCP port scans to certain IBM SAN controllers can bring down the entire disk array. Trust me; you do not want to be on phone with the CIO explaining why you were the one who brought down a critical system.

Vulnerability assessment activities must have acceptance from the highest levels of your organization. It is critical that the management team understands the importance of the assessment to the organization and give the security team the approval to perform the activities and assume the risks of scanning. Security teams that perform assessments should have a Vulnerability Assessment Policy[1] (in many companies this can be the Risk Assessment Policy) that clearly outlines:

- The authority to perform the assessment from management
- Clearly identify who can initiate the scans
- What the expected scan intervals should be (weekends or outages)
- How the data will be secured

© SANS Institute 2008, Author retains full rights.

- Frequency of reports to be consumed by management
- False positives and exclusion handling.

See appendix A for an example vulnerability assessment policy.

A security team that has been performing scans for any length of time is bound to encounter the vulnerability scan that causes an outage. Your policy is the difference between a conversation with the HR department and a conversation about where the business unit can find the posted policy. Be sure to have a finalized version of your policy highlighting executive sign off.

Additionally, a successful program will include awareness training for the system owners. Scanning will produce entries in log files that appear to be malicious in nature and it is always a good idea to let your administrators know what they can expect. Typically the administrators you educate about the vulnerability assessment tools will also be the same groups that will mitigate the patching and remediation efforts generated from the assessments. Your awareness training should include details around:

- Definition of vulnerability assessment and the company goals for utilizing the technology.
- Explanation of how the VA scanning appliance will operate
- What areas of the infrastructure will be in the assessment scope
- How false positives can be reported to your team
- Expectations around reporting and what requests can be made
- How the reports can be used to show details around the vulnerabilities and where the patches can be found
- How the technology could be used to benefit their departments
- Details around the severity levels and at what level the company will deem something mission critical

© SANS Institute 2008, Author retains full rights.

Categorization of Assets

So what do you want to scan? The simple answer is everything you can get your scanners to reach. With today's blended threats that can attack most anything running IP, you will want to know what is on your network infrastructure and how it could be compromised.

In corporate technology environments there is a common set of devices that can be broken up into manageable asset groups

- Workstations consisting of laptops, desktops UMPC and kiosks
- Servers consisting of your Windows, UNIX, Solaris, etc.
- Network Gear consisting of routers, switches, access points, load balancers video conference units, etc.
- Miscellaneous equipments consisting of network enabled printers, stand alone webcams, facility HVAC controls, shipping equipment, electronic door controls, fire alarms, audio video gear and even medical equipment.

For the sake of simplicity, this paper will assume the company we are building the vulnerability assessment program for has all of the technology managed by one technology department. In this scenario our server assessment data will be consumed by the server team, the workstation data will be consumed by the client support team, and the network data will be reviewed by the network engineering team. Our miscellaneous devices will get dispersed separate teams to handle the one off situations.

© SANS Institute 2008, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

Discovery of Assets

There are several methods for discovering company assets. The first and least painful method will be to obtain network diagrams from your network team. Network diagrams should give you a head start in discovering your network ranges, boundaries, and definitely help in identifying your network gear.

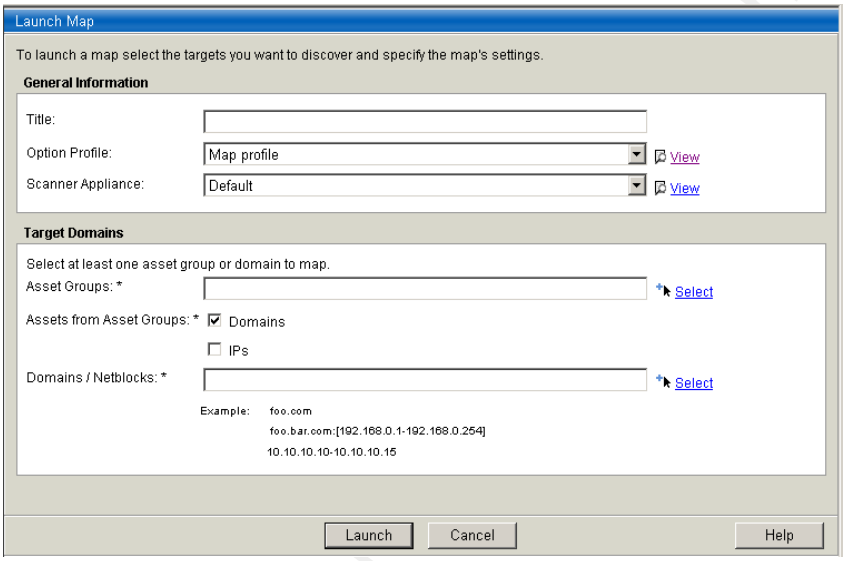
Second, meeting with your network engineers will aide greatly in understanding the scope of where your assets will be found. Vulnerability assessment scanners rely on a configuration that will allow them to scan only appropriate networks and nothing further. It should be noted here, if you point your vulnerability assessment scanner at devices that are not under your company's direct control, you may find yourself in legal trouble. Know that most corporations do not like a foreign entity scanning their devices. Be sure you document what network subnets are controlled by your company and note any that could reached but would be in violation of the policy.

