Global Information Assurance Certification Paper

Intelligent Vulnerability Scanner
Eric Harnist
January 20,2002

Introduction

One of the big concerns for Information Security Managers is the management of vulnerabilities in large networked Information System environments. Vulnerability scanning technology plays a key role in this area. The intend of this document is to describe the context for using such technology, and to highlight some of the limitations found in commercial products. New techniques have recently emerged that improve their efficiency. NeXpose vulnerability scanner, introduced December 2001 by Rapid7 Inc., will illustrate the implementation of these improvements.

Construct the vulnerability picture

Vulnerabilities can be defined as design flaws or configuration errors, providing means to exploit a system or network which would not be available otherwise. New vulnerabilities are discovered every day and the pace of discovery doesn't slow down. Moreover, attack tools are widely available, automating the exploit of one or several vulnerabilities with minimum effort and knowledge. Vulnerable machines can be exploited by hackers to gain administrative privileges and execute arbitrary code or to launch denial of service attacks against third-party systems involving your company brand name. Vulnerable machines also enable malicious code to propagate autonomously. Consequently, the Confidentiality, Integrity and Availability of your information assets are at risk if you are not properly managing vulnerabilities in your information system infrastructure. Managing your vulnerabilities will bring your organization in a proactive security mode by deploying the right security safeguards rather than being stuck in a reactive mode where you constantly run after fixing the problems while they occur.

Information security managers are responsible to protect information assets that are located at the top of the infrastructure layers. These layers can be defined to be: network, operating system, middleware (web server, database server, etc…) and applications. While each of these layers can provide direct access to the information assets, all of these layers have their own vulnerabilities. This demonstrates the need to manage vulnerabilities at all the layers of your infrastructure.

Getting to the knowledge of all existing vulnerabilities in your particular environment is a tedious task and requires time and efforts. Bugtraq and CERT Coordination Center are wise sources of publicly available information that can be used to get to this knowledge. Vulnerability scanners products can also be used by security managers to efficiently assist them in identifying vulnerabilities on remote systems. These tools use a database of known vulnerabilities (sometimes called signatures). Current vulnerability scanners

products are able to identify hundreds of vulnerabilities. However, imagine the time and resources needed trying to fix all single vulnerabilities found using a vulnerability scanner on a complex environment, scanning for all possible vulnerabilities… This is often the reason why there are still so many vulnerable systems hosting well known critical problems; just because there are too many holes and administrators do not have enough time to fix them all.

However, not all vulnerabilities apply equally to your infrastructure and not all vulnerabilities have the same severity or are as easy to exploit. Moreover, it turns out that most hackers do search for limited number of vulnerabilities they well know how to exploit. This largely affects the probability for a certain vulnerability to be exploited. Consequently, the security manager must be able to rank the severity of vulnerabilities his infrastructure is exposed to, and identify the most critical ones in order to prioritize his effort in fixing them. To help in this vulnerability management process, SANS Institute and the FBI have released a list of the "Twenty Most Critical Internet Security Vulnerabilities" (October 2001). The Experts' Consensus". This list describes the vulnerabilities that were exploited by the majority of successful attacks on computer systems via the Internet. This list includes as well all necessary information to correct the vulnerabilities.

Management of vulnerabilities

Managing vulnerabilities is not only about using the right vulnerability scanner product. Bruce Schneier said, "Security is not a product, it's a process" (Crypto-Gram Newsletter, December 1999). This applies as well to vulnerability assessment. A vulnerability scanner alone does only provide a list of vulnerabilities it is able to identify on a system; if you don't act upon what it reports, your security state will not change. Adequate resources and processes are required to analyze the vulnerability reports, evaluate the risk, identify adequate solutions, and apply necessary corrective actions. Part of this process, is also to keep constantly updated with new coming vulnerabilities. This means that vulnerability assessment should not be a side process, but must be part of the organization's larger information security risk management program. Security manager must examine the complete information security needs: know where your assets are located, identify the type of threats your are exposed to, identify your organizational & technical vulnerabilities, assess the risk of intrusion, and develop a protection strategy to deploy safeguards and monitors. Security policies must reflect what the security requirements are and must be well understood by your organization's people.

