Blended Security Assessments

Combining Active, Passive, and Host Assessment Techniques

February 7, 2007
(Revision 8)

Renaud Deraison
Director of Research

Ron Gula
Chief Technology Officer

Table of Contents

TABLE OF CONTENTS 2
INTRODUCTION 3
VULNERABILITY ASSESSMENT TECHNIQUES 3
TENABLE'S BLENDED VULNERABILITY ASSESSMENT SOLUTIONS 4
VULNERABILITY ASSESSMENT CHALLENGES AND TENABLE'S BLENDED SOLUTIONS 5
STRENGTHS AND WEAKNESSES OF ASSESSMENT TECHNOLOGIES 9
TENABLE'S SECURITY CENTER IS THE KEY TO BLENDED VULNERABILITY ASSESSMENT AND MANAGEMENT 10
CONCLUSION 10
ABOUT TENABLE NETWORK SECURITY 11

Introduction

Modern enterprise networks face a plethora of technical, political, and business hurdles which make accurate security assessments difficult and costly. Tenable Network Security offers a wide variety of network security assessment technologies which can fit into any environment with minimal impact. This paper will discuss several security assessment challenges facing large enterprise networks and Tenable's solutions to overcome them. This paper emphasizes the benefits of using a combination of host-bases, network, and passive vulnerability assessment technologies.

Vulnerability Assessment Techniques

The network security market has many types of vulnerability assessment product offerings from many different companies who utilize the same words to describe different technologies. As such, we need to take a moment and define exactly what Tenable means by the terms *active*, *passive*, *host-based,* and *blended* network assessments.

Active Assessments

Tenable feels that any use of a network scanner to find hosts, services, and vulnerabilities is a form of active assessment. Regardless if the scan is sending one ICMP packet, or a full fledged DOS attack, any assessment invoking placing packets on the wire to interrogate a host for unknown services or vulnerabilities is an active assessment.

Many network scanners have controls on how aggressive they pursue their interrogation of the network and the servers they encounter. For example, Nessus (http://www.nessus.org) has a concept of "safe checks" which causes it to be less intrusive when performing security audits of network services. Other commercial scanners have a similar mode which is deceptively called "passive scanning". This term will be defined in a moment.

Tenable's experience with the extensive Nessus user community has found that most network outages caused by scanning comes from the underlying port scan and host enumeration. We see little difference in the effect on the underling network when vulnerability scanners are placed into a less aggressive state.

As manager of Nessus, Tenable is regularly contacted by manufacturers of network software and hardware who wish to report a crash condition when their products are port scanned or pinged. For example, Tenable was contacted in 2004 by a phone manufacturer who said its voice over IP application crashed when an out of sequence SYN-ACK packet was sent to it.

The point of the example is that although many active scanners have the ability to reduce the intrusiveness of the checks they conduct, they still place packets on the network which can cause network outages. You simply cannot scan for web servers without sending port 80 packets with a network scanner.

Passive Assessments

Tenable defines sniffing network traffic to deduce a list of active systems, active services, active applications, and even active vulnerabilities will be referred to as a passive assessment. As previously stated, some vendors use this term to signify an active scan.

Tenable also feels that the passive assessment is a continuous effort such that the sniffer performing the analysis can see the network 24x7. An active assessment is really a picture of the network at a point in time. Passive assessments offer a more accurate listing of who is actually using the network.

There are a lot of "gotchas" with passive assessment. For example, how does one know if an IP address is active or not? Consider a DHCP network. Through the course of a week, many hosts will boot up and receive an IP each day. If the host gets a different IP each day, by the end of the week, it will look like many hosts are active on the network.

Host-based Assessments

Any type of security check which can perform a patch level or configuration level check through a command line or API of a given system is considered to be a form of host-based assessment. For example, an active scan may be able to connect to port 21 and observe if an FTP server is running, and even see the version number, but a process with access to the underlying operating system would be able to check the actual patch level of the FTP daemon.

Tenable also sees no difference between performing this task with network-based credentials or with a host-based agent. The distinction is the underlying technology to determine the vulnerability. A host agent who performs command line UNIX manipulation does not run anything different than a network user who can run commands via Secure Shell. Similarly, a host agent who is performing lookups into the Windows registry is not running anything different than a network user running the same APIs.