Third, is to utilize mapping. The term mapping, when referring to vulnerability scanners, typically implies a very simple TCP, UDP or ICMP scan to discover devices on the network. Most internet protocol enabled devices when sent a TCP SYN packet will respond and thus identify them as an active device. Sections of any network divided into parts can be effectively mapped in a reasonable amount of time. For example, if you have a sales office that you know has been allocated the network 10.31.10.0/24, configuring your scanner to map this network would be trivial. Schedule your scanner to map 10.31.10.1 to 10.31.10.254 and the resulting map will identify your devices.

In addition to the standard mapping techniques, Qualys offers yet another option which is domain mapping. With Qualys you have the ability to enter specific IP, net blocks or registered domains. For example you could choose to

© SANS Institute 2008, Author retains full rights.

map internal.mydomain.com or external.dmz.com and allow the scanners to utilize your DNS infrastructure.



You may find, in certain scenarios, that the above discovery methods will not identify all devices. There are network based devices that do not respond to ICMP sweeps or will not have common TCP ports open. Be aware of these devices as they can still be susceptible to network based attacks and should be included in your assessments. When possible, have these IP included in your scanning configuration found in the next section.

Whether network maps, querying staff or mapping is used, you should begin to see where your assets can be found on the network.

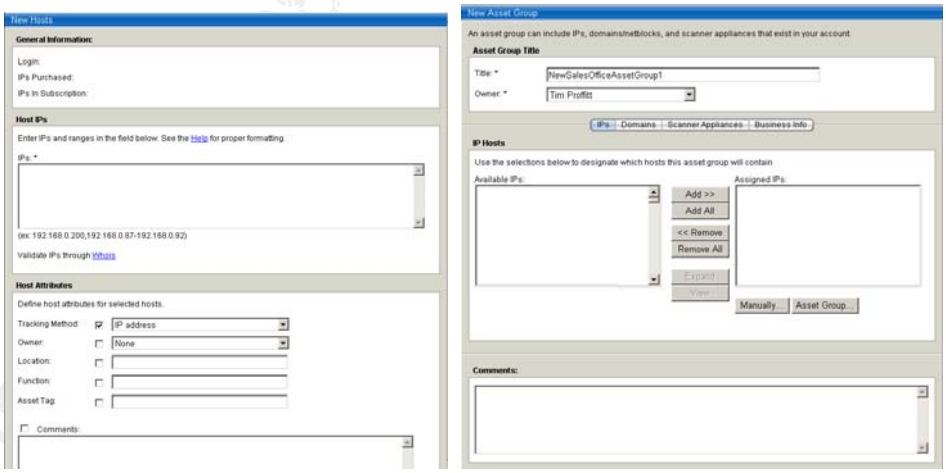
Host and Asset Configuration

At this point in your program you should have a general idea of what network segments your server, workstations, printers, routers, etc are on. Additionally, you should also have an idea of what networking equipment is going to be included in your scans.

© SANS Institute 2008, Author retains full rights.

It is at this point you can begin planning the placement of your physical scanner devices. Geographic barriers, large network segments, firewalls, business unit service level agreements, WAN links and the Internet can all play a role in how you will disperse your scanners. Your primary goal is to place scanners in strategic locations that allow for assessments of your devices in a reasonable time, without causing traffic issues. In most cases you will not want to scan through firewalls, load balancers or over the Internet. Your objective will be to divide up your targets into network segments and assign those segments to scanner appliances.

