TENABLE
Network Security®

Dedicated and Distributed Vulnerability Management

December 2002
(Updated February 2007)

Ron Gula
Chief Technology Officer

Table of Contents

Introduction

It has become best practice for organizations with large networks to conduct “vulnerability assessments”. These assessments produce a list of network computers which have security problems that may allow information to leak out unauthorized, or possibly allow an intruder to enter a computer illegally. Typically, these vulnerability assessments are conducted on a periodic basis, by a select group of people specifically responsible for computer security within the organization, or by a third party such as a consultant group on a periodic basis.

Unfortunately, this manual approach is too slow to keep up with the fast pace that vulnerabilities are disclosed to the general public. It is also the wrong approach to provide information to all of the system administrators within a large organization whose job it is to secure the detected vulnerabilities.

This paper will outline the need for a dedicated approach to conducting vulnerability assessments and also address many of the advantages of distributed vulnerability scanning. We will describe how a dedicated solution to conduct vulnerability assessments can approach the type of solution to effect real vulnerability management.

The Need for Vulnerability Assessment

Every year, the Computer Emergency Response Center (http://www.cert.org/) publishes more and more vulnerability disclosures. These disclosures come from product vendors, security research companies, and many other sources. In 2000, CERT reported 1,090 vulnerabilities. In 2001, this number rose to 2,437 vulnerabilities, and by Q3 of 2002, over 3200 have been reported.

Of course, each one of these vulnerabilities are not present on every network, and each vulnerability is not as serious as the next one, but there is no way to know the impact of the vulnerabilities on a given network without looking at how they affect the given network directly. For example, a simple vulnerability in a web service application which allows the remote browsing of the contents of a directory may seem innocuous, but combined with a server that processes credit card information, this vulnerability could disclose end-user private information.

The challenge of the security professional, whose job it is to assess a network for each of these potential vulnerabilities, is also quite daunting. To do this, automated tools are used to catalog each of the computers on a network, and then to interrogate the discovered computers for any known vulnerabilities. Typically these automated tools are run from a single computer and have a database of the top 1000 vulnerabilities. When run, they produce reports about the types of computers discovered, and lists of the potential vulnerabilities found.

Once the vulnerability assessment is completed, the information is communicated to those who can fix the problems discovered. This starts a feedback loop of scanning, patching, and then re-scanning to discover new vulnerabilities, or vulnerabilities which were known and yet to be mitigated.

Manual Vulnerability Assessment

The process of having a security professional conduct an automated vulnerability scan is referred to as a manual vulnerability scan. Even though the tool used is highly automated, the process of scheduling a scan, selecting the network targets and producing a report is highly subjective and may change from scan to scan. Typically, there may be a longer time between scans associated with this approach due to scheduling, availability of consultants, and maintenance windows.

Advantages

Lest the reader conclude that the author is against professional security testing, we will now point out the many advantages of this approach. Please keep in mind that our goal is to illustrate the differences between a manual scan and dedicated vulnerability assessment.

1. Manual scans are typically more thorough

   When compared with a solution that simply checks for a large number of vulnerabilities on a regular basis, a manual scan is much more likely to discover unique vulnerabilities. Although you may hear about how a particular vendor's vulnerability scanning solution "emulates a hacker", the truth is that these solutions do not stand up to the types of information that can be discovered by an experienced penetration tester. It is also much more likely that a manual penetration test will be able to chain together many smaller vulnerabilities to uncover a major security flaw.

2. Manual scans can investigate human and physical weaknesses

   Typically, a manual scan (most normally associated with an outside consultant) will also include an investigation into the practices of the IT and network engineering staff, as well as an evaluation of the security policy, physical security and possibly even incident response procedures.

3. Manual scans can be very unbiased

   A manual scan that is conducted by a third party is also much less likely of being biased. This can include tainting of the report to reflect more or less seriousness of discovered vulnerabilities. It can also be advantageous when discovering systems on a network. For example, someone that is familiar with a network may assume that just because a target machine has the IP address of the laser printer, that it is indeed the laser printer and not try more exhaustive attacks.

4. Manual scans can identify architectural flaws in security

   An experienced security auditor should be able to make generic recommendations that have extremely high impact to reduce the overall security exposure. This may include subtle changes to the security policy, firewall policy, maintenance of systems, education of network users, and so on.

