



TENABLE

Network Security[®]

Boosting Your Network Defenses with Tenable's Integral Attack Path Analytics

June 19, 2012

(Revision 1)

Copyright © 2002-2012 Tenable Network Security, Inc. Tenable Network Security, Nessus and ProfessionalFeed are registered trademarks of Tenable Network Security, Inc. Tenable, the Tenable logo, the Nessus logo, and/or other Tenable products referenced herein are trademarks of Tenable Network Security, Inc., and may be registered in certain jurisdictions. All other product names, company names, marks, logos, and symbols may be the trademarks of their respective owners.

Table of Contents

Introduction 3

How Tenable Can Help 4

How The Tenable Solution Works 5

Benefits Of The Tenable Solution..... 8

About Tenable Network Security.....10

INTRODUCTION

Tenable's attack path analytics enhance the value of ordinary vulnerability scans by leveraging a combination of robust filtering and detailed intelligence pertaining to host roles, activities, and relationships to proactively identify open paths through which malware and attackers can gain access to an organization's most valuable data/resources. The Tenable solution also enables more accurate prioritization of detected vulnerabilities based on attack path findings, while providing essential notification, workflow, and reporting capabilities to facilitate follow-on mitigation and remediation activities.

A fairly routine approach for attackers is to first compromise a less critical internet-facing host, and then use it as a launch point to progressively exploit trust relationships and compromise more critical systems en route to reaching the sensitive data they are seeking. Because of the widespread adoption of Web 2.0 technologies – which makes it relatively easy to inject malicious code into 3rd party web sites – the same can now be said for internet-consuming systems as well.

Unfortunately, traditional vulnerability assessment products provide little protection against either of these threats. Sure they can identify each of the individual vulnerabilities used to ultimately gain unauthorized access to sensitive internal resources. Because they don't understand the situation any more deeply than this, however, they will invariably portray the actual risk involved inaccurately. The primary issues are twofold.

First, ordinary vulnerability scanners typically don't have access to the right data. Although they can identify individual vulnerabilities and correlate whether they are exploitable, they lack:

- > Visibility into host activities, such as serving or consuming internet content;
- > Visibility of the trust relationships between different hosts; and
- > Visibility of the available communication paths between different hosts.

The second issue is that many of these tools don't have the means to adequately analyze available data. Their lack of highly flexible yet quick and efficient filtering capabilities, support for dynamic asset lists, robust data visualization, and inability to correlate across the entire spectrum of security events basically keeps them from putting all the pieces of the attack path puzzle together. The result is faulty risk scoring, misguided prioritization of mitigation and remediation efforts, and greater overall exposure to malware, opportunistic and targeted attacks.

To overcome these deficiencies, IT organizations have historically resorted to separate attack path analysis or penetration testing tools – each of which have their own issues. For example, a notable weakness for attack path tools is that they rely on modeling. To the extent specific device types and models are supported, these tools typically 'ingest' point-in-time configurations for an organization's routers, switches, firewalls, and so forth. They then overlay point-in-time vulnerability data and enable manual and/or automated analysis of the resulting network model to reveal potential attack paths. Although useful, this approach is far less reliable (read: accurate) than periodically exercising the actual network (as is the case with penetration testing), or, better yet, continuously measuring and evaluating it (as is the case with the Tenable solution).

On the other hand, a significant challenge with penetration testing tools is that of scaling – typically, it's simply not practical (or even possible) to test every potential combination of

attack paths. Another shortcoming for both alternatives is the need not only to invest in yet another tool but also to integrate it with the other components of your vulnerability management infrastructure. Tenable changes everything by providing robust attack path analytics as an integral feature set of its Unified Security Monitoring solution.

HOW TENABLE CAN HELP

The components that make up the Tenable solution for attack path detection and mitigation are ones that many organizations already have in place to help with their broader vulnerability, security event, and compliance management objectives. They include:

SecurityCenter – A central management console, SecurityCenter facilitates and unifies essential security processes for discovering network assets, conducting configuration and compliance audits, detecting vulnerabilities and data leaks, and managing corresponding events. Among its many functions, it serves as the primary interface for administrators to view, analyze, process, and report on the vulnerability, activity, and relationship data gathered by other Tenable components.