Qualys uses the concept of *Host Assets* and *Asset Groups* to bundle your devices into manageable buckets. Host assets are where you will define individual IP, IP subsets, or entire ranges. These host assets are the specific IP or ranges that your scanner can touch and additionally where licensing with Qualys will be accounted against.



Asset groups are logical containers for your host assets. Here is where you could define a group for geographic Windows servers, lump all of your network enabled printers together or create groups that places financial workstations into a group. Companies find that utilizing existing DCHP scopes are perfect containers for finding workstations and creating an creation of asset groups for core network switches and routers are beneficial for executive reporting.

© SANS Institute 2008, Author retains full rights.

To ease the complexity when it comes time to schedule scanning, Qualys allow you to select a preferred scanner device per asset group. Allowing you to assign a scanner appliance to a group allows you to schedule a scan involving large number of asset groups and choosing to default the scanning appliance assigned to the group. With this option you are ensured to optimize which scanning appliance will assess which groups. When dealing with companies that span the globe, this assignment of scanner to resources is vital.

You will find in vulnerability programs, there are devices you wish to exclude. Documenting your exclusions is an important task as these devices will not be noted in your overall risk stance. You may find that you want to exclude certain check processing printers or audio video equipment. Careful documentation is needed as most scanner appliances, after a device is excluded, will never be scanned again. Once again, check your policy on exclusions and how they are permitted to be on this exception list.

Configuring Scanning Details

Once we have defined our asset groups and know what it is we want to assess, it is time to configure a scan.

Defining a scan will require several components.

- Assets groups you are wanting to scan
- Which scanner(s) will be used
- What time frame will the scan run during
- Will authentication be used?
- What scan template will be followed

© SANS Institute 2008, Author retains full rights.

- How aggressive will you make your scans

Each company will have their own scenario when it comes to scanning but the majority of the time you will see devices sharing common characteristics get scanned together. For example: bi-monthly Windows server scans, weekly sales office desktop scans, external Internet router scans, nightly high risk database clusters, etc.

These scans can be company wide and should incorporate as many scanner devices as deemed necessary. Dividing up the assessment process among multiple scanners can significantly reduce the time for a scan to complete. However, one scanner placed in your core could meet your requirements depending on the number of devices to be assessed.

In your scan configuration you will select your target asset group(s) and determine which time will be best for assessing these devices. Server scans are typically run at night when the processing load is less, while workstation scans will kick off during the middle of the day to optimize the chance to catch users on the network. There is some talk among vulnerability experts to keep your scanning intervals a secret. Some experts note this is a good idea so that more intelligent users of the system cannot circumvent your assessments by removing systems during scheduled scan windows.

The next step in the process is defining a scan template. A scan template allows you to customize scans according to what your target devices may be for that assessment. Scan templates will involve choosing TCP or UDP protocols, whether you wish to perform a three way handshake, choosing a subset of TCP ports or all of them, how aggressive you want to scan by throttling connections per second, performing password checking for default passwords, identifying the extent of vulnerabilities you wish to check for, and choosing whether you wish to utilize authentication when checking the operating system.

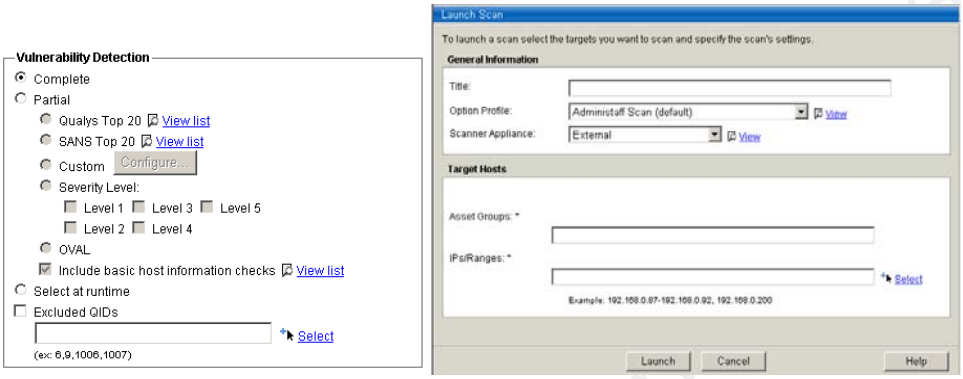
© SANS Institute 2008, Author retains full rights.

