Attack Path Analytics

A Strategic Approach to Vulnerability Remediation
# Table of Contents

Overview ................................................................. 3
Lost in the Noise .......................................................... 3
Using Attack Path Analysis .............................................. 3
  Step One: Data Discovery ............................................ 4
  Step Two: Attack Path Analysis ..................................... 4
  Step Three: Attack Path Response and Mitigation ............ 4
Conclusion ............................................................... 5
About Tenable Network Security ...................................... 5
Overview

Security organizations have no problem finding vulnerabilities on enterprise networks – the volume of security data is constantly growing. The greater challenge is sifting through this data to determine which situations present the greatest risk to the business and prioritizing remediation efforts. Using attack path analytics enables a strategic, risk-based approach to security remediation.

Most security assessments combine broad vulnerability scanning with deep configuration audits of critical devices. This approach leaves many gaps through which attacks can operate. Attack path analytics filter this data with information about host roles, activities, and trust relationships to identify open paths through which malware and attackers can gain access to valuable data and resources.

Lost in the Noise

Attackers typically start by compromising an Internet-facing host with lower levels of defenses. Once in, they use this foothold to progressively exploit trust relationships and compromise other, more critical systems until they reach the sensitive data they are seeking. A system is only as secure as the systems it trusts.

Vulnerability scanners can identify the individual vulnerabilities that attackers use to gain access to sensitive internal resources. But they cannot generally identify trust relationships. Because scanners do not add this essential context to vulnerability information, they cannot accurately portray the real risk of a vulnerability.

The problem is twofold:

1. Vulnerability scanners typically don’t have access to the right data. Although they can identify individual vulnerabilities, they lack essential visibility into:
   - Host activities, such as serving or consuming Internet content
   - Trust relationships between different hosts
   - Available communication paths between different hosts

2. Few of these tools have the means to adequately analyze the data that they do have. They lack flexible and efficient filtering capabilities, support for dynamic asset lists, robust data visualization, and the ability to correlate across the entire spectrum of security events. Without these analytic capabilities, you cannot put together 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, most IT organizations use additional, distinct tools for attack path analysis and penetration testing. This approach has limitations. Attack path tools rely on modeling, which is less accurate than penetration testing. They typically ‘ingest’ point-in-time configurations for an organization’s critical infrastructure devices, such as routers, switches and firewalls. 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.

On the other hand, penetration testing doesn’t scale well. It’s typically not practical (or even possible) to test every potential combination of attack paths.

Another problem with the multiple tool approach is the challenge of integrating them into a cohesive threat management program. Individually, each tool produces a large volume of potentially useful data. But it takes human intelligence to identify and prioritize the threats from that data. Even if your critical systems are all running on fully patched servers protected by firewalls and other security devices, they may still be vulnerable to malware and targeted attacks via the systems that access them.

For example, systems administrators often use their own desktop systems to access high-value servers. They also tend use these same desktop systems for casual Internet surfing or other activities that could introduce malware. So the administrator’s desktop system is a great launch pad for an attack on critical servers. If you are only look at vulnerability data or configuration issues for critical servers, you miss exposures such as this one that can have devastating effect.

Using Attack Path Analysis

Attack path analysis unifies real-time vulnerability, event, and compliance monitoring data for administrators, auditors, and risk managers. It helps them evaluate, communicate, and report information necessary for effective decisions and systems management.
Using attack path analysis, security managers can:

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

A comprehensive attack path analysis process involves three steps that are consistent with the basic vulnerability management lifecycle: discover/assess, analyze, and respond.

**Step One: Data Discovery**

Traditional vulnerability assessment tools lack the data needed to detect open attack paths. They can only obtain critical information, such as an inventory of installed software or patch data, by logging into the systems. Typically, vulnerability scanners only look at external services that are listening on a port – missing client-side software such as Chrome, Firefox and Internet Explorer, to name just a few.

Traditional vulnerability scanners do not examine network data flows to identify specific host activities, as well as which hosts are communicating with each other, over which ports and protocols. Yet this information can be critical. The discovery process should uncover potential attack paths, such as:

- A machine that connects to Facebook or Twitter, and then later to a high-value host
- An internal server that makes an outbound connection to the Internet
- A host participating in or communicating with a known botnet
- The presence of malware on a host
- Misconfigured or missing antivirus software

**Step Two: Attack Path Analysis**

Analysis is the heart of the attack path detection process. Effective analysis combines manual and automated techniques to analyze the data discovered in the previous step for multiple classes of common attack paths, such as:

- Internet-facing services that are known to be exploitable
- Internet-browsing clients that are exploitable
- Servers that trust exploitable clients

Create a series of asset lists that progressively hone in on the desired results. For example, start by asking the question: “Which servers on the enterprise network accept connections directly from the Internet, and where are they located?”

Answering this question will require a combination of external scanning, internal system analysis and monitoring network traffic for systems that accept external connections. Then continue to ask questions to focus in on the real risk:

- Which internal systems connect to the Internet? (You can further refine this question for specific Internet destinations, 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 with 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?

These questions are just a starting point. More detailed analysis can identify the presence of unsupported or illegal software or other business risks.

**Step Three: Attack Path Response and Mitigation**

The final step entails actually doing something about the attack paths you have discovered. Use the information gleaned from attack path analysis to prioritize your responses to underlying vulnerabilities. Without attack path context, the detection of a vulnerability for any given system is a low-level event. You can refine this classification using factors such as the value of the associated system, severity of the vulnerability, and existence of a corresponding exploit. Using attack path analytics adds another critical factor for classifying vulnerabilities and prioritizing remediation efforts: the potential for a vulnerable system to be used as a stepping stone to high-value resources.
Conclusion

Attack path analytics can help companies address the threat of modern malware and the increasing prevalence of targeted attacks. Using attack path analytics, security teams can:

- **Simplify infrastructure and operations.** Comprehensive data analysis can 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 easily identify unauthorized/unintended communication paths, detect misconfigured boundary devices, and better prioritize their vulnerability remediation efforts.

- **Help establish the need for supplemental countermeasures.** Attack path findings can help clarify the need for additional tools and processes, such as next-generation firewalls offering more granular access control, host intrusion prevention, and better security information and event management capabilities.

The business benefits are equally compelling:

- **Reduce risk.** Identify and shut down the common attack paths used by modern malware and targeted attackers. By escalating remediation efforts for what would otherwise be classified as low-risk vulnerabilities, you can reduce the window of opportunity for hackers, spies, and thieves.

- **Demonstrate compliance.** Administrators can fulfill and document adherence to policies, regulations, and requirements pertaining to access control, boundary defenses, continuous monitoring, and 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 CAG, 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.