Vulnerability Management Is Not Simple...

But It Does Not Have to Be hard

By Kelly Hammons – ISSA member, Cowtown (Fort Worth), USA Chapter

Vulnerability management is one of the basic tenants of information security, but it is not simple. But with proper planning, consistent processes, and the right tools, it does not have to be hard. This article examines some of the challenges and tricks to implementing a successful vulnerability management program.

When Vince Lombardi became coach of the Green Bay Packers, he was asked what he was going to change. Lombardi is reported to have said, "We will use the same players, the same plays, and the same training system. But we will concentrate on becoming brilliant on the basics."[1]

According to the Verizon *2012 Data Breach Investigations Repor*, "97% of breaches could have been avoided through simple or intermediate controls."[2] And the IT research firm Enterprise Security Group said in its 2012 *Security Management and Operations* report, only "40% of security professionals say their organizations test the effectiveness of their security controls "constantly" rather than on an as-needed basis."[3]

As technologists and security practitioners, we like to focus on things that are new and exciting, like data loss prevention (DLP) and advanced persistent threats (APTs). Of course, those are important, but the fact is that most breaches occur without complicated hacking: the attackers are just walking in through a wide-open door. If we could consistently apply the needed "simple or intermediate controls," then attacks will be exponentially more difficult.

General vulnerability management strategy

A well-designed vulnerability management (VM) program is a closed-loop system where the findings of vulnerability assessments (VA) are prioritized, reported, mitigated, and the mitigation confirmed. It requires consistent, easily repeated, and automated processes to keep on top of the ever-evolving threat landscape. That sounds simple enough!

While every company's needs are different, there are some general recommendations that apply to every VM program. First of all, you will need to strike a balance between scanning too infrequently to be relevant and scanning so aggressively that you impact the network by overloading the network devices. Experiment with the speed settings in your VA tool, starting off on the slow end and gradually speeding up until the scans finish in an acceptable time frame. Build an incremental scan schedule, starting with a small section of the network and expanding as you gain confidence in your VA tool and in the processes that you've built around it.

1 http://edt6392.wordpress.com/tag/attitude/page/2/.

2 Verizon, *2012 Data Breach Investigations Report*, (March 2012), http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.

3 ESG, *Security Management and Operations Report*, (July 2012), http://www.esg-global.com/research-reports/security-management-and-operations/.

"Black-box" or "port" scanning is the most common form of vulnerability assessment, but most VA tools also allow for authenticated scanning, which allows the scan to log on to the target hosts with credentials that you provide in order to determine exact patch levels—by checking version numbers on DLLs, for example. Authenticated scanning will greatly improve the quality and quantity of the vulnerabilities that are reported. You may, however, get pushback from the patching team as this will just seem to add to the long queue of vulnerabilities that they need to remediate. But it's better to have too much information and not need it, than to need it and not have it. You can always filter out the lower priority vulnerabilities from your reports.

Your assessment scans will discover a veritable mountain of vulnerabilities, so you will need to find a logical and easily implemented evaluation of risk to prioritize them. It takes time and money to remediate, so the reports should be properly prioritized such that the initial remediation efforts have the greatest positive effect on your security stance.

Questions to ask

Before you start a new project to build or improve a VM program, try to gather as much information as possible. Here is a sample list of the kinds of questions that you need to ask:

Qualifying questions:

- What is the time frame for the initial project, and when is it expected to be operational?
- Who will be involved in the project and in what capacity?
- Is there buy-in from senior management? Who? Has this been communicated to the rest of the business?

Documentation:

- Ask for a copy of the security policy; there may be requirements outlined that will affect the project.
- What is the change control process?
- Which regulations does the company adhere to (PCI,[4] HIPAA,[5] NERC CIP,[6] internal, etc.)?
- Will we be scanning business partners, and if so do we already have permission in writing?
- Is there a set of metrics that has already been agreed upon?
- How will risk be calculated and vulnerabilities prioritized?

Network diagram:

- When was it last updated?
- Where are the VPNs, WAN links, intrusion prevention systems (IPS), wireless controllers, guest networks, and firewalls?
- Where will we place the scanner appliances?
- Which firewalls are going to be scanned through?
- What are the requirements for network segmentation?