Since every environment is different, your scan template will reflect that. If you are going to scan a server segment that does not contain Apple Macintosh workstations, do you need to include those vulnerabilities? If you are going to scan your core network Cisco equipment do you need to scan all 65535 TCP and 65535 UDP ports? If you are going to scan a sales office that resides on the other side of your MPLS cloud, do you want to scan at the maximum number of processes that can be run at the same time per host? If you are going to scan severs in a DMZ, behind a firewall and from an Internet scanner, do you need to perform the scan using full OS credentials? The collective answer to the above questions is a no. Correctly configuring the template for each scenario will allow for accurate results, relevant data and scans completed in a timely fashion.

Additionally, you will want to consider authenticated versus non-authenticated scans. Authenticated scans are assessments where your scanning devices have administrative credentials on the device targeted. This authentication allows the scanner to peer deeper into the operating system. For example, Windows domain controllers require administrative rights to view sections on the registry and view event log files. Un-authenticated scans will run in an anonymous mode and will yield fewer weaknesses on your systems. Note: un-authenticated scans can be advantageous in that they will give you a view into the vulnerabilities an unauthenticated entity will see if they were to perform a scan against your infrastructure.

When configuring scan templates, Qualys uses the term *Option Profiles*. Qualys profiles allow for the common set of features that have been listed above, in addition to breaking out how vulnerabilities can be detected. The creator of the template has the ability to choose to scan everything Qualys has in its database to only what Qualys deems a level five severity. Optionally, you can choose to scan against the SANS top 20 and nothing additional.

© SANS Institute 2008, Author retains full rights.



When your template is complete, it is time to schedule a scan. Qualys scans can be immediate, scheduled or reoccurring. To initiate a scan, you will need to provide:

- A title
- Which scan template (option profile) you wish to use
- Scanning appliance assigned to the asset group
- The target asset groups or IP for the scan.

In selecting your vulnerability detection details, Qualys offers support for OVAL. Open Vulnerability Assessment Language (OVAL) is an international information security community whose goal is to promote a standard that will allow the transfer of vulnerability data across any security tools OVAL compliant.[2] If you have the requirement to utilize your assessment data with other applications, you will find this feature a benefit.

- A simple and straightforward approach for determining if a software vulnerability, configuration issue, program, or patch exists on a given system.

© SANS Institute 2008, Author retains full rights.

- Standard Extensible Markup Language (XML) schemas that outline the necessary security-relevant configuration information.

- A single XML document that encodes the precise details of specific issue.

- An open alternative to closed, proprietary, and replicated efforts.

- Supported by a community of security experts, system administrators, and software developers

Once your scan has been kicked off, whether scheduled or immediate, scan results are sent to Qualys. The final results of the scan will be posted to the *Finished Scan Section* with the provided title.

It is important at this point to identify the accuracy of the data you will obtain using the Qualys scanning engine. Qualys states that their existing revision of QualysGuard, as of 2007, is scanning at a Six Sigma level**.** **"**Six Sigma"[3] is a set of practices originally developed by Motorola to systematically improve processes by eliminating defects, and in this case false positives. The term "Six Sigma" refers to the ability processes to produce output within a certain specification. In particular, processes that operate with six sigma quality produce at defect levels below 3.4 defects per (one) million opportunities. Six Sigma's implicit goal is to improve all processes to that level of quality or better. With this level of defect levels in the Qualys engine, you can be comfortable with the data you will be reporting with.

Report on Your Results

The generation of reports against your collected assessment data is critical to your vulnerability assessment program. Providing the right data to the right

© SANS Institute 2008, Author retains full rights.

people is the key to a successful effort. Like the scan templates outlined earlier, reports can have templates also.

Reporting templates allow you to filter and customize the vulnerability details for a particular scan or set of scans. For example, you may have configured a weekly scan that assesses an entire data center but the scan contains a mix of Windows, UNIX, and workstations. In this hypothetical example, each of these operating systems is supported by a different team and you want to break out just the vulnerabilities that are applicable to only those teams. In this case, you would create three report templates and run each of them against the single data center scan.

- A Unix report containing only Unix servers to be delivered to the Administrators
- A Windows report containing only Windows Servers delivered to the MS administrators
- A workstation report containing Apple, XP and Solaris delivered to the desktop support group.