Nessus Vulnerability Scanner – With more than five million downloads to-date, Nessus is the world's leading active vulnerability scanner. Key features include high-speed vulnerability discovery, asset profiling, agentless configuration and compliance auditing, sensitive data discovery, and in-depth assessments that help characterize and quantify an organization's overall security posture. A flexible architecture enables distributed deployment of Nessus scanners throughout an entire enterprise, while continuous support by a world-renowned research team ensures accuracy and currency of audit checks, as well as related remediation and knowledge base content. From an attack path perspective, a significant strength of Nessus is its ability to identify vulnerabilities in services and components that are not routinely active on the network but that can still be exploited by malware or hackers as part of a multi-step attack.

Passive Vulnerability Scanner (PVS) – A software-based network discovery and vulnerability analysis solution, PVS delivers real-time network monitoring and profiling for continuous assessment of an organization's security posture in a non-intrusive manner. PVS monitors network traffic at the packet level to determine topology, provide visibility into both server and client-side vulnerabilities, and identify the flow of sensitive data and the use of common protocols and services. Unlike an active scanner, which takes a snapshot of the network in time, PVS behaves like a security motion detector that continuously observes everything crossing its path, including unauthorized, unintended, and suspicious interactions between hosts.

Log Correlation Engine (LCE) – LCE is a software module that aggregates, normalizes, correlates, and analyzes event log data from the myriad of devices within your infrastructure. LCE can be used to gather, compress, and search logs from any application, network device, system log, or other sources. This not only makes it an excellent tool for forensic log analysis, IT troubleshooting, and compliance monitoring, but also provides an alternative means to reveal the roles, activities, and relationships between different hosts.

Together, these four components form the backbone of Unified Security Monitoring, a Tenable solution that unifies real-time vulnerability, event, and compliance monitoring into a single, role-based interface for administrators, auditors, and risk managers to evaluate, communicate, and report information necessary for effective decision making and systems management.

Specific ways the Tenable solution helps today's organizations defend against modern threats gaining access through common attack paths is by enabling them to:

- Identify unintended and/or unauthorized communication paths due to mis-configured security and boundary devices
- Identify unintended trust relationships between different systems
- Identify undesirable and unproductive activities that needlessly increase exposure to attacks
- Identify legitimate communication paths and trust relationships that require closer attention, and possibly enhanced defenses
- More accurately prioritize response activities for seemingly low-impact vulnerabilities that are, in fact, part of a potentially high-impact attack path

HOW THE TENABLE SOLUTION WORKS

Let's assume that all of your high-value servers are fully patched. Perhaps they're even guarded by firewalls and other network security devices. Does this mean they're protected from modern malware and targeted attacks? Even if we put aside the potential for zero-day vulnerabilities, the answer, unfortunately, is still no. What if the high-value resources are administered from less-well protected clients/devices that are routinely exposed to the Internet? Maybe it's not an administrative situation at all, but just another, more exposed system that routinely interacts with the high-value resources.

The purpose of Tenable's attack path solution is to enable detection of situations such as these so they can be properly accounted for during both day-to-day operations and more strategic efforts concerning selection and deployment of additional countermeasures. An integral feature set available at no additional cost to Tenable customers, the attack path solution involves three steps that are consistent with the basic vulnerability management lifecycle: discover/assess, analyze, and respond.

Attack path data discovery. A critical shortcoming of traditional vulnerability assessment tools is that they lack the data needed to detect open attack paths in the first place. The Tenable solution has no such flaw. When configured to perform a credentialed scan, Nessus can obtain much more than just the vulnerability and patch data for a host's network-facing services. By logging into the operating system and gaining access to the list of installed software, it can also enumerate vulnerabilities and identify missing patches for everything on the system, including client-side software such as Chrome, Firefox, and Internet Explorer.

Even more significant when it comes to detecting attack paths, however, are the additional details *continuously* being captured by PVS. In addition to itemizing vulnerabilities for software and services it sees operating on the network, PVS also captures sufficient communications data to enable identification of the specific activities individual hosts are engaged in, as well as which hosts are communicating with each other hosts, over which ports and protocols. For example, with the output from PVS, administrators can determine that a given machine connected to Facebook and Twitter, and then later to a high-value host; or that a given server in fact made an outbound connection to the Internet – all of which is useful information when piecing together potential attack paths.