Points of contact:

- Who is in charge of patching?
  - … the firewalls?
  - … the IPS?
  - … the wireless environment?
  - … the standardized workstation/server images?

Integrations:

- Is there a security information and event management (SIEM) system to tie into?
- Is there an asset management system for host ownership and value/classification?
- Is there a ticketing system to export vulnerabilities into? How is it currently being used?
- Are there client-side firewalls or host-based IPS (HIPS) where we will need to whitelist the scanner appliances?

Scanning:

- Which IPs/IP ranges are going to be scanned (immediately and any later extensions)?
- Which IPs and ports are excluded (maintain an exclusion list with reasons)?
- Are the printers and IP phones to be scanned or excluded?
- Will we be using a "device discovery" scan before the full vulnerability scans start?
- Will we be using authenticated scanning? If so, where do we get the credentials?
- What is the desired scan frequency and when are the scan windows? (Obtain sign-off on the schedules before scanning begins)
- Will we be doing any unannounced scans to test for alert triggers and security team response?

Prioritization

Prioritization is likely the greatest challenge to a successful VM program. The amount of information coming out of an assessment can be overwhelming, so you will need to find a method to highlight the most important vulnerabilities. In general, network-facing vulnerabilities cause the greatest risk to an organization, so those should be at the top of the remediation queue.

Most vulnerability assessment tools will tell you how valuable the host is (based on which services are running, but which should be customizable) and how bad the vulnerability is, usually represented with a CVSS[7] score (CVSS is a vulnerability scoring system designed to provide a standardized method for ranking the severity of vulnerabilities from 0 to 10).

But which is more important, a CVSS 9 vulnerability on a workstation or a CVSS 4 on a database in the DMZ? I find it

4 https://www.pcisecuritystandards.org.

5 http://www.hhs.gov/ocr/privacy/.

6 http://www.nerc.com/pa/CI/Comp/Pages/default.aspx.

7 Common Vulnerability Scoring System, http://www.first.org/cvss.

more useful to include ***accessibility*** in the calculation. Simply put, is the vulnerable service running on a port that is accessible to a threat source?

This can be found through a holistic analysis of how the firewalls and routers work in concert, taking into consideration not only obviously open ports but also NAT and dynamic routing. A threat source is *anything* that is outside of your control, including the Internet and links from business partners, and may even include parts of your own network that are known to be insecure or compromised.

For example, consider a simple network with four hosts (figure 1):

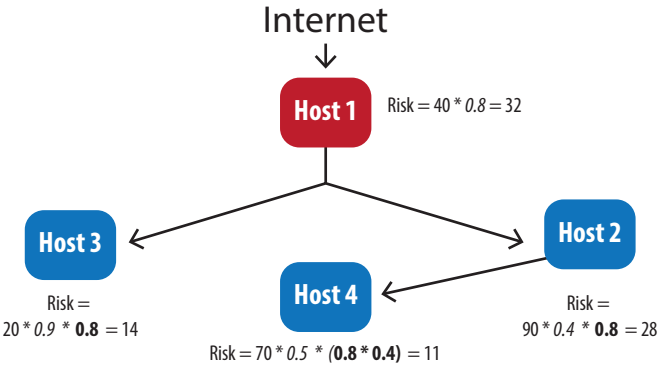


Figure 1 – Network and risk calculations

- Host 1 is a web frontend that is directly exposed to the Internet. We have found a vulnerability in the Apache service that has a CVSS score of 8. Since this host does not hold important data and can be easily replaced from backup, we set the Host Value to 40.
- Host 2 is a database backend for Host 1. The postgres service has a CVSS 4 vulnerability, and the Host Value is 90.
- Host 3 is an administrator's workstation that has direct access to and from Host 1. There is an SSL service running with a CVSS 9 vulnerability, but it's just a workstation so the Host Value is 20.
- Host 4 is a backup database for Host 2. The postgres service has a CVSS 5 vulnerability and is not quite as important as the primary database, so the Host Value is 70.

The risk score for each host is determined with the formula:

Host Value * *CVSS* * **accessibility**

The CVSS scores have been divided by 10 to accurately reflect a decreasing risk through multiple hops; **accessibility** is calculated by multiplying the CVSS scores of the upstream vulnerabilities that would need to be compromised before the given host could be reached.