Additionally, you could break your reports up between Server Support, containing all UNIX, Windows and then workstations for the Desktop Support group.

To create a report, Qualys has built an elegant method utilizing their templates. When creating the template you will need to provide:

- A title for the report template

© SANS Institute 2008, Author retains full rights.

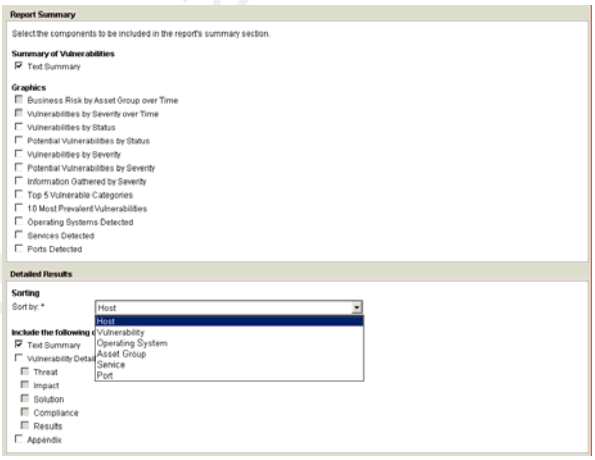
- The scan data you wish to report against. Note: this can be selected at runtime or over a period of scan intervals (example: current month, quarter, year)

- Choice of pre summarized data elements such as Top 10 vulnerabilities and explanations of found vulnerabilities

- How to Sort the data in the report (host, vulnerability, OS, Asset, Service or Port)

- How detailed you want the information pertaining to the identified vulnerabilities

- Whether you want to show trending data (historical)



When generating your report, by utilizing the pre-configured template, you will be obtaining the specific information for the recipients of the report.

© SANS Institute 2008, Author retains full rights.

In addition to point in time reporting against a vulnerability scan, Qualys has the ability to provide trending data. Reporting on the Status with Trend options use vulnerability data collected from past scans. Each time you generate a report with one of these settings, Qualys automatically collects from the database vulnerability data for the hosts you've specified in the template. These reports use vulnerability history and host data to identify the current status of vulnerabilities and produce trend information. The report will now show New, Fixed, Re-Opened, Active status for each system reported against.

- Include daily | weekly | monthly data. Generate a trend report analyzing vulnerability information on a daily, weekly or monthly basis. The reporting engine will select results based on the time frame you specify. You may specify up to 31 days, 20 weeks or 12 months.

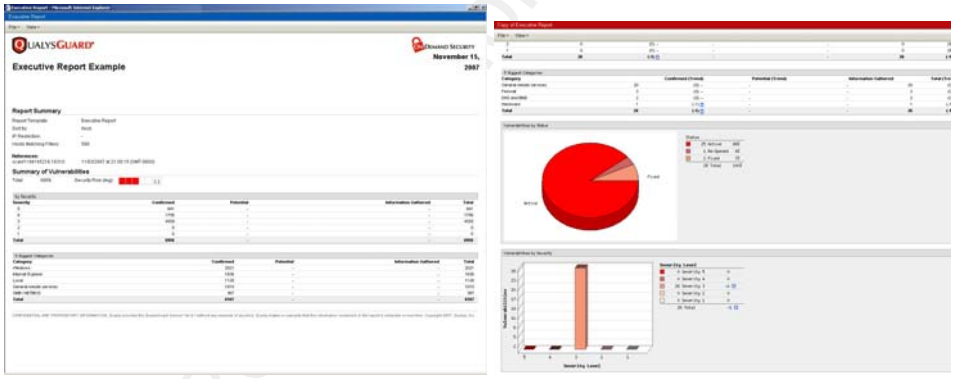
- Only include scan results from the specified time frame. Select this option to ensure that only vulnerability information gathered in the time frame that you've specified is included in the report.

- Include vulnerability information for the past 2 detections. Select to compare the most current vulnerability information to the last known information. The reporting engine will analyze the last two detections for each vulnerability on each host, comparing the current vulnerability status (New, Fixed, Re-Opened, Active) to the last known vulnerability status.

Qualys has several options when it comes to extracting reports, whether you are looking for a real-time view or an electronic copy you can hand around. Each time you generate a report for download, you can choose from many common file types. PDF, HTML, Web Archive (MHT) or XML are all typical report formats and each will have its own niche.