It should be noted that attack path detection is not the only way the Tenable solution helps protect organizations from modern malware. Nessus is also capable of: detecting when a host is participating in or communicating with a known botnet; detecting when known

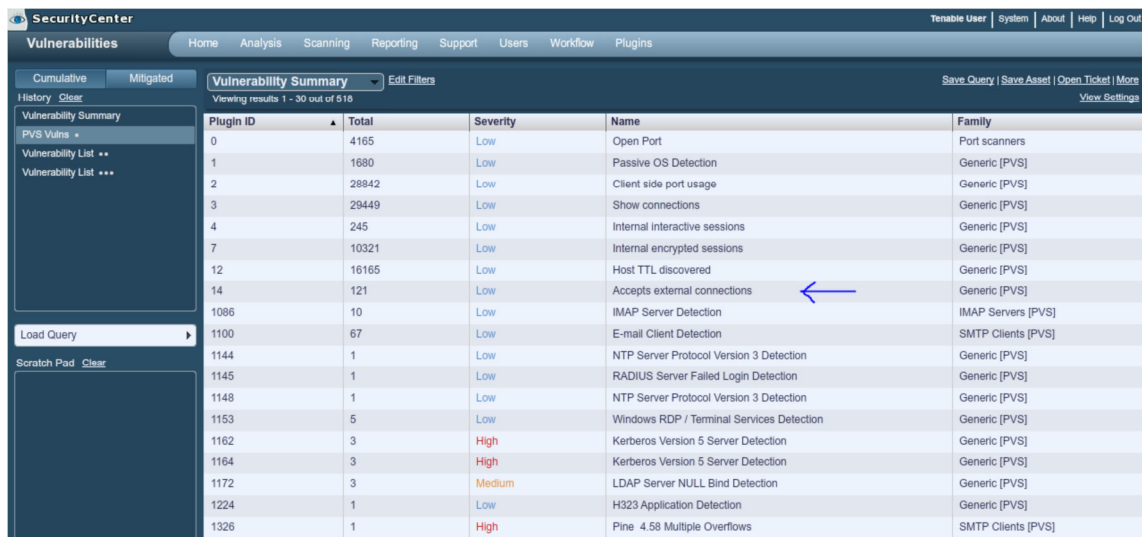
malware is running on a host; and auditing for the presence and configuration of antivirus software.

Attack path analysis. This next step is the heart of the attack path detection process and involves a combination of manual and automatic techniques to analyze the previously discussed data. By leveraging SecurityCenter’s extensive asset classification, filtering, and reporting capabilities, administrators are able to mine the available data to expose multiple classes of common attack paths, such as:

- Internet-facing services that are known to be exploitable;
- Internet-browsing clients that are exploitable; and,
- Servers that trust exploitable clients.

The basic approach is to use SecurityCenter’s analytic features to create a series of asset lists that progressively home in on the desired results. For example, a practical starting point is to answer the question: “Which servers on the enterprise network accept connections directly from the Internet, and where are they located?”

This can be accomplished in part by using Nessus to conduct an external scan and then storing the results in a dedicated repository (to keep from introducing information from other scans about open ports behind the firewall, which are not relevant in this case). Another method is to deploy PVS in a manner to monitor external network traffic. This will reveal all of the systems and services that are in use, including instances of PVS plugin ID #00014 (“accepts external connections”). For instance, the below screen capture indicates 121 unique combinations of ports and IP addresses that are serving content directly to the Internet.