Vulnerability scanners are getting fully valuable when they are part of the risk management program to identify vulnerabilities in the selected components of the infrastructure enabling the security manager to better evaluate risk and develop adequate security protections. Once the security safeguards are in place and policies are well known and understood, vulnerability scanners are still valuable to automate the auditing of the infrastructure's security looking for vulnerabilities that should not be there

according to the security policies. This regular assessment is essential in the ever-evolving infrastructure to maintain the expected security state.

There are additional areas where vulnerability scanner tools are also very useful:
. During penetration test procedures, to enumerate live network services, identify remote operating systems, and determine existing holes and patch levels.
. To know how vulnerable you are to a new coming threat: for instance when a new worm is spreading over the Internet using a particular vulnerability and may infect your intranet; the vulnerability assessment tool will provide you with the knowledge of which systems in your perimeter are vulnerable to the specific worm's infection process. Knowledge of your exposure is essential to make the right decisions in a short timeframe. This capability requires however that your vulnerability scanner is programmable to execute your personalized tests.

Vulnerability scanners limitations

Vulnerability scanners are tools that generally achieve several different tasks: they check for live network services on target systems, attempt to identify remote system's operating systems, check for possible configuration vulnerabilities, and verify presence of vulnerabilities.

One of the key expectations from a vulnerability scanner tool is to accurately report publicly known vulnerabilities at all the layers of your infrastructure like what a hacker would be able to see. Current approaches have however some limitations:

1. Vulnerability scanners have false negative: False negative are known vulnerabilities that exist on the target system, but not reported by the vulnerability scanner product. This makes the security manager mistakenly believe he has a certain security state while some doors are widely open.
2. Tools report false positive alerts: False positives alerts are vulnerabilities reported by the scanner that actually do not exist on the target system. False positive reports makes administrators waste their time on manually analyzing the vulnerability and correcting it while the vulnerability does not exist.

Vendors sometimes describe the accuracy of their tool in terms of false negative and false positive rates. These rates are calculated by dividing the number of reported false positives (or false negatives) by the total number of reported vulnerabilities. These rates are essential to the security manager selecting a product because they will determine the level of trust that can be put in the tool and the potential administrative resource overhead to manage the tool.

Security managers will have to look at the false negatives issue by verifying if the selected vulnerability scanner product does efficiently address the type of vulnerabilities in his environment (with the help of Bugtraq, CERT resources and the top twenty vulnerabilities list). In addition, security manager must verify how close the vendor is in tracking new vulnerabilities and issuing new signatures for its tool. The security

manager must be considering frequent updates in his production environment to keep his tool to the latest vulnerabilities identification capabilities and get the best out of his tool.

False positive alerts are a real issue, because they quickly reduce the benefits of a tool. A tool generating a high false positive alert rate will simply become unpractical in a large production environment because there will be too many false alerts to manage. Administrators will start paying less attention to alerts believing they are false positives or may simply turn the tool off. Some vendors claim a false positive rate below 1%. This may be acceptable if you scan your environment on which you never applied any correction. You may expect to get numerous alerts on missing patches and default configurations and may afford a 1% false positive rate. However, if your vulnerability scanner is part of your larger protection measures, you will scan for vulnerabilities over systems that you have updated to the latest software versions, with most security patches applied, with configuration management in place, etc. In this case, assuming the tool will report the same number of false positives while the total number of reported vulnerabilities has diminished, the false positive rate may be much higher.