© SANS Institute 2008, Author retains full rights.

You will find advantages and disadvantages to varying vulnerability reports depending on use. Qualys packages several out of the box reports, such as the Executive Report and the Technical Report, which can provide meaningful data to your management team. You may find that your management team is not interested in the details but will request trending data over time or the current risk threat level. Choosing to provide a 300 page PDF report containing all workstation vulnerabilities may be comical to provide an external auditor, but will not be advantageous when dealing with your patching team. Providing a 2 page MHT report containing the highest severity vulnerabilities found on your workstations will be much better received.



Example: Executive and Technical Reports.

Note there is a hidden danger in vulnerability reporting. In some cases you can run the risk of information overload for the individuals who will consume your reports. Irrelevant data, giant reports and false positives are the easiest ways to get people to take your vulnerability reporting less seriously and can jeopardize the credibility of your vulnerability program. Your goal will be to create quality, relevant and filtered reports for the teams that will be conducting the remediation.

Rank Your Risks and Remediate

You have scanned your computing infrastructure and generated your reports, so what now? At this point it is time to review the results of your

© SANS Institute 2008, Author retains full rights.

assessments. For most major vulnerability assessment software packages, vulnerabilities will be ranked according to some value determined by the vendor. Invariably, your first sets of assessments will be chocked full of potentially serious items. Taking the top down approach is used most of the time where the most severe vulnerabilities are addressed first with serious, high and medium following after.

To avoid information overload, filter your initial assessment reports for the highest vulnerabilities that exist the most in your environment or your team deems are the highest risks to your company. Schedule monthly or bi-monthly meetings with the groups responsible for patching and remediation and review the assessment reports to quickly reduce the risk to your business. There will be some vulnerabilities and configuration changes that need explanation and reasons why the effort to mitigate is valuable. Familiarize your team with the reported vulnerabilities and understand how they can impact your environment. Patching and configuration steps are a very vital step in a defense in depth strategy for your company.

After your initial push for remediation of the severe items, your reporting should then address the rest of the vulnerabilities discovered. At a minimum, monthly review of vulnerability assessment reports with the patching and remediation teams will be important to your program. Reports you will see at this phase will typically be sorted:

- By severity (each system effected by the vulnerability)
- By system (each vulnerability on the device listed)

Additionally, discuss new vulnerabilities discovered, patching efforts, false positives (items identified in your report that have been proven to not be susceptible to the weakness) and new segments of the business you would be interested in adding into your scanning scope.

© SANS Institute 2008, Author retains full rights.

Larger more experienced organizations will move to automatic ticket generation when vulnerabilities are discovered by scans. When a scan identifies a new vulnerability on a device that was not visible prior, a ticket will be generated. These assessment tickets, which can generate email, can then be used to create trouble tickets in you internal ticket tracking system.

Qualys has a built in ticketing system termed – Remediation. In the remediation section, teams can view their outstanding tickets. Users can view, edit and delete tickets for assets that they've been assigned, even if they are not the ticket owner. Users can search to find tickets by ticket number, ticket state/status, due date and other criteria. When a ticket has been assigned an owner, the ticket can be modified to several statuses:

- Resolve
- Close-ignore
- Reopen
- Reassign

When using remediation with Qualys, new reports can be generated to analyze mitigation efforts. Outstanding tickets, number of tickets closed and vulnerabilities ignored are just a handful of reports that can be created to help manage the program.

Handling Verification and False Positives

Handling of false positives is yet another important step in your program. There is no vulnerability assessment software that will completely eliminate false positives, and your team should be prepared to deal with these events when they are identified. I have seen many cases where the vulnerability assessment group

© SANS Institute 2008, Author retains full rights.

will continue to report on a weakness even after the patching team has remediated the event.

Vulnerability Scanners will utilize several things to determine if a system is susceptible to a known weakness. Location of known files, registry entries, services running, TCP ports, banners, etc are all standard means of identifying system and how it is operating. In some cases, a workaround or a patch will not change enough of the fingerprint for the assessment scanner to see the weakness mitigated. This is when your team will need to step in and administer your assessment tool.

With Qualys there are a few options for dealing with false positives. You can choose to ignore a single vulnerability for your entire enterprise, ignore a single vulnerability on specific systems or change the details of the vulnerability. Each of these choices has its place and should be used when necessary. To modify vulnerabilities you will be working in the Knowledge Base Menu.

