Blended Security Assessments

Combining Active, Passive and Host Assessment Techniques

May 11, 2011

(Revision 10)

Renaud Deraison
Director of Research

Ron Gula
Chief Technology Officer

Table of Contents

Introduction **3**

Vulnerability Assessment Techniques **3**

Active Assessments 3
Passive Assessments 3
Host-based Assessments 4

Tenable's Blended Vulnerability Assessment Solutions **4**

Blended Assessments 4
Active Assessments with Nessus and the SecurityCenter 4
Passive Assessments with the PVS and SecurityCenter 4
Host-based Assessments Nessus and the SecurityCenter 5

Vulnerability Assessment Challenges and Tenable's Blended Solutions **5**

Strengths and Weaknesses of Assessment Technologies **8**

Active Scanning Strengths 9
Active Scanning Weaknesses 9
Passive Scanning Strengths 9
Passive Scanning Weaknesses 9
Host-based Scanning Strengths 9
Host-based Scanning Weaknesses 9

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 that make accurate security assessments difficult and costly. Tenable Network Security, Inc. offers a wide variety of network security assessment technologies that 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-based, network and passive vulnerability assessment technologies.

VULNERABILITY ASSESSMENT TECHNIQUES

The security market has many types of vulnerability assessment product offerings from many different companies that 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 to manage how aggressively 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" that causes it to be less intrusive when performing security audits of network services. Other commercial scanners have a similar mode that is deceptively called "passive scanning". This term will be defined in the next section.

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

As the 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 that can cause network outages. You simply cannot scan for web servers without sending packets to port 80 or 443 using 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 as a passive assessment. As previously stated, some vendors use this term to signify an active, but "less intrusive" 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 given point in time. Passive assessments can also offer a more accurate listing of who is actually using the network.

There are many "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 that can perform a patch level or configuration level check through the 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 determine 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 presence of a vulnerability. A host agent that performs command-line Unix manipulation does not run anything different than a network user who can run commands via Secure Shell (SSH). Similarly, a host agent that is performing queries 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" security assessment will utilize a combination of active, passive and host-based techniques. Tenable believes that no single method can capture the entire picture. Each has several advantages and disadvantages that can be used to offset a variety of technical and political limitations imposed by large enterprise networks.

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

Active Assessments with Nessus and the SecurityCenter

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 SecurityCenter for scheduled scanning, distributed scanning, reporting and remediation management. Nessus performs more than 43,000 network-based active assessments and Tenable continues to add new checks daily. In addition, Nessus can be configured to perform more specialized scans such as web application vulnerability scans and credentialed database scans that are not available using passive or host-based methods.

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

Passive Assessments with the PVS and SecurityCenter

The Passive Vulnerability Scanner (PVS) is a passive "sniffer" that will produce a list of hosts, their clients, their services and any vulnerability associated with the discovered

information. Tenable first offered PVS (formerly NeVO) in October of 2003 and has been continuously improving it. When Tenable's security research group releases Nessus vulnerability checks, similar plugins are written for the PVS.

PVS can be deployed stand-alone and can produce Nessus-compatible information. Multiple PVS sensors can be deployed with a SecurityCenter for distributed management and centralized vulnerability analysis.

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

HOST-BASED ASSESSMENTS NESSUS AND THE SECURITYCENTER

One of the major challenges faced when maintaining the configuration of large enterprise software deployments is the placement of an agent on every server. This approach creates a considerable overhead, as administrators must spend time installing and updating the agent software. To overcome this, Tenable enhanced Nessus to conduct host-based assessments using system credentials rather than a software agent.

The Nessus vulnerability scanner supports the ability to log on to Unix-based systems via the SSH protocol using username or certificate authentication. It also supports logging on to other system types such as Windows XP, Vista and 2008 via SMB account or Kerberos. These 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 direct access to the operating system can result in more accurate findings as Nessus can examine the system to see if a given service has "backported" patches (i.e., installed critical security patches without changing the version of the software). In addition, this level of access permits Nessus to optionally perform configuration audits of web servers and databases by comparing their configuration files against known good settings.