Limitations

Although the manual approach has many advantages, in practice, many networks continue to fail security audits and contain high numbers of security flaws. The point of a dedicated vulnerability assessment solution is to address many of these shortcomings.

1. Manual scans can be painfully slow

To conduct a scan of a class B (over 60,000 potential IP addresses) can take one computer a full week to conduct a scan. This is very difficult because you may be paying for the engineer's or consultant's time to complete the scan. During this time, the topology of the network may radically change as new systems are moved, added and removed.

2. Manual scans can cause network outages

   Modern network applications are not as robust as you may believe. It is very easy to conduct a localized denial service attack on applications which are poorly written, or have high CPU consumption. Conducting a manual scan of a network can inadvertently cause a network crash. Also, the act of network discovery can cause stability issues with firewalls, load balancers, routers and switches. To increase performance, modern network hardware attempts to accelerate network transactions by keeping track of network sessions. When faced with large amounts of port scans, i.e. scans which launch more than 10,000 scans per second, many of these hardware and software optimizations become stressed and fail.

3. Manual scans are difficult to communicate

   Once a scan is completed, a worse case scenario that many Chief Security Officers face is the realization that fixing all of the detected vulnerabilities is difficult. There is ample room for system administrators to claim lack of resources, lack of patches, or in some cases, lack of direction. In some cases, it can be very difficult to find out who even "owns" a particular server to even have a conversation with them about patching it. As such, many reports are read and then shelved. In other cases, the security group presents the IT or network organizations with unrealistic security requirements, which creates tension and a culture of where the groups are working against each other instead of being cooperative.

Advantages of Dedicated Vulnerability Assessment

When we say "Dedicated Vulnerability Assessment" we are talking about deploying a solution for a large organization that should have the following properties:

Predictable Scanning

The solution should be able to scan the network at a regular interval. This should include being able to scan sensitive systems during maintenance windows or off-hours. When scans start and stop, they should notify people so that if something goes wrong, an analysis of the impact of the scan can be conducted. The same network ranges should be tested repeatedly for discovery of missing and new systems.

The advantage of predictable scanning is that it becomes part of network operations. It may take time to create a culture to accept scans on a regular basis, but it is a very good way to catch new vulnerabilities in a short amount of time. Once this becomes part of the network culture, it is also less likely that network users will run unauthorized servers and applications. It can also become a very good way to prevent the use (or detect the use) of file sharing applications such as Bear Share, WinMX and Goto-My-PC.

Incremental Tracking of Trends

The solution should track the trend of vulnerabilities and network information. It would be great to see over time the change in deployed operating systems for example. It is of even more use to identify which subnets are always lagging behind in patches or have the most vulnerabilities. Later we will discuss correlation with intrusion detection systems. Some organizations have drawn parallels between poor security and the number of intrusions (which should be obvious), but they have then related this to the cost of responding to incidents and used this as a justification for more resources.

The direct advantages of trending vulnerabilities should be obvious to the reader. One advantage of conducting this trend that may not be so obvious is that the solution should make available, the most recent snapshot of the network's systems and vulnerabilities. This is vital to determine what the current baseline is. Typically, a manual scan may compare a scan of last quarter with one from this quarter to find differences. With a dedicated solution that kept a database, "new" systems can be identified as soon as they are discovered. For example, if a baseline existed and a new Windows 2000 server was added to the DMZ, this could be detected, even though it may not have any vulnerabilities on it. This would allow a security group to keep better track of what is occurring on a network.

"Appliance" and Web Solutions

Any dedicated solution should take advantage of modern network infrastructure. Deploying the vulnerability assessment solution on a dedicated platform guarantees the proper network availability, bandwidth and visibility into the scanned networks.
Conducting scans from outside of the network is interesting, but is only an external scan. Placing a dedicated scanning server within the infrastructure allows for better visibility. Deploying on an appliance (or dedicated server) also provides the opportunity to harden the system and control access to it. Compared to a mobile scanning laptop, this solution is much more secure. The solution should also be able to securely publish the results of its scans via a web interface. This would guarantee that almost every system administrator would be able to view the vulnerability results for their system. Compared to systems which are only viewable on X-windows or the Windows operating system, distributing the raw results can be difficult.