Tenable's Blended Vulnerability Assessment Solutions

Blended Assessments

Simply put, a "blended" form of security assessment will utilize a combination of active, passive, and host-based techniques. Tenable believes that no one method is better than another. Each has several advantages and disadvantages which can be used to offset a variety of technical and political limitations imposed by large enterprise networks.

The remainder of this paper will discus Tenable's product offerings and how they overcome many of the challenges faced when conducting a large security assessment.

Active Assessments with the Nessus Vulnerability Scanner and Security Center

As previously stated, Tenable manages the Nessus Vulnerability Scanner which is available for UNIX, Windows, and OS X operating systems. Nessus can be managed by the Security Center (formerly Lightning Console) for scheduled scanning, distributed scanning, reporting, and remediation management. Nessus performs more than 10,000 network-based active assessments and Tenable and the Nessus user community continue to add more checks daily.

When deployed in a distributed architecture, full scans of large Class B networks can be completed within just a few hours.

Passive Assessments with the Passive Vulnerability Scanner and Security Center

The Passive Vulnerability Scanner (formerly NeVO) is a passive "sniffer" which will produce a list of hosts, their clients, their services, and any vulnerability associated with the discovered information. Tenable first offered Passive Vulnerability Scanner in October of 2003 and has been continuously improving it. When Tenable's security research group releases Nessus vulnerability checks, similar passive plugins are written for Passive Vulnerability Scanner.

The Windows and UNIX versions of Passive Vulnerability Scanner can be deployed stand-alone and can produce Nessus compatible information. Multiple Passive Vulnerability Scanner sensors can be deployed with a Security Center for distributed management and centralized vulnerability analysis.

When deployed with Security Center, passive assessments are completed instantly. Passive vulnerability data from each sensor is continuously fed into the Security Center. A user viewing the Security Center can see all vulnerability data for each host passively detected in near-real time.

Host-based assessments with Nessus Vulnerability Scanner and Security Center

One of the major challenges faced when maintaining the configuration of large enterprise software deployments is to place an agent on every server. Because of this, Tenable's solution to conduct host-based assessments is agent-less. Tenable's active vulnerability scanner, Nessus, simply requires credentials to log on to any UNIX or Windows host to conduct host-based checks.

The Nessus Vulnerability Scanner supports the ability to log on to UNIX systems via the Secure Shell protocol. It also supports logging on to Windows 2000, XP, and 2003 systems via an NTLM network API. Both techniques allow the vulnerability scanner to have direct access to the Windows registry and the various patch management systems under Red Hat, FreeBSD, Solaris, and other supported UNIX operating systems.

Having access to the underlying configuration of a scanned server increases the speed and accuracy of vulnerability assessment. The absolute patch level can be checked without having to exercise the actual daemons. The speed of checking these systems is also much faster as network latency is not present. Also, knowing the actual patch level of a system can affect how certain false positives and administrator actions are interpreted. For example, if a system administrator has claimed to have patched Apache 1.3, they may have in fact simply disabled it. This allows the Nessus vulnerability scanner to determine the difference between a quick fix and a fully mitigated security issue.

Vulnerability Assessment Challenges and Tenable's Blended Solutions

Challenge #1 - Scans take too long

When scanning a large Class B network, using an active scanner can take a very long time. To make the scan go faster, most solutions opt to reduce the number of ports scanned or the vulnerabilities checked. In some cases, users of active scanning tools will overly focus on specific parts of their network, and not attempt to discover new hosts. Tenable can help in several areas.

First, Tenable allows customers to deploy multiple Nessus vulnerability scanners for intelligent distributed scanning. Security Center is used to associate the scanners with specific target networks and to also load-balance the scans. Security Center allows scans to be scheduled, paused, and even executed during specific outage windows when scanning may only be allowed.