The fact is that false positives often originate form the difficulty and complexity to remotely identify vulnerabilities on a target system through the network considering the variety of configuration and installed software the remote system could have. During the evaluation of vulnerability scanner product, false positives were identified while checking for open UDP ports. The tool reported several open UDP ports while no services were actually active on the remote system. A network protocol analyzer was necessary to understand the wrong behavior (the free ethereal tool was used from http://www.ethereal.com/). The final reason of the false positive was that the remote system had a host-based firewall installed. This firewall was configured to stealth any unused ports. While the vulnerability scanner sent UDP datagram with a fixed payload (in this case all 7) to scan the remote system's network services, it expected to get in return an ICMP packet type 3 code 3 (Destination unreachable – Port unreachable) to identify a "closed" port. Unfortunately, since the firewall on the target system did stealth unused ports, no ICMP packet was returned, and the vulnerability scanner misleadingly interpreted this behavior as an open port.

False negative and false positive rates are the weak points in vulnerability scanner products. Vulnerability scanner vendors have focused their effort on reducing these rates. A "testing" methodology has been introduced to validate the existence of vulnerabilities. This means that each time a vulnerability has a potential to exist in a remote system, the vulnerability scanner attempts to exploit it. NeXpose product implements this technology.

NeXpose plugins and Services Advertising

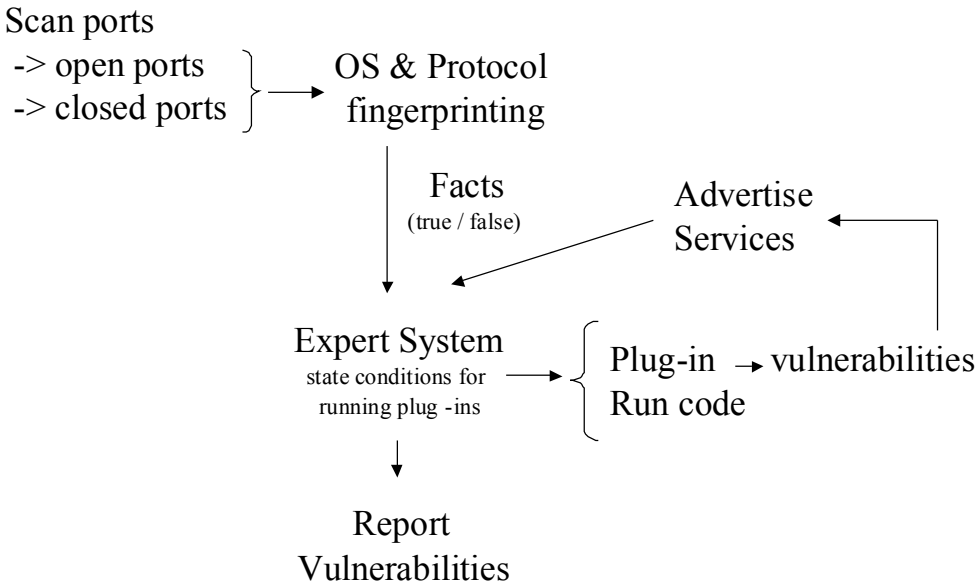
After NeXpose uncovers vulnerabilities on remote system's network, operating system and middleware layers, it validates the penetration capabilities by using small programs

called plugins. Plugins are designed to attempt to exploit a specific vulnerability, or to check configuration issues like default account names and password in operating systems. A set of default plugins is coming as part of the tool to address known vulnerabilities. In addition, plugins can be designed by NeXpose's users to create specific tests.

Several vulnerability scanners products are already implementing the plugin technology. NeXpose product however goes one step further compared to static vulnerability scanner products. It uses accumulated knowledge and combines discovered vulnerabilities to make extensive test attempts at multiple entry points. This is achieved through a correlation engine that advertises the result of the penetration tests (also named "service") to the other test programs to enable more in-depth intrusion attempts. When a penetration test is successful on a discovered vulnerability, it advertises the newly acquired capability to the other test programs extending the penetration capabilities. For instance, the Microsoft IIS Unicode Traversal vulnerability provides remote execution services. If there is a plugin stating it needs remote execution services to perform its exploit, it can then make use of the advertised service without knowing how the service is being provided.