Having access to the underlying configuration of a scanned server increases the speed and accuracy of vulnerability assessment. The exact patch level can be checked without having to exercise the actual daemons. The speed of checking these systems is also considerably faster as network latency is not an issue. In addition, 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

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 or specific services, 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 is permitted.

Second, by utilizing the PVS, 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 PVS can be used to identify networks and vulnerabilities that should be scanned. For example, one of Tenable's customers deployed the PVS 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 rogue networks had been configured without their knowledge. With the Security Center, they were able to conduct an active scan to complement the passive vulnerabilities initially discovered by the PVS.

Finally, if given host-based credentials, the Nessus vulnerability scanner can conduct a complete patch audit of all hosts, typically in less than a minute. The main speed advantage a host based audit has over an active scan is that port scanning, host enumeration and connecting to each network service does not need to 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 restricted from scanning specific hosts or networks. The reasons are often political, not technical. Sometimes they relate to the fear that an active scan will impact the performance or availability of a network resource. Other times, a server group will be restricted from extending host-based credentials to a security group due to a restrictive security policy. Tenable's PVS can help.

The PVS 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 on the traffic it monitors. It first keeps a 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 PVS, any particular host of interest will have a list of all open ports (e.g., a web server on port 80), any ports that have been browsed (e.g., visiting the Internet on port 443) and a list of all hosts that have communicated with it per port (e.g., a list of all hosts who have communicated with it on port 22).

Although this information is extremely useful, the PVS's focus is actually finding evidence of real vulnerabilities and applications. When the PVS 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 critical vulnerabilities to each administrator is difficult

SecurityCenter can be used to allow a security group to communicate with hundreds of network administrators. SecurityCenter will provide any detected vulnerability to an administrator of the system 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 for what security holes should be fixed first.

SecurityCenter allows the security group to see the big picture and assign "asset values" to each detected server. The big picture allows the group to see what 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 who 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.

To be successful in communicating with an IT or network engineering group, knowledge of vulnerabilities is crucial. Passive assessments allow for 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 SecurityCenter 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 which services are exposed. If required, this can be done on a daily basis to see if the firewall is allowing new services it should not be.

Second, the PVS can be placed inside or outside of the firewall to verify the ports and services traversing it. The PVS 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 exceedingly difficult. With an active or passive scanner, the presence of a patch is not directly tested. Instead, active and passive scanners look for specific mannerisms in how network services behave and respond. Because of this, continued monitoring and "rescanning" of networks must be performed 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 that 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. This huge jump in network activity 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 PVS has the advantage of reporting a majority of the vulnerabilities detected with an active scan, but without the potential of sending packets and adversely affecting network devices. The PVS 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 the privileged ports (1 through 1024). With the PVS, it simply "sniffs" traffic. If it sees that a particular server has port 37,462 open, it logs it. Many of Tenable's customers initially report that the PVS 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, Oracle or SSH. 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 PVS 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 agent. Tenable has deployed the PVS 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 PVS 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

Tenable's Security Center is ideally suited to perform this task. Solutions that 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 PVS 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 which services are running, which 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 and end up discovering only a subset of the real vulnerabilities. However, this issue is mitigated largely by the use of credentialed scans with Nessus' built-in Netstat port scanner. 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 network impact and the minimal time it takes to find real results. A passive scanner operates 24x7. When you want to know what vulnerabilities it has detected, a report can be generated on the fly. Passive scanning also has an advantage of discovering client side vulnerabilities and vulnerabilities in intranet networks that may not be in the immediate scope of a given 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 PVS will never see it. Tenable's PVS has been deployed on many large enterprise networks. In most cases, the PVS 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 a large amount of email, P2P, web browsing, file sharing and network management traffic that advertises them to the PVS. As a worst case, the PVS 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 are speed and accuracy. It takes the Nessus vulnerability scanner less than a minute 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 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 must 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 to just 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.

SECURITY CENTER IS THE KEY TO BLENDED VULNERABILITY ASSESSMENT AND MANAGEMENT

For a large enterprise with many different networks, 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 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 that 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 that make it fit to function in a large and complex network infrastructure.

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/.

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