Second, by utilizing the Passive Vulnerability Scanner, a user will automatically see a wide variety of vulnerabilities, ports in use, and active networks. The active networks advertise themselves. When combined with the Security Center, the data discovered by the Passive Vulnerability Scanner can be used to identify networks and vulnerabilities which should be scanned. For example, one of Tenable's customers deployed the Passive Vulnerability Scanner in front of two "Class B" networks. They had allocated the lower 100 "Class C" networks in both "Class B" networks, and were stunned to discover more than a dozen rouge networks had been configured without their knowledge. With the Security Center, they were able to conduct an active scan to compliment the passive vulnerabilities initially reported by the Passive Vulnerability Scanner.

And finally, if given host-based credentials, the Nessus Vulnerability Scanner can conduct a complete audit of all patches, usually in less than 30 seconds. The main speed advantage over an active scan is that port scanning, host enumeration, and connecting to each network service does not occur.

Challenge #2 - We do not have permission to scan

For many reasons, it is very common for network security groups in large enterprises to be barred from scanning specific hosts or networks. The reasons are often political. Sometimes they have to deal with the fear that an active scan will impact the performance or availability of a network resource. Other times, a server group will be barred from extending host-based credentials to a security group due to a restrictive security policy. Tenable's Passive Vulnerability Scanner can help.

The Passive Vulnerability Scanner is deployed like a sniffer and is focused on a specific range of network addresses. When it observes a network session, it performs a wide variety of security audits. It first keeps an active model of "active" hosts. Each time a network session is discovered, its model of the network is updated. Each session is used to identify which hosts are alive, which are "serving" applications, what ports are being browsed, and who is talking to whom. With the Passive Vulnerability Scanner, any particular host of interest will have a list of all open ports (such as a web server on port 80), any ports that have been browsed (such as visiting the Internet on port 80), and a list of all hosts which have communicated with it per port (such as a list of all hosts who have communicated with it on port 22).

Although this information is extremely useful, the Passive Vulnerability Scanner's focus is actually finding evidence of real vulnerabilities and applications. When the Passive Vulnerability Scanner evaluates a network session, it attempts to identify what the service or client is, and if any vulnerabilities are associated with it. For example, the scanner can find all of your SSH vulnerabilities at both the client and the server.

Challenge #3 - Communicating which vulnerabilities to fix to each administrator is difficult

The Security Center can be used to allow a security group to communicate with several hundred network administrators. The Security Center will provide any detected vulnerability

to an administrator if they want to see it. However, most network administrators do not conduct vulnerability scanning often enough, nor do they have the experience to discern false positives or set priorities in which security holes should be fixed.

The Security Center allows the security group to see the big picture and also assign "asset values" to each detected server. The big picture allows the group to see which vulnerabilities are present across many different forms of network assets. This allows them to diagnose common problems and identify a trusted solution. This solution can be delivered to just the administrators which are affected by the vulnerability. For example, when detecting an insecure SNMP community string, separate "fix" information can be sent to administrators who manage different asset types such as Cisco routers, Windows 2000 web servers, and HP laser printers. This minimizes the time spent by both the security group and the administrator.

Knowledge of vulnerabilities is crucial to be successful when communicating with an IT or network engineering group. Passive assessments allow early detection of vulnerabilities. Host-based assessments allow highly accurate assessments of the underlying patch level and can also confirm when a patch has been upgraded.

Challenge #4 - I can't see "behind" our firewalls

Within large enterprise network that have deployed many firewalls between their networks, effective assessments of trust relationships, exposed services, and the network infrastructure can be difficult. Tenable has two solutions in this area.

First, the Security Center can be used to deploy distributed active Nessus vulnerability scanners such that some are "behind" the firewall and others are "outside". Normally, the internal scanners will scan and report on the machines inside the firewall. However, the external scanners can be used to scan the addresses behind the firewall to see what is exposed. If needed, this can be done on a daily basis to see if the firewall is allowing new services it should not have.

Second, the Passive Vulnerability Scanner can be placed inside or outside of the firewall to verify the ports and services traversing it. The Passive Vulnerability Scanner will accurately report trust relationships, open ports, and browsed ports. This information can be used to verify firewall rules and identify trust relationships.