Plugin ID	Total	Severity	Name	Family
0	4165	Low	Open Port	Port scanners
1	1680	Low	Passive OS Detection	Generic [PVS]
2	28842	Low	Client side port usage	Generic [PVS]
3	29449	Low	Show connections	Generic [PVS]
4	245	Low	Internal interactive sessions	Generic [PVS]
7	10321	Low	Internal encrypted sessions	Generic [PVS]
12	16165	Low	Host TTL discovered	Generic [PVS]
14	121	Low	Accepts external connections	Generic [PVS]
1086	10	Low	IMAP Server Detection	IMAP Servers [PVS]
1100	67	Low	E-mail Client Detection	SMTP Clients [PVS]
1144	1	Low	NTP Server Protocol Version 3 Detection	Generic [PVS]
1145	1	Low	RADIUS Server Failed Login Detection	Generic [PVS]
1148	1	Low	NTP Server Protocol Version 3 Detection	Generic [PVS]
1153	5	Low	Windows RDP / Terminal Services Detection	Generic [PVS]
1162	3	High	Kerberos Version 5 Server Detection	Generic [PVS]
1164	3	High	Kerberos Version 5 Server Detection	Generic [PVS]
1172	3	Medium	LDAP Server NULL Bind Detection	Generic [PVS]
1224	1	Low	H323 Application Detection	Generic [PVS]
1326	1	High	Pine 4.58 Multiple Overflows	SMTP Clients [PVS]

Subsequent drill down can be used to reveal the specific ports involved and to create dynamic assets list for later use, such as “all internet facing servers” or “all internet facing servers on a given port.” Dashboard panes can also be created to track any of these items over time.

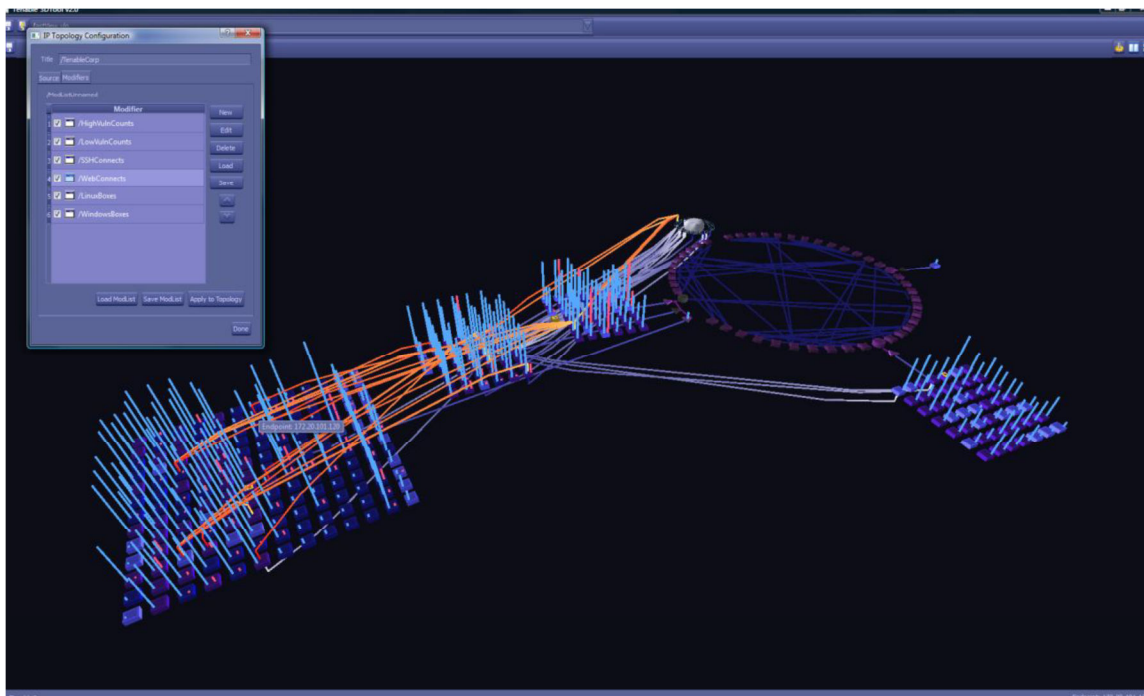
More important in this context, however, is moving on to reveal the first set of attack paths. This is done simply by applying an “exploit available” filter to the asset list for “internet facing servers.” Administrators can also elect to filter on the CVSS score level. This way

they can account for the severity of a vulnerability instead of (or in addition to) the presence of a known exploit. Either way, the resulting filters can also be leveraged for real-time altering, reporting, and dashboards by taking advantage of SecurityCenter's numerous automation features.