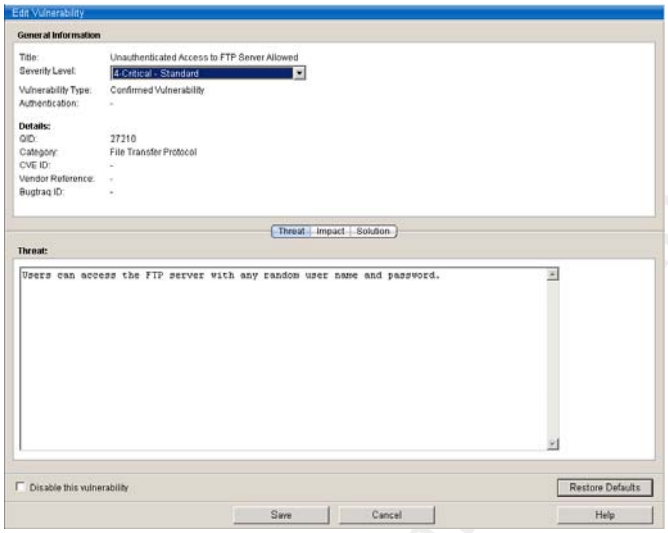
- Change the severity level. Vulnerabilities are assigned a severity level by Qualys. This "standard" severity level is decided based on the security risk associated with its exploitation. You can apply a different severity level by selecting a new level.

- Edit vulnerability content. You may rewrite the vulnerability threat description, impact description and solution instructions. Your revised text will appear whenever the vulnerability is reported or listed.

- Disable the vulnerability. Administrators can disable vulnerabilities in order to globally filter them from all hosts in all scan reports. Disabled vulnerabilities are filtered from reports, host information, asset search results and your dashboard. You may

© SANS Institute 2008, Author retains full rights.

include disabled vulnerabilities in scan reports by changing report filter settings.



Removing a false vulnerability from a specific device can be accomplished via a trending report. A trending report containing the targeted device will provide the option, next to the identified device, to ignore that specific vulnerability. This is handy if you find that you only want to ignore the vulnerability for just the device and not your entire infrastructure.

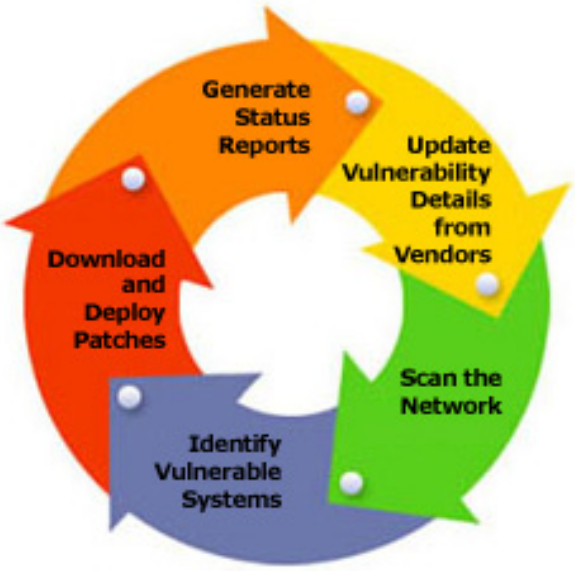
It is always a good idea to contact Qualys support when you believe you have identified a false positive. For quality assurance reasons, Qualys will want to investigate this issue, in addition to aiding you in correctly confirming the false positive. I have witnessed cases where we believed we had identified a false positive, to only have Qualys support show that the vulnerability still existed. Qualys will utilize a Linux application they provide to help further investigate the issue. This small scanning applet will perform a targeted scan against the device in question and generate a log type file. The log file can then be sent to Qualys for investigation. In both cases, you are aiding Qualys in increasing the accuracy of the product and confirming you can remove the false positive from your reporting data.

© SANS Institute 2008, Author retains full rights.

False positives can negatively impact trending data. If you have a management team that has decided to track vulnerability metrics, such as number of critical severities remediated over a period of time, keeping the false positives to a minimum will be a desired result.