Automatic Updates of Vulnerability Checks

It should go without saying that a vulnerability solution that is not updatable with the latest vulnerability checks will become less and less relevant and provide a false sense of security. Almost every vendor solution includes some sort of live updates. However, a solution that can schedule the updates such that it can guarantee that the most recent checks are available is desirable. Manual updates are convenient, but make it difficult to set a policy of synchronizing every 24 hours. Keep in mind that vulnerabilities are published so fast, one update can be the difference between finding a major vulnerability which is being actively exploited today, versus finding it two or three days later.

The advantages of automatic updates include the confidence that your vulnerability scanner is checking for the latest potential problems.

Distribution of Results and Tasking to End-Users

This is a key advantage of a permanent vulnerability assessment solution. With manual scanning, the distribution of vulnerability information can be chaotic. How do you get the vulnerability information for just one system administrator to them? A dedicated solution can slowly build a list of end-user or system administration owners though population of a database. When it becomes a corporate requirement to use such a system, the management of system administrators will populate the system with a hierarchical approach. For example, the manager of a network may know that she has ten administrators for fifty machines and will enter each one into the system of “approved” end-users.

Although this may seem difficult, it has two advantages. First, it provides the system with a chain of ownership. Any server can be associated with one or more end users, and the end users can be associated with specific organizations. This provides accountability. Second, when a particular system is found vulnerable, the “owner” can be quickly contacted.

For patching systems, many solutions exist which allow security personal to task IT and network engineering personal with patching and mitigation orders. These systems typically fail in large organizations. This is because the security group rarely has a good understanding of the realities facing operating a large network and the folks that are supposed to “fix” these vulnerabilities do not work for the security group.

What is needed is a flexible way for the security group to issue recommendations that are generally followed by the rest of the organizations. It is important for the end user system administrators to have flexibility in how they patch something. First off, it is important that any dedicated system be flexible in the recording of how a vulnerability is mitigated. For example, a web server may be found to be vulnerable, but to also be not needed at all. In this case, it should be up to the system administrator to have the flexibility to simply disable the web server. Any dedicated system should be able to record the recommendations of the security group, and the remediation actions that the system administrators undertake.

The advantage of this approach is flexibility and accountability. The security group is able to issue information which is helpful. The system administrators are also able to record what they do to fix the security problems. This provides a feedback loop which can also identify problems which bring back old vulnerabilities.

Scanning can be Tuned to Minimize Impact

With a dedicated vulnerability assessment solution, the entire system of system administrators and security personal can provide feedback to tune the system. For example, if a certain vulnerability check crashed a DNS server, this check could be disabled until the server is protected. This can make for very efficient scanning. Also, some vulnerability checks will produce false positives in that they say a particular vulnerability exists, when in fact it does not. Working with system administrators can eliminate these false positives over time.

The advantage of tuning a vulnerability scan results in better vulnerability information. With a dedicated system and scans occurring often, the scan can be modified to avoid outages and product better results.

Correlation with Intrusion Detection Systems

One of the last basic advantages that a dedicated vulnerability assessment solution can provide is direct correlation with intrusion detection systems (IDS). Many intrusion detection systems produce thousands, if not tens of thousands of alerts a day. A majority of these alerts are valid attacks, but are not valid compromises. Many are false positives that have detected an attack that would not work against the target system because it is not vulnerable to the attack.

By employing a solution that can correlate IDS events with known vulnerabilities, high quality IDS alerts can be obtained. It is fairly trivial to build a list of IDS events that correlate to known vulnerabilities through the use of the Common Vulnerabilities and Exposures database (http://cve.mitre.org/). This database has cataloged the many thousands of vulnerabilities and assigned unique serial numbers to them. This allows many security vendors to maintain their own unique intellectual property of security knowledge, but reference the relevant CVE information for correlation and more information.

From a vulnerability assessment standpoint, a high quality IDS event is one that we know is a “real” compromise or information leak. For example, if we knew that one system in a server group were vulnerable to a particular vulnerability, and we had an IDS event occur which went against that same vulnerability, we could conclude that particular IDS event had a much higher chance of being successful than other IDS events which did not go against known vulnerabilities. Put another way, IDS solutions tend to generate thousands of events, many of which are not applicable or have no chance of succeeding. Only alerting on the events which targeted vulnerable systems can greatly reduce the signal to noise ratio of IDS alerts.