Challenge #5 - Verifying patch levels is difficult

In many enterprise networks, verifying how patches are deployed is exceeding difficult. With an active or passive scanner, the presence of a patch is not directly tested. Instead, active and passive scanners look for artifacts in how network services behave and respond. Because of this, continued monitoring and "rescanning" of networks must be accomplished to verify patch levels.

With the Nessus vulnerability scanner, host-based credentials for UNIX or Windows servers can be used to assess the specific patch level of each host. This drastically reduces the time it takes to scan a host and provides little doubt if a system has been patched or not.

Challenge #6 - Stop crashing my routers

Regardless of active scanning technology, vulnerability and port scanners have a reputation for crashing network devices. The reason is that many network devices track a finite

number of network sessions which are defined by a sequence of source and destination IP addresses and ports. For any given network, a certain number of machines will be checking mail, browsing the web, or sharing files. Some power users may run P2P or chat tools, and some servers may be serving several hundred connections at one time.

However, when a port scan is launched, each host may be tested for several thousand open ports. It is this huge jump in network activity that can make a "class c" LAN look like it is carrying the network sessions of a "class b". If any network device is not equipped to keep track of these extra sessions, real sessions can be dropped. This means lost VPN, network management, email, and database updates. If the device is not robust, the device may reboot or cause a hard reset.

Tenable's Passive Vulnerability Scanner has the advantage of reporting a majority of the vulnerabilities detected with an active scan, but without the potential impact of injecting packet probes onto the network. The Passive Vulnerability Scanner is also more accurate in finding open ports. For a full active scan of TCP ports, a user would need to define a port range of 1 through 65,535. This takes an extremely long time and most users simply scan ports 1 through 1024. With the Passive Vulnerability Scanner, it simply "sniffs" traffic. If it sees that a particular server has port 37462 open, it logs it. Many of Tenable's customers initially report that the Passive Vulnerability Scanner has found many high-port mail relays, backdoors, and unauthorized command shells.

Challenge #7 - We want to keep track of "client side" vulnerabilities and usage

Most active network scanning tools (including the Nessus Vulnerability Scanner) are not equipped to scan for client-side vulnerabilities. Instead they are focused on vulnerabilities in network services such as Apache or Secure Shell instance. To get an idea of a large enterprises exposure to a particular client side vulnerability, most organizations resort to an exhaustive network wide deployment of host-based software management or host-based vulnerability scanning. Many times, these deployments are costly, impact the system administration of desktops devices, and cause network instability.

Tenable's Passive Vulnerability Scanner can assess a wide variety of vulnerabilities in client applications such as Internet Explorer, the Eudora email client, and even UNIX script tools such as the command line *wget* web browser. Tenable has deployed the Passive Vulnerability Scanner on common web sites like http://www.nessus.org and has tracked more than 20,000 vulnerable clients in a day's worth of visitors. The Passive Vulnerability Scanner searches for client side security problems at the same time it searches for server side security problems.

Challenge #8 - Correlating my vulnerabilities with my IDS logs is difficult

The Security Center from Tenable is ideally suited to perform this task. Solutions which simply take a copy of "the last scan" and use it for correlation are not getting the full benefit of vulnerability assessment. Tenable has integrated support for many leading IDS solutions with the vulnerabilities obtained by Nessus and the Passive Vulnerability Scanner through active, host-based, and passive analysis. For example, when Security Center receives a report about an out of date SSH service, it does not matter if that information came from a Nessus scan of an SSH server, a host-based patch level check, or through passive analysis. The vulnerability will be automatically correlated with the relevant IDS events.

Strengths and Weaknesses of Assessment Technologies

Active Scanning Strengths

All active scans can be independent of any network management or system administration information. This makes for a much more "honest" security audit of any system or network. Active scans can provide extremely accurate information about what services are running, what hosts are active and if there are any vulnerabilities present.

Active Scanning Weaknesses

Unfortunately, the information discovered by an active scan may be out of date as soon as the scan is completed. Many small changes to the network topology, such as the addition of new hosts, will go unnoticed until the next active scan. To compensate for speed and potential adverse impact, many enterprise network security groups will minimize the ports and the vulnerabilities scanned for which actually ends up discovering a subset of the real vulnerabilities. Active scans can also generate an excessive amount of firewall and intrusion detection logs.