Up to this point, everything that has been described – the ability to correlate exploits with vulnerabilities in internet serving hosts – is not uncommon. Where the Tenable solution really shines is in the application of these same techniques (e.g., selective filtering, regular expressions, asset list creation, etc.) to answer further questions that other solutions lacking the requisite data are simply unable to address. These include:

- > Which internal systems connect to the Internet? (This list can also be refined by specific activity, such as YouTube, Facebook, etc.)
- > Which of the previous systems have exploitable client-side software?
- > Which Internet-facing servers have client-side applications with exploitable vulnerabilities? (This list accounts for many modern, complex web applications that include outbound communication capabilities, e.g., for obtaining content updates.)
- > Which internal systems are/use clients trusted by important servers?
- > Which of the previous systems have security issues that are easily exploited?
- > Which of the previous systems also connect to the Internet?

And this is still just a starting point. As already alluded to, further refinements can easily be made to more narrowly delineate specific attack paths – for example, by filtering on the presence of unsupported software, or specific ports, operating systems, browser types, device types, and so forth. The point is that the richness of the data obtained with Nessus and PVS combined with the flexibility of SecurityCenter's analytic features means it's not only possible but relatively easy to uncover all types of attack paths that an organization has open to modern threats.



Another SecurityCenter feature for revealing complex relationships among systems is Tenable's 3D Tool. In this screen capture, the number of open ports on each host is reflected by the blue columns, while orange and grey lines indicate connections (i.e., trust relationships) between hosts (reported by PVS plugin #0003). The small cloud-like object near the top of the image indicates connections to the Internet.

Attack path response and mitigation. The final step entails actually doing something about the attack paths once they're discovered. To this end, SecurityCenter enables configuration of extensive alerting logic to trigger emails, trouble tickets, and in-system notifications. Pre-defined and customized reports can also be created, saved, scheduled, and distributed to keep both IT operations and line-of-business personnel fully informed of the risks facing systems relevant to their interests and responsibilities.

Moreover, the information gleaned via attack path analysis can be used to ensure underlying vulnerabilities are treated with the appropriate degree of attention. In the absence of other details, the detection of a vulnerability for any given system is a low-level event. This classification is subsequently refined based on factors such as value of the associated system, severity of the vulnerability, and existence of a corresponding exploit. Now, with integral attack path analytics, administrators can further enhance the fidelity of these classifications – and the priority of associated remediation and mitigation efforts – based on yet another important factor: the potential for a vulnerable system to be used as a stepping stone to high-value resources.

BENEFITS OF THE TENABLE SOLUTION

Companies that utilize the Tenable attack path solution to help address the threat of modern malware and the increasing prevalence of targeted attacks stand to gain in a number of important ways. To begin with, significant technical benefits include the ability to:

- Simplify infrastructure and operations. The same integrated set of Tenable solutions can be used to unify all of an organization's vulnerability, event, and compliance management activities, not just those associated with attack path detection and mitigation.
- Focus and streamline day-to-day operations. Over-burdened network administrators can home in on what matters most by being able to easily identify unauthorized/unintended communication paths, detect mis-configured boundary devices, and better prioritize their vulnerability remediation efforts.
- Help establish the need for supplemental countermeasures. Attack path findings can be used to clarify the need for other additional tools and processes, such as next-generation firewalls offering more granular access control, host intrusion prevention, and more thoroughly leveraging security information and event management capabilities.

Equally compelling are the business-oriented benefits of using Tenable. These include the ability to:

- Reduce risk. Common attack paths used by modern malware and targeted attackers can be identified and closed. Remediation efforts for what would otherwise be classified as low-risk vulnerabilities can also be escalated accordingly, thereby reducing the window of opportunity for hackers, spies, and thieves.
- Reduce TCO. In addition to proactively reducing the number of security incidents an organization has and improving operational efficiency, with Tenable there is no need to invest in separate attack path analysis or penetration testing tools.
- Demonstrate compliance. Administrators can fulfill and document adherence to policies, regulations, and requirements pertaining to access control, boundary defenses, continuous monitoring, and truly effective vulnerability management.

ABOUT TENABLE NETWORK SECURITY

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management, and compromise detection to help ensure network security and FDCC, FISMA, SANS CAGn and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit <http://www.tenable.com/>.

Tenable Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
410.872.0555
www.tenable.com