One last advantage of IDS correlation with known vulnerabilities is to assess the intent of what a hacker may be attempting when targeting a vulnerable server. The server may indeed have other vulnerabilities that the hacker had tried to exploit which were not detected by the IDS. If a targeted system has many vulnerabilities and is attacked, it raises the importance that the machine be secured and vulnerabilities mitigated.

Advantages of Distributed Vulnerability Assessment

Although we have been discussing some of the advantages of dedicated vulnerability assessment solutions, deploying a distributed vulnerability detection system still has more advantages. Some of these are discussed below:

Speed

When scanning a large network, the speed of the scan is paramount. Slow scans can take days if not weeks to scan very large networks. It is quite common for manual scans to break up a large network by subnet and scan them individually.

By distributing the scan across many nodes, parallel scanning can occur. When scanning in parallel, the list of vulnerability checks and target IP addresses is split up between each node. Since vulnerability scanning is a combination of CPU intensive checks, and a good deal of time waiting for responses from target machines, splitting up the effort can greatly decrease the time it takes to scan a network.

Typical scans sweep the target network to find the active hosts, sweep the hosts to find the active ports, and then interrogate each port to find active vulnerabilities. This process involves a lot of checks which send specific packets or queries and then wait for the reply. In some cases, the scanner never gets a reply and it has to wait 30 seconds or so to “time out”. For example, checking a host to see if it is alive may require 3 seconds. For 60,000 hosts this can be done in parallel by a single computer, but only so many hosts (possibly

100) can be done at the same time. Splitting this among 5 or more scanners can allow scans to proceed much quicker.

An advantage of speed is that an organization can quickly access its network structure and build a topology without having to wait 24 hours or longer. If a new security flaw is discovered and it is a priority to find all of the servers who have this problem, accessing a very large network for it can occur in a matter of minutes with a distributed solution.

Minimal Network Infrastructure Impact

Even though we have more systems conducting scans across a network with a distributed approach, there can be less impact to the network infrastructure. By placing scanning agents closer to their target networks, the port scans and other probes do not flow across the core router and switching fabric. This causes less network outages and performance degradation, rather than pumping 15,000 packets or so per host against up to 60,000 hosts.

As was discussed in a previous section, modern networking equipment is over-optimized to accelerate network transaction on a per-session basis. When these devices are presented with high new-session rates, or simply high numbers of sessions, there can be problems. Also, networks scans can produce large numbers of packets designed to exercise their targets. These odd packets can stress switches and routers. If network equipment is not robust, the simple act of carrying an attack from one side of the network to the other may be enough to crash a router or server.

Another advantage of placing scanner agents closer to the target networks is that the scans may take place behind a firewall. Having to reconfigure a firewall to let a security scan in can be a troublesome security task. Likewise, scanning a network protected by a firewall will let you see how the external world to the network sees it, but many internal vulnerabilities can go undetected.

Conclusions

Large networks should deploy dedicated vulnerability assessment systems to truly participate in the benefits of vulnerability discovery. They should also continue to conduct manual vulnerability assessment solutions as well. In essence, corporations should take the next step and participate in vulnerability management and create a culture through their organization of minimizing vulnerabilities

About the Author

Ron Gula is a Founder and Chief Technology Officer of Tenable Network Security. Tenable is a company that produces the Lightning Proxy for high-speed Nessus vulnerability scans and the Security Center (formerly Lightning Console) for correlating IDS data with vulnerability data and making it available to multiple people in multiple organizations. Previously, Mr. Gula was the original author of the Dragon IDS and CTO of Network Security Wizards which was acquired by Enterasys Networks. At Enterasys, Mr. Gula was Vice President of IDS Products and worked with many top financial, government, security service providers and commercial companies to help deploy and monitor large IDS installations. Mr. Gula was also the Director of Risk Mitigation for US Internetworking and was responsible for intrusion detection and vulnerability detection for one of the first application service providers. Mr. Gula worked for BBN and GTE Internetworking where he conducted security assessments as a consultant, helped to develop one of the first commercial network honeypots and helped develop security policies for large carrier-class networks. Mr. Gula began his career in information security while working at the National Security Agency conducting penetration tests of government networks and performing advanced vulnerability research.

About Tenable Network Security

Tenable, headquartered in Columbia, Md., USA, is the world leader in Unified Security Monitoring. Tenable provides agent-less solutions for continuous monitoring of vulnerabilities, configurations, data leakage, log analysis and compromise detection. 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