Global Information Assurance Certification Paper

GSEC Practical Requirements (v.1.2e)

Adrien de Beaupré

Know yourself: Vulnerability Assessments

Know yourself: Vulnerability assessments.

How can systems and network administrators evaluate the state of their own security? How can management be assured that their systems and network security is alive and well? One suggestion has been to "Know Your Enemy" [23]. Through analysis of 'black hat' activities we can learn how to better defend ourselves. Armed with the knowledge of the tools and techniques used to attack we can build better defensive systems and protect our 'crown jewels'.

We all know that in an ideal world system and network security should be designed and properly implemented from the ground up. A layered defense strategy is developed that properly prevents or deters attackers from gaining access to sensitive information or systems. At the very least the firewall should slow them down. Logging and active monitoring should let us know when something improper such as misuse or an intrusion might have occurred. However, out in the real world networks seem to 'happen'. The larger the network, the more it tends to grow in a haphazard fashion, without any particular rhyme or reason. Security concerns give way to functionality and performance.

It is a given that we should have some measure of security; the question is how to increase security without scrapping existing networks and re-building from scratch? The answer seems to be that, in order to defend a network, you have to know everything there is to know about it. Preferably before an intruder does. A popular method of doing so is to hire a consultant to do some sort of penetration testing. The theme of this paper will be to explore how security vulnerability assessments can help increase and promote a more secure set of systems and networks. The ultimate goal of the entire endeavor would be to plan and perform a comprehensive documentation of the entire infrastructure.

The key to security is, of course, always policy. Without a coherent set of policies it really isn't possible to ever be 'secure'. You might fool yourself into feeling secure because you have installed the latest and greatest firewall and intrusion detection suite, however technical controls are only part of a properly developed security program. The security process is all about applying the appropriate policies through proper procedures and management practices. For example, how can you secure all of the entry points to your network if modems are allowed without a policy prohibiting or controlling their use? [17] The simple answer is that you can't. Assume that security is not a static achievable state, but a moving process that must be maintained over time. There is no magical silver bullet to solve all security problems, however vulnerability testing is a key element in an overall security program for any organization [6]. "There is a significant issue with vulnerability assessments in that they are a 'snapshot in time' of a system or network's security posture. As such, testing is limited to known vulnerabilities and the current configuration of the network" [19].

There currently isn't a broad consensus as to the precise meanings and definitions of the term vulnerability assessment as used here. This activity is sometimes also referred to as security testing, which seems to imply using a specific quality assurance type of methodology. This misunderstanding with a particular client about 'testing' led me to be more careful with the specific meaning and definition of the terms I use. Other terms can include security auditing, threat or risk assessments, ethical hacking, white-hat security testing and security diagnostics. The lines between the various terms and their applications are also not always clear. For example they may all use similar methodologies, people and tools. For purposes of this discussion I will use the definition from Ira Winkler [29] for an assessment as "an overt study to locate security vulnerabilities". The NSA Glossary of Terms Used in Security and Intrusion Detection defines penetration testing as " the portion of security testing in which the evaluators attempt to circumvent the security features of a system" [21]. This definition normally implies emulating the activities of hackers/crackers. A security audit is defined as a comparison of the security implementation of systems against a given set of standards to measure compliance. The way I look at it is, penetration testing is done from the outside poking inwards to see what happens and how far you can get. Vulnerability assessments are something you do to your own networks and systems from the inside to understand them better. Audits are something done by auditors, either corporate or otherwise.

In my mind I always try to associate increasing security with reducing risk. The trick is to discover as many vulnerabilities as possible, decide how risky they are to your environment, and then reduce the risk they pose. Vulnerability assessment is one method of helping you find and plug the holes, before others get through those holes first with evil intent. It is not possible to reduce the risk to none, only to an acceptable level. As long as you remain aware of how much risk you are assuming in the current state of your environment. We must "consider that for a given threat, target (impact), and system vulnerabilities, increasing the countermeasures will reduce the risk of loss." [1].

So, where do you start? Start with a thorough evaluation of your policies. Examine the current state of your infrastructure; compare that with how your infrastructure should look based on security best practices and your policy. You have to attain a comfort level that your infrastructure is so well documented and has been assessed for vulnerabilities. This goes way beyond simply installing a firewall and maintaining an Intrusion Detection System. I would consider these two an absolute requirement and a bare minimum, not the entirety of any security program [16].