Host 1: Value 40, *CVSS 8*, directly accessible from the internet

Risk = 40 * *0.8* = 32

Host 2: Value 90, *CVSS 4*, is accessible through Host 1)

Risk = 90 * *0.4* * **0.8** = 28

Host 3: Value 20, *CVSS 9*, is accessible through Host 1

Risk = 20 * *0.9* * **0.8** = 14

Host 4: Value 70, *CVSS 5*, is accessible through Host 2 (through Host 1)

Risk = 70 * *0.5* * (**0.4** * **0.8**) = 11

We can also extrapolate a further metric for downstream risk, which is the summation of the risk scores for all hosts that would be exposed if a given host were compromised (see figure 2).

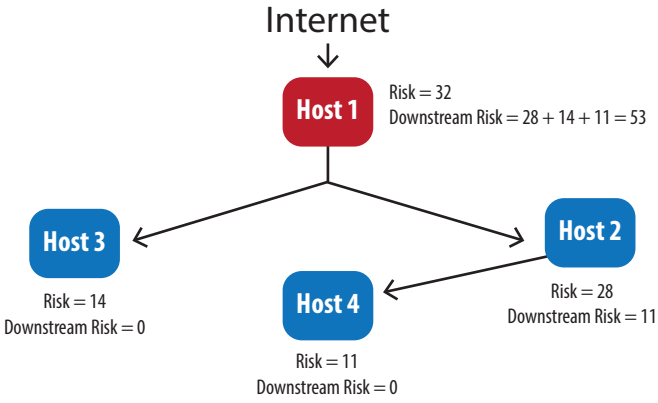


Figure 2 – Downstream risk calculation

Continuing with the above example:

Downstream risk for Host 1 = 28 + 14 + 11 = 53
Downstream risk for Host 2 = 11

The resulting risk and downstream risk values are used to prioritize vulnerability remediation, ideally feeding back in to your ticketing system so that the patching team has clear guidance on what is most important to fix. The accessibility calculations can also be used to run attack simulations or to explore the extent of an actual breach (what if Host 1 has been discovered to have been compromised).

Locally accessible vulnerabilities such as outdated versions of Acrobat Reader, Java, and Microsoft Office should have a secondary priority to network-facing vulnerabilities. The calculation here for risk is a simple Host Value * CVSS. But you can take into consideration the likelihood of exploit, for example Internet Explorer on a workstation versus a server. You can also take in to consideration that installing one patch (for example a Service Pack) may fix several reported vulnerabilities in one step.

Network facing vulnerabilities that are not accessible from a threat source (for example there is a compensating control such as a firewall) should have the lowest priority.

Remediation

Your initial scans have run. You have prioritized the results and provided clear and concise reports that are actionable and relevant to each recipient. It is now time to start fixing things. The vulnerability scanner should provide specific guidance for mitigation, which generally involves either installing a patch, upgrading the software, or disabling/uninstalling the service.

Those are not always an option, so you may need to look into creating a compensating control such as modifying the network fabric (router access control lists, firewalls, or IPS). You could also add a client-side firewall and/or HIPS. Or if you determine that the cost to protect the vulnerability outweighs the potential damage, then be sure to document the exception and review it periodically.

Regardless of the prioritization method used you should have a very loose service level agreement (SLA) to begin with in order to focus attention on the worst vulnerabilities, and then tighten it up later. This will give the patching team and system owners time to adjust to the new system and catch up on the queue.

You will also need to provide metrics to senior management in order to demonstrate the effectiveness of the vulnerability management program, to show that all the money that they are spending on security is going to good use, and to highlight areas that need improvement.

Some basic metrics that your VA tool should provide automatically are:

- Average Host Risk Score: Basic (Host Value * CVSS score)
- Top Vulnerable Systems by Risk Score
- Vulnerability Distribution by OS/device type
- Vulnerability Distribution by Severity
- Average Days Since the Most Recent Scan
- Percent of Systems with High Severity Vulnerabilities
- Percent of Systems Exempt from Vulnerability Scanning

There are more advanced metrics that require some extra digging, but which provide much greater insights. For example:

- Average Host Risk Score: Advanced (Host Value * CVSS score * Accessibility)
- Downstream Risk Score (Risk score sum from all hosts that would be exposed if the given host were compromised)
- Perimeter and Network Segmentation (vulnerabilities exposed vs. total vulnerabilities)
- Patched/fixed Vulnerabilities (total and trending by month/quarter) (individual hosts, by group, total) (by risk rating)
- Discovered False Positives
- Exempted Vulnerabilities
- Number of Network Services Running per System (weighted and raw)
- Mitigation Response Time (total and trending by month/quarter) (individual hosts, by group, total) (by risk rating)
- Unscanned Hosts/Network Segments
- Patching Response Time (critical and noncritical)

Challenges

You will likely encounter resistance from network operations, the patching team, and the device owners. You can expect network devices and hosts to become impaired for a variety of reasons, commonly when poorly designed services behave improperly due to unexpected input or allow a buffer overflow. So make sure that the device owners and change management are aware of the scan schedules; send them an extra notification right before new segments are scanned for the first time.

Network devices will probably become saturated. There will be firewalls in places that no one knows about, and it will be very easy to fill the state tables of older devices. Let network operations know the scan schedules and give them access to the vulnerability assessment console so that they can stop a scan if it is causing a network outage.

The patching software will not always agree with the VA tool. Patching is looking for the absence of patches, but the VA tool is looking for the presence of vulnerabilities. For example, there may be an outdated DLL that is no longer used. Patching will give the all clear, but VA will report a problem.

One way to help bring the other teams to your side is to have "security heroes" instead of a "wall of shame." Turn it around and show the top groups in terms of vulnerability mitigation. You might also consider pushing for a bonus system or something similar to encourage participation.

If you do not have an updated asset management system, it may be difficult to figure out who the system owners are so that you can send them vulnerability reports. The authenticated scan data can help here: it should include the last logged-in user, MAC address, installed programs, and local users.

You may be required to scan external IPs to satisfy some regulation, but internal IPs will give you a much clearer picture of how vulnerable the host is. Scanning through a firewall is actually only testing the efficacy of the firewall, not the security of the host. And the ports that are exposed to the Internet may change depending on the source IP. You will also need to know which vulnerabilities can be exploited if the perimeter has been breached.

It might not be possible to avoid scanning through internal firewalls if your network is highly segmented. If you must scan through firewalls, then you should at least whitelist the VA scanning appliances. VA scanning uses malformed packets to probe for network-facing vulnerabilities; firewalls can drop or "correct" malformed packets from whitelisted traffic, so many vulnerabilities will not be reported. But authenticated scans use "normal" traffic, so in this case authenticated scans are doubly important.

Interoperability

A vulnerability management system can add value to other silos of information security—the whole is indeed greater than the sum of its parts.

Asset management

VA scan data can include information about installed applications and recent users. Asset management data can be used to determine the value of hosts for vulnerability prioritization and to determine who is responsible for patching.

Patching

Patching tools look for the absence of patches while VA looks for the presence of vulnerabilities. Integrating the two can eliminate confusion when the patching tool refuses to install a patch that the VA tool insists is necessary. You could also

allow the patching team to run ad hoc vulnerability scans to confirm that patches have been properly installed.

Penetration testing

VA scan data can speed up a pen test, and a pen test can be used to confirm the presence of disputed vulnerabilities.

SIEM/IPS/IDS

Adding VA scan data to the SIEM, IPS and/or IDS can help fine tune and add context to alerts and mitigate false alerts. Alerts can also be used to bump up the priority of vulnerabilities that are currently or commonly exploited. Configuring the IPS and IDS to ignore sanctioned vulnerability scans will also remove a lot false alerts.

Ticketing

Some VA tools have their own ticketing, but you might want to integrate it into your existing ticketing system. This would simplify workflow for the patching team and system owners, and give you more flexibility in how the tickets are handled. For example there could be one ticket per vulnerability, one ticket per host with multiple vulnerabilities included, or even one ticket with a single vulnerability across multiple hosts. Also consider adding a process to rescan for vulnerabilities that have been marked as "fixed" and to have the VA tool automatically close tickets where the vulnerability is no longer detected.