Compliance and Life Cycles

Vulnerability Assessment has a never ending life cycle. This cycle continually scans, reports, assesses, remediates and evaluates. Vulnerability management needs to be addressed as a continued lifecycle to be truly effective. Daily, there are new attack signatures being developed, viruses and worms being written, buffer overflows discovered, changes in your organization's infrastructure and new technologies are being developed. Each of these actions affects the risk posture of the organization. Any one piece of the lifecycle cannot be effective without the other.



There is a movement by corporations that have assessment programs to utilize data generated by the vulnerability scans for compliance efforts. In some

© SANS Institute 2008, Author retains full rights.

sectors of business vulnerability assessment is a requirement to meet compliance laws.

- Companies subject to Sarbanes Oxley find trending reports can be utilized as proof of internal patching controls.

- Certain PCI standards can be met with high scores on the vulnerability reports. [4]

- Sections if the HIPAA law addresses vulnerability assessment of systems containing ePHI. [5]

- Sections of GLB regulatory compliance can be met with vulnerability assessment reports.

Qualys has launched a platform designed to help organizations that accept credit card transactions online comply with new Payment Card Industry (PCI) standards. The Qualys PCI On-Demand platform features an easy-to-use dashboard that helps to guide companies through the processes they need to complete PCI certification, including the completion of a self-assessment questionnaire. Qualys scanning technology is also built into the platform, enabling firms to locate and remediate vulnerabilities in accordance with PCI rules. Automated report preparation eases the process of reporting compliance and leaves an audit trail enabling companies to show due diligence in the event of a data breach. As an approved PCI scanning vendor, Qualys is fully certified to help merchants and service providers assess and achieve continuous compliance with the PCI standard. It allows merchants and service providers to complete all validation requirements. Using Qualys PCI users can easily complete and submit the PCI self-assessment questionnaire online, and perform pre-defined PCI scans on all external systems to identify and resolve network and system vulnerabilities as required by the PCI standard.

© SANS Institute 2008, Author retains full rights.

In Conclusion

A good vulnerability assessment program can be leveraged to ease the burden of compliance efforts, aide corporations in reducing their risk levels, perform due diligence, provide forensic data and generate reports that can be used as technology metrics. By creating a comprehensive VA program, you will be adding yet another layer to your defense in depth and add a piece of mind to your management team in an area that can only be speculated about without a program in place. Identifying those key vulnerabilities to your business and performing mitigation actions before those vulnerabilities can be exploited is at the heart of risk management. A successful comprehensive vulnerability assessment program will position your business for a safer more secure computing environment.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

Appendix A

1) **Vulnerability Assessment Policy Example**

a) **Purpose**: The purpose of this standard is to establish standards for the periodic vulnerability assessments conducted by <*company*>. This standard will empower the Technology Department to perform periodic security risk assessments for the purpose of determining area of vulnerabilities and to initiate appropriate remediation.

b) **Ownership and Responsibilities:**
   i) The execution, development and implementation of remediation programs are the joint responsibility Technology Solutions and the department responsible for the area being assessed. All employees are expected to cooperate fully with any risk assessment.

c) **General Audit Guidelines:**
   i) Discovery of assets, procedures and departmental policies
      (a) Hardware
      (b) Software
      (c) Services
      (d) Data stored, transmitted and/or processed
      (e) Source Code
      (f) Systems and technical safeguards
      (g) Administrative and policy safeguards
      (h) Physical safeguards
   ii) Analysis of assets, procedures and policies
      (a) Follow up questions
      (b) Third Party Contacts
      (c) VA Scans
         (i) Workstation
         (ii) Server
         (iii)Network equipment
   iii) Identify threats and their likelihood of occurrence. Identify impacts and threats were they to occur
      (a) Compile findings into general threats and specific threats
      (b) Label threats for High, Medium, or Low
   iv) Enumerate recommendations for mitigating or eliminating the risks of threats to satisfy policies and state laws
   v) Devise a timeline for addressing the threats

d) **Revision History**

e) **End of Standard**

© SANS Institute 2008, Author retains full rights.

[1] http://www.sans.org/resources/policies/Audit_Policy.pdf?portal=3bba01aac3b06f2bd435b648994e0d6b

[2] http://oval.mitre.org/language/about/index.html

[3] http://www.qualitydigest.com/dec97/html/motsix.html

[4] https://www.pcisecuritystandards.org/

[5] http://www.hipaadvisory.com/action/security/riskanalysis.htm

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, Author retains full rights.