Passive Scanning Strengths

The greatest strength of a passive scan is the lack of any impact to the network and the minimal time it takes to find real results. A passive scanner operates 24x7 and when you want to know what vulnerabilities it has seen, a report can be immediately generated. Passive scanning also has an advantage of discovering client side vulnerabilities and vulnerabilities in Intranet networks we do not have permission to scan.

Passive Scanning Weaknesses

Unfortunately, for a passive scan to work, a detectable host must elicit or respond to a packet. If a server never communicates on the network, the Passive Vulnerability Scanner will never see it. Tenable's Passive Vulnerability Scanner has been deployed on many large enterprise networks. In most cases, the Passive Vulnerability Scanner typically discovers more information passively than the customer was finding with purely active techniques.

The world's most insecure backup DNS server will not be detected if no one talks to it. However, Tenable has found that most enterprise networks have large amount of email, P2P, web browsing, file sharing, and network management traffic which advertise themselves to the Passive Vulnerability Scanner. As a worst case, the Passive Vulnerability Scanner will identify the presence of a server at the same time a probing hacker does.

Host-based Scanning Strengths

The greatest strengths that host-based scanning has going for it are speed and accuracy. It takes the Nessus Vulnerability Scanner less than thirty seconds in most cases to complete an audit of all patches for a Red Hat or Windows 2000 server if credentials have been provided. This audit consists of well-known APIs and patch management tools provided by the underlying operating system. This makes things much simpler and efficient than an active or passive scan. Both of those techniques involve implementing models of a vulnerability, and looking for a specific stimulus and response. Compared to a check for a specific patch with a known serial number, the information searched for with an active or passive technique is much more complex.

Host-based Scanning Weaknesses

The largest weakness for host-based scanning with the Nessus Vulnerability Scanner is that credentials need to be supplied. Often, obtaining these credentials is more of a political battle than a technical battle. In many cases, an IT group may not appreciate giving a security group the ability to audit it at any time.

An advantage of the Security Center is that the trust relationships between the scanners and the target systems can be managed by individual Security Center users. This means that if an administrator who was managing ten DNS servers wanted to grant credentials just to scan her servers, she could do it. The security managers of the Security Center would be able to see the results, but would not have any added rights to scan with those host-based credentials.

Tenable's Security Center is the key to Blended Vulnerability Assessment and Management

For a large enterprise with many different networks, network administrators, and security personal, the Security Center is ideal for managing security. It can detect security issues through "blended" vulnerability assessments by utilizing host-based, network scans, and passive scans. It can communicate this information to senior management in business terms they understand and it can also communicate relevant information to network and system administrators in their language.

With the Security Center, management of host-based, network-based, and passive vulnerability assessments is very easy. Any user with the proper credentials can perform analysis of the vulnerabilities discovered by any form of blended assessment. The Security Center has many ready-to-run policies which will invoke only active or host-based forms of assessment. Vulnerabilities detected can be filtered with the click of a button by asset type, by vulnerable port, or by network address. This makes it very easy for users to run their own form of assessment, or analyze the results of someone else's assessment of their network.

Conclusion

Tenable's solutions solve a variety of vulnerability assessment problems faced by large enterprise networks. No one combination of Tenable's products will fit each unique enterprise's combination of technical and political requirements. It is Tenable's depth of product offerings and vulnerability assessment techniques which makes it fit to function in a large and complex network infrastructure.

About Tenable Network Security

Tenable, located in Columbia, Md., develops enterprise security solutions that provide vulnerability management, intrusion detection, and security event notifications across entire organizations for effective network security management. Tenable is uniquely positioned to detect vulnerabilities with active and passive scanning and analysis, and host-based patch monitoring for enterprise networks. Key product lines include: Nessus Vulnerability Scanner, the leading global technology utilized for vulnerability scanning; Passive Vulnerability Scanner, for continuous passive vulnerability monitoring; Security Center, for enterprise security management; and Log Correlation Engine, for secure log aggregation and analysis. For more information, please visit us at http://www.tenablesecurity.com.

TENABLE Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
TEL: 410-872-0555
http://www.tenablesecurity.com