The way NeXpose is working is described in the following figure.

NeXpose Methodology



1. When a scan is launched, NeXpose first tests presence of the target system.

2. If target is confirmed to exist, NeXpose scans the system to identify open and closed network services over TCP and UDP protocols.
3. It uses the previously obtained information to attempt to fingerprint the target's operating system as well as applications running behind the network services. From this identifications steps it issues a certain number of statements named "Facts" used in later steps.
4. An Expert System based on a correlation engine is using the "Facts" to launch appropriate test programs named "plugins".
5. Once a plugin has successfully tested an exploitable vulnerability, it does "advertise the service" meaning literally that it shares the new exploit capabilities with other plugins enabling them to achieve their own exploits.

At the end of the scan process, NeXpose displays a detailed report making clear distinction of what it was able to confirm or not:

- ➔ "Confirmed – Vulnerabilities" when the test program did successfully achieve the exploit
- ➔ "Unconfirmed - Vulnerabilities" when the vulnerability was identified but the plugin was not able to successfully exploit it and validate it's presence (the design of the test programs may have some limitations as well)
- ➔ "Confirmed – Non Vulnerabilities" when executing the plugin resulted in the system not being penetrated (revealing for instance that you are not vulnerable to the default password attack on the ftp account)
- ➔ "Unconfirmed – Non Vulnerabilities" where the system is not vulnerable to a specific vulnerability but NeXpose was not able to run an appropriate plugin to confirm it

NeXpose uses as well colors to indicate the severity of reported vulnerabilities.

This type of detailed report is highly valuable to the administrator because it provides, in a single view, several different level of vulnerabilities assurance. This improves the trust that can be put in the stated "confirmed" results, while knowing where to focus the analysis efforts.

Conclusion

Vulnerability scanner products are key in evaluating your security risks and auditing your information security state. The new generation of tools is focusing on reducing the false alert rates and is becoming more efficient to run in large production environments. It is however mandatory to clearly understand how your vulnerability scanner product works and to keep in mind it limits in order to better interpret its results and effectively integrate it into your layered security protections. NeXpose has added to the vulnerability scanner arena a new capability to intelligently correlate vulnerabilities. This is a real advance in the vulnerability identification assurance.

References

. Pete Herzog. “The Open Source Security Testing Methodology Manual”. Draft 2.0 July 2001. http://ideahamster.gnutec.com/osstmmdraft.htm

. Christopher J. Alberts. “OCTAVE [SM] Catalog of Practices”. Ver 2.0. October 2001. (Page 20) http://www.cert.org/archive/pdf/01tr020.pdf

. SecurityFocus. “Bugtraq Vulnerabilities”. http://www.securityfocus.com/cgi-bin/vulns.pl

. CERT Coordination Center “Vulnerabilities, incidents & fixes”. http://www.cert.org/nav/index_red.html

. SANS Institute. “The Twenty Most Critical Internet Security Vulnerabilities (Updated), The Experts’ Consensus.” Version 2.100. October 2, 2001. http://www.sans.org/top20.htm

. Bruce Schneier. "Security Is Not a Product; It's a Process". Crypto-Gram Newsletter December 15,1999. http://www.counterpane.com/crypto-gram-9912.html#SecurityIsNotaProductItsaProcess

. Mahesh V. Tripunitara and Eugene H. Spafford. “Security Assessment of IP-based Networks: A Holistic Approach”. February 1999. http://www.cerias.purdue.edu/coast/papers/99-02.pdf

. Rapid7 Inc. “NeXpose Installation and Quick Start Guide”. December 2001. http://www.rapid7.com/NXpsInst.pdf

Last Updated: May 30th, 2017

Upcoming Training

Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event