Not only is vulnerability assessment useful for discovering potential problems, it is also a method of testing your own intrusion detection systems. External penetration testing should set off alarms on the firewalls and any other public hosts, such as web servers. An Intrusion Detection System, either network or host based, should detect internal scanning. In fact examining log files on systems that have been tested should give you an idea of what to look for in looking for actual intrusions. It would normally be a good idea to ensure that anyone who may receive such an alarm, or may notice traces later, is aware of the fact that vulnerability assessments are taking place.

Implementing changes based on the assessment analysis should still be subject to change management process and configuration management approval process. There is a simple reasonableness test; will this change actually improve protection based on the things in our organization we consider valuable? Does the expense or effort required to make the change outweigh the benefit of reducing that particular vulnerability risk? In a way vulnerability assessment can be an extension of systems configuration analysis. It may assist you in detecting unauthorized changes to important servers. Vulnerability assessments can also demonstrate that you have followed due care in applying known best practices for IT security.

Running an assessment can carry it's own inherent risks. For example, capturing traffic or files that contain user names and passwords, then cracking them exposes the potential harm if an intruder duplicated this particular attack. It also creates a new risk of what to do with the list of cracked passwords. Either malicious or careless use of these types of tools can pose an enormous risk and cause tremendous harm. Again, here is a case where policy and procedures must specify who, how and when vulnerability assessment tools are used.

> *"What are the drawbacks to testing?*
> *Of course, there is a down side to penetration testing. Limits to the tests must be spelled out. For instance, the testing could shut down the facility. Is that allowed? Can that work only be done off-hours? If a hole is found, should it be exploited to determine other problems with the security of the facility? If it's not done carefully, testing can "negatively impact" the site being evaluated. It could look like a denial of service attack, for instance. Or if the testing goals are not explicit, the tests (and testers) could run amok. Legal consequences can occur if the testing grounds aren't spelled out, or if the test team goes beyond the limits imposed. One recommended solution to all these risks is to have someone from your site work closely with the team, without interfering. By inviting a penetration test team on-site, you run the risk of exposing confidential corporate information to outsiders. Be sure the team you hire is trust-worthy. In the worst case, someone from the team could create security holes and use them later. Management planning and buy-in might be hard to obtain."* [10]

There are methodologies that should be applied when doing any form of vulnerability assessment. The Open-Source Security Testing Methodology Manual (OSSTM) [15], along with other reading referenced in the bibliography, may be helpful in developing the test plan scope and project parameters. The testing plan should be properly documented and approved by the client or management authority before any tool or technology is even considered. The actual process of running the tools may involve a certain amount of flexible or even intuitive reactions to results. For example, if an unknown port is identified to be open on a host currently being tested but the scanner cannot identify the specific service, a simple connection to that port may answer the question of 'what the heck is that? and why is it on my server?'. Further investigation is always required beyond simply running the scans in order to correctly identify the precise nature of significant vulnerabilities. One of the most important parts of vulnerability assessments is the analysis afterwards. Judgment and experience will help filter through the many many

pages of information these tools produce. The thing is to pinpoint the important areas that must be remedied immediately and address them as soon as possible. You have discovered what is wrong, where the problems are and probably identified whom and how to fix them. The next thing to consider is why do those vulnerabilities exist? Then you can tackle prevention of future problems.

The tools and people that you use to perform security testing must be carefully chosen. There is significant debate over using an external consulting firm or internal resources to perform the scanning. Firms such as En Garde Systems [39] or eSecurityOnline [41] can be hired to perform either external or internal vulnerability assessments or penetration tests. Another debate rages over the use of reformed or ethical hackers [30]. The people running the scanners and interpreting the data pretty much make or break the assessment. Anyone can run these tools; it really isn't all that difficult. Running them well and making the results intelligible, meaningful and relevant are the real key elements. Whomever you decide to employ, I believe that the key areas are to have well defined goals, a clear intent and skilled trustworthy people running the tests. In other words, be very careful who uses sharp tools exploring your playground.

Another big consideration in the equation is the tools themselves. Wouldn't it be nice if it were possible to individually audit each network segment and system looking for problems? Even if normal system administrators, network managers and auditors weren't busy enough already with their own workload, we all know that this simply isn't feasible. Enter the automated vulnerability assessment toolkits. They have a variety of features, may run on different operating systems, some are better at some tasks than others, but they all have some similar functions in common. I have always recommended using a COTS (Commercial Off The Shelf) scanner such as CyberCop [35] from NAI or Internet Scanner [36] from ISS in conjunction with well-known openly available tools from the Internet such as nessus [38] