ALIEN VAULT

Vulnerability Management: Think Like an Attacker to Prioritize Risks

Working Smart Beats Working Hard and Failing

Attackers care about ROI – they want to accomplish their objective with the least investment of time and resources possible. To most effectively manage vulnerabilities, you need to think like the attacker: how would you go about doing damage, exfiltrating valuable information and making money? What are the key assets in your network that you would target? How would you get to these assets?

Applying every patch and security update right away to every device on your network is usually not feasible for several reasons. Patching business-critical systems and applications requires thorough testing, which takes time and effort. In addition, there are too many patches and security updates to keep up with. There may be another group in your company that actually makes the changes to your network and systems, and strict change control policies can cause delays. Finally, some patches have side effects, such as limiting functionality or requiring upgrades to other software..

It's easy to get caught up with a vulnerability assessment tool sold to you by a security or compliance vendor and to busily scan everything in your network. From this, you can create an impossibly long list of things you need to fix. This approach is hard work and prone to failure, especially for the small- or medium-size business.

Instead of hitting your head against a brick wall, a smarter approach is to take the attacker's perspective. And since you care about ROI too, a unified approach to security management is going to help you send attackers into the brick wall without breaking your budget.

What We Mean by "Changing Threat Landscape"

Five or 10 years ago, the most common type of attack that a hacker was using from the outside to get into your organization involved reconnaissance around your internet-exposed systems, your servers, web servers, mail servers, and so on to try to find vulnerabilities in those systems. The attacker would then exploit those vulnerabilities in order to use a system that was exposed to the internet as an entry point into your network, and from there they would hop around and get access to other interesting and valuable systems in your environment.

That was the old attack paradigm. And for security professionals, it was actually relatively easy to deal with, if you had the right resources in place. Basically, you only needed to establish a good vulnerability scanning protocol and procedure, have a firewall and a good intrusion detection system (IDS) in place, and you could identify these threats. You'd block them from the network when they popped up and started causing trouble, and it was a relatively straightforward process.

Unfortunately, attackers have gotten pretty smart over the past 5-10 years or so in terms of the evolution of their attack vectors, which have largely transitioned over to malware, which is brought in by users, at this point. The typical attack strategy involves malicious code that they can get implanted into your network by your users with well-known, but tricky-to-defend tactics, like phishing.

As a result, your internet-exposed servers/services are not necessarily the thing that you need to spend the most time monitoring. Obviously, you need to have good controls on those systems, you need to have good monitoring in place on those systems, but you can't stop there.

Your users are actually far more vulnerable and far more exposed to the internet than any of your servers or services are. The footprint of your users in your environment is probably larger than the number of servers that you have in your organization, and they're accessing the internet with vulnerable web browsers, with vulnerable Adobe Flash, with vulnerable Java versions – vulnerabilities that give the attacker the ability to compromise their local workstation just through web browsing activity. It's a much easier path to get into your network for the attacker.

How to Think Like an Attacker to Prioritize Vulnerabilities

You know you need to find and fix vulnerabilities in your network and systems because these weak points are what attackers like to find and exploit. Since there are quite a few vulnerabilities, and finding all of them, and trying to figure out if, how, and when you can patch them has to be managed as a **process** rather than a task.

If you purchased a vulnerability scanning product, or work with a 3rd party to do vulnerability scanning or compliance scanning, it is possible that a checklist mindset has taken over and your original purpose has been forgotten. There are two basic reasons to scan for vulnerabilities: to pass audits and to prevent nasty incidents. You are going to need to prioritize ruthlessly. And the key to prioritization is to view vulnerabilities the way the attacker does, and to include the context of actual threats facing your environment.

Thinking like an attacker is not something we automatically do. It's far more natural to look at vulnerabilities in the context of how we value our assets, according to business priority. Actually, attackers are looking for vulnerabilities that are exposed – ones offering an attacker a way to pivot into the truly valuable assets on your network.

A trap you might fall into is to consider only the severity of a vulnerability in your prioritization efforts. The Common Vulnerability Scoring System (CVSS) is an open source standard used by many vendors and others in the industry to give you an idea of the severity of a vulnerability. The CVSS score of 7.0 – 10.0 is considered critical, with 4.0 – 6.9 being major and 0 – 3.0 being minor.

While these numbers are important, we come back to the same point: for a vulnerability to be exploited, it must be exposed to a threat. An unexploitable vulnerability can pose little to no risk to an organization. For example, you could have a 'critical" vulnerability present on a server but if that server is not connected to the rest of the network, there's little to no risk. While the CVSS system does take these considerations into account with environmental scores, many people just use the published base score and do not consider the environmental scalars, which provide a more realistic assessment of risk.

A vulnerability that is only a 'major" or 'minor" impact on an Internet-facing machine could pose significant risk to your organization as a great entry point for attackers to get at your key assets. So the trick becomes viewing vulnerabilities in the context of real, actual threats present in your network, and taking environmental factors into account so that you can prioritize remediation efforts.

A thoughtful risk management thought process is required, since 'you can't fix everything." You are going to need to prioritize ruthlessly to be successful. No product vendor can tell you your risk priorities – it's something that is different for every business. You can hire a consulting firm to help you determine your risk priorities, or you can figure it out yourself.

If you choose to figure it out yourself, as most small and medium businesses do, you need to reach out to your lines of business leaders and figure out what information and systems are critically important to your business. Once you have this 'short list" of what really counts, you need to think about how attackers might enter and pivot to them. The critical assets and the entry/pivot points are the assets you need to have on your remediation priority list.

From an attacker's perspective, the best target is any asset that allows them to achieve their goals, as cheaply as possible. Several pop to mind:

- Client systems used by administrators are valuable targets, as they contain cached credentials, notes and other information about the network. In addition, it will not look unusual to security monitoring systems if these systems are used to access important systems and run at elevated privileges.
- 'Forgotten systems" – systems that quietly run in a closet that nobody touches or thinks about are nice places to start an assault.
- Mobile systems can be especially attractive to attackers, as users are likely to fall prey to exploits and bring the problem right into your network.

Vulnerabilities on these types of systems are dangerous, and this should be considered in your prioritization process. A real-world consideration is that management may choose to acknowledge some of the vulnerabilities you find and prioritize, but decide not to remediate them immediately. It's the nature of business, sometimes it's better to accept certain risks rather than taking on the financial investment required to address them. In this case, it would be wise to document the decision in case there are repercussions.

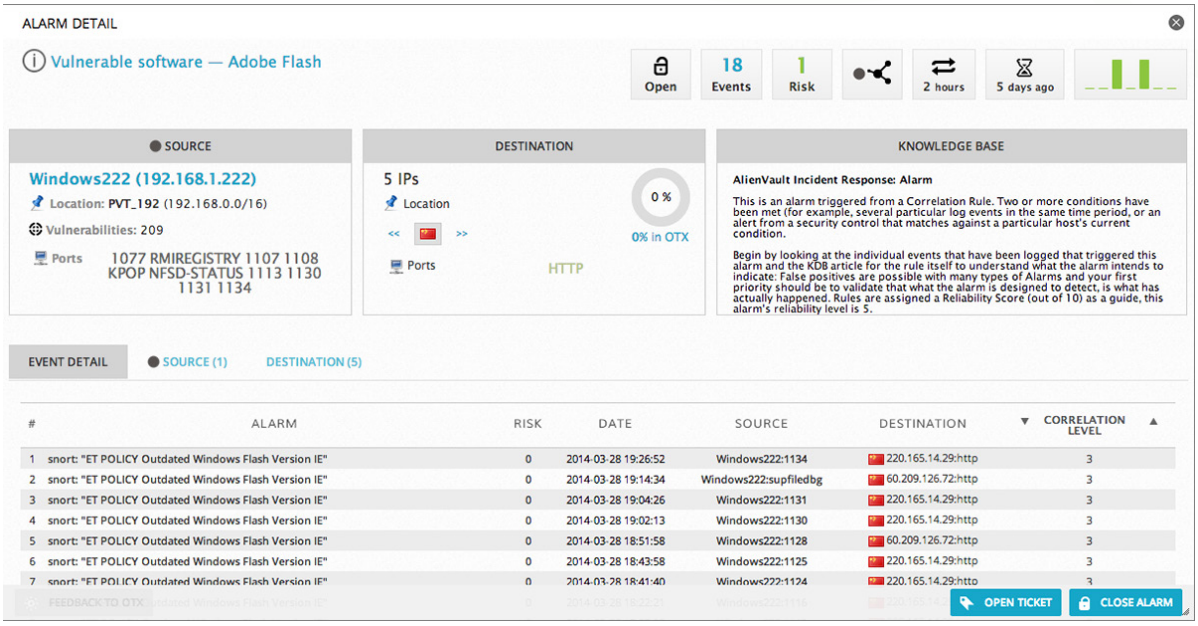
Some factors you may want to consider to make your prioritization more robust are:

- Which users are logged into the system
- What services are running on the system
- What other systems are on the same network
- Whether the system is currently accessible from the internet
- When the system can route to critical assets

Finally, bear in mind that the attacker cares about ROI and is likely to attack weak targets with as little effort as possible. Although zero-day exploits are heavily publicized, attackers often use older, proven exploits very effectively. Fortunately, many such exploits are well known and have clear remediation methods.

Avoiding the Vulnerability Management Brick Wall – A Unified Approach to Security Management

AlienVault Unified Security Management (USM) gives you visibility to vulnerabilities in real-time for prioritization and incident response. Because USM combines vulnerability management with asset inventory, host-based IDS, network IDS, netflow analysis, file integrity monitoring, and SIEM event correlation, all of the rich information captured by these capabilities is viewable in a single screen. As soon as an alarm is triggered, you can immediately identify known malicious IPs interacting with a vulnerable host, along with all events involving that host, details on the vulnerabilities discovered, notes on who owns the system as well as all the software installed on it.

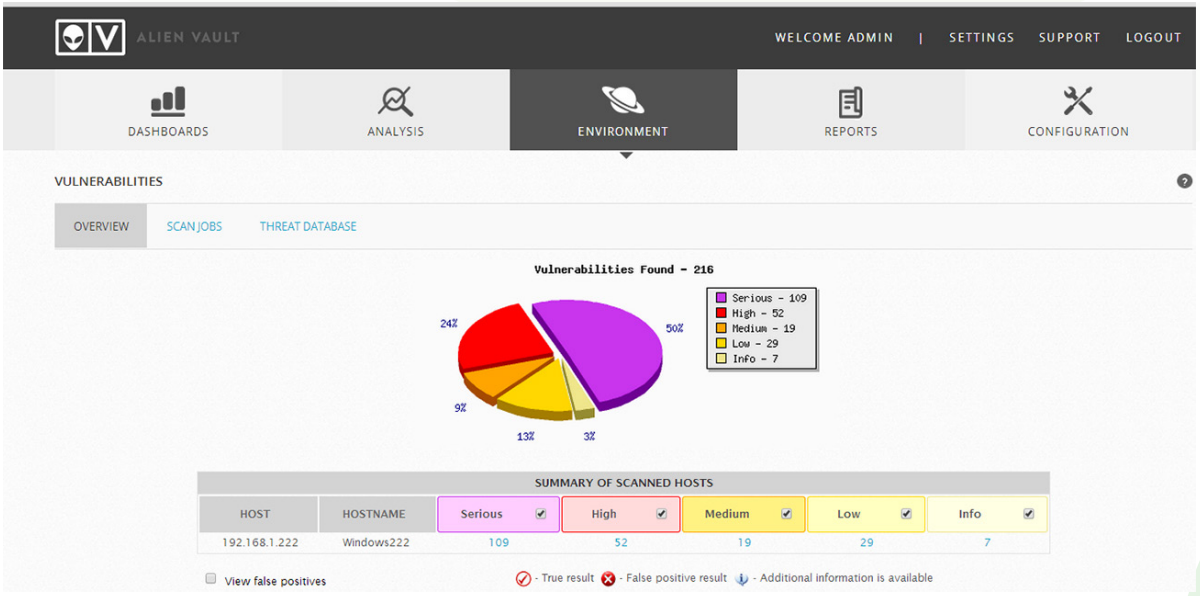


Vulnerable software that is identified via passive monitoring

In addition, if there are certain vulnerabilities that IT is well aware of, and they have been deemed to not be an issue, USM allows these known, but harmless vulnerabilities to be suppressed from correlation and reporting, saving management time. USM helps you filter through the noise of false positives and vulnerabilities that are of lesser importance and allows you to focus on risks that truly matter to your business.

Built-in Active Vulnerability Scanning and Assessment

USM provides **continuous vulnerability monitoring**. Also known as **passive vulnerability detection**, USM correlates the data gathered by its asset discovery scans with known vulnerability information for improved accuracy. This provides valuable vulnerability information while minimizing network noise and system impact. USM supports **unauthenticated scanning**, which is scanning without requiring host credentials. This scan probes hosts with targeted traffic and analyzes the subsequent response to determine the configuration of the remote system and any vulnerabilities in installed OS and application software. USM also supports **authenticated scanning** – which is scanning with credentials. This entails access to the target host's file system, to be able to perform more accurate and comprehensive vulnerability detection by inspecting the installed software and its configuration. USM allows you to mix and match these methods as well. For example, you may wish to run authenticated scans on compliance-related assets and throttle back to passive vulnerability assessment on low risk assets where reducing network traffic matters more than validating stringent security configurations.



This vulnerability scan found 216 vulnerabilities, of which 109 were serious.

USM also lets you set up a scanning and reporting cadence for your vulnerability management process. USM's built-in vulnerability assessment lets you schedule scans, with flexibility to select which network segments are to be scanned, and at what frequency. Findings from the scans can be used to create alarms on the USM web interface, and can be correlated with other events occurring on your network.

Remediation Advice for Every Vulnerability

USM also provides remediation advice for vulnerabilities that are found. It includes dynamic incident response templates and 3rd party references to help you figure out how to remediate vulnerabilities that a scan may find. This advice saves you time researching each vulnerability and tracking down this information yourself.

No name	801399	general (0/tcp))	Serious

Overview: This host is prone to Remote Code Execution vulnerabilities.

Vulnerability Insight:
The flaws are due to:
- An error in the loading of dynamic link libraries (DLLs). If an application does not securely load DLL files, an attacker may be able to cause the application to load an arbitrary library.
- A specific insecure programming practices that allow so-called 'binary planting' or 'DLL preloading attacks', which allows the attacker to execute arbitrary code in the context of the user running the vulnerable application when the user opens a file from an untrusted location.

Impact:
Successful exploitation will allow attackers to execute arbitrary code or to elevate privileges.

Impact Level: Application.

Affected Software:
Micorsoft Windows 7
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2003 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior.
Microsoft Windows Server 2008 Service Pack 2 and prior.

Fix: Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link,
htttp://www.microsoft.com/technet/security/advisory/2269637.mspx

References:
http://secunia.com/blog/120/
http://www.microsoft.com/technet/security/advisory/2269637.mspx
http://www.network-box.com/aboutus/news/microsoft-advises-insecure-library-loading-vulnerability

CVSS Base Score : 9.3

This is a specific vulnerability that USM found. It provides information about the vulnerability and its potential impact, as well as information on how to fix the problem.It also provides helpful external links for additional information.

In terms of remediation, USM can send email alerts, open a ticket in the built-in ticketing system, or send an email to an external help desk / ticketing system. USM's built-in software ticketing system creates trouble tickets from vulnerability scans and alarms. These tickets specify who owns the remediation, the status and descriptive information. The tickets also provide a historical record of issues handled, as well as the capability to transfer tickets, assign them to others and push work to other groups.

Since exploits often opportunistically follow the discovery and public announcement of vulnerabilities by the security community, the USM vulnerability database is constantly updated with the latest details on known vulnerabilities. The built-in remediation advice is also kept up-to-date and vetted by the AlienVault Labs security research team.

Parting Thoughts

Vulnerability management is never 'done", as increasing attack vectors and software complexity require continuous monitoring and methods to prioritize remediation. Since newly-found vulnerabilities are constantly surfacing, and the organization's IT infrastructure is typically changing over time, consistent diligence is required for effective vulnerability management. By taking the attacker's perspective and thinking through your business priorities, you can better focus your risk management efforts.

A unified approach to security management , including vulnerability management, helps you discover new assets, monitor user and network behavior and use multiple security tools in concert. With AlienVault USM, you can use one product from one vendor to effectively prioritize vulnerabilities and drive attackers into a brick wall rather than vice-versa.

Learn more about AlienVault USM:

Download a Free 30-Day Trial
Try the Interactive Test Drive
Join Us for a Live Demo

About AlienVault

AlienVault provides organizations of all types and sizes with unprecedented visibility across the entire security 'stack' with the AlienVault Unified Security Management™ (USM™) platform. Based on OSSIM—the de facto standard open source SIEM created by AlienVault—the USM platform has five essential security capabilities built-in: asset discovery, vulnerability assessment, threat detection, behavioral monitoring and security intelligence. The AlienVault Open Threat Exchange™, a system for sharing threat intelligence among OSSIM users and AlienVault customers, ensures USM always stays ahead of threats. AlienVault is a privately held company headquartered in Silicon Valley and backed by Kleiner Perkins Caufield & Byers, Sigma, Trident Capital and Adara Venture Partners. For more information visit www.AlienVault.com or follow us on Twitter.

042814

ALIEN VAULT™
www.alienvault.com