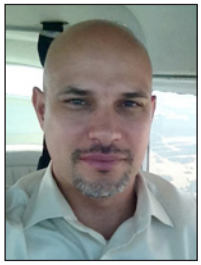
Vector analysis

Vector analysis (access paths from one subnet to another) can be used to get "accessibility" values for prioritizing network-facing vulnerabilities. Combined with VM, vector analysis can effectively become a continuous "white-box" pen test, where all information about the network infrastructure and vulnerabilities are analyzed together. Vector analysis can also be used to identify subnets that have not been scanned for vulnerabilities.

Conclusion

When the build project is finished, you should have a vulnerability management system that is efficient, effective, and easy to maintain. Vulnerability management is one of the basic tenants of information security, but it is not simple. But with proper planning, consistent processes, and the right tools, it does not have to be hard. You too can be "brilliant on the basics."

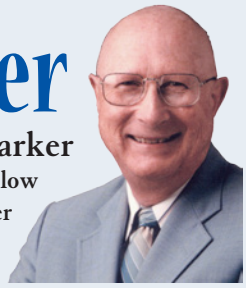
About the Author



Kelly Hammons, CISSP, is the Principal Consultant for Secutor Consulting. He has been in IT for 20 years and in information security for the last 12. Kelly has assisted many companies in building, expanding, and improving their vulnerability management programs. He can be reached at Kelly@SecutorConsulting.com.

COMMENT?

Donn's Corner



By Donn Parker
ISSA Distinguished Fellow
Silicon Valley, USA Chapter

COMMENT?

The Golden Age of Cybercrime

This new column in the *Journal* will present and briefly explain my sometimes controversial information security maxims (general rules, principles, or truths) for your edification. The topics I will address start with cybercrime followed by information security solutions, advice for information security management, cybercrime predictions, and security's future. A caveat is in order: for every maxim, there is an exception.

I started pioneering information security in 1967, when as CIO of a service bureau I had to fire a programmer for stealing my customers and computer services. (He unsuccessfully reasoned that he used only idle computer time that would otherwise go to waste.) I started to wonder and worry about a dark side to computing, and the rest is history. I retired about 15 years ago, but I remain active in the profession. ISSA was kind enough to honor me with Distinguished Fellow status, the 1992 Individual Outstanding Achievement Award, and the 1999 Hall of Fame award.

There are frequent disputes over the definitions of computer crime and cybercrime. A crime is a crime only if it is proven to be a violation of a law in a court. Informally any adversity that seems to be intentional is called a crime. "Computer crime" is a term used synonymously with "abuse and misuse of computers," and now we call it "cybercrime." One simple definition of cybercrime is a type of crime involving a computer or device using a computer.

A broad definition of cybercrime is necessary so as not to overlook the need and range for information security solutions. This makes many, if not most, crimes today cybercrimes. Now even many of the violent crimes are also cybercrimes such as when they involve a social networking website. The Madoff Ponzi scheme was a cybercrime based on my definition. Madoff carried out his crime using computers as fraud tools and as producers of results that can be trusted.

I found it useful to help keep an audience's attention by quoting a maxim now and then. I believe my collection is still as relevant today as it has been for the 45 years of my practice. Types of crimes, errors and omissions, and security solutions do not generally become obsolete; they accumulate and evolve as technology and its use expand and advance.

Another caveat: my cybercrime collection, from which I derived some of the maxims, is biased. All 200 perpetrators I interviewed were just the ones caught, performed acts rich with security implications, and were easily accessible. Here is my first maxim:

We are in the golden age of cybercrime between disaster and annihilation.

It is a golden age of rapid criminal expansion in the dark side of computing and the Internet. Wrongdoers of all types have discovered the power and leverage provided by computers in their nefarious activities. They are expanding into apps, smartphones, tablets, robots, and all kinds of things containing computers. Disasters such as the $5 billion Madoff investment fraud and 2008 recession may be overshadowed by the possible coming annihilation of the Internet as cybercrime reaches a level so high that we may no longer be able to afford it. What do you think?

Donn Parker, CISSP, Retired, Distinguished Fellow, and information security pioneer, donnlorna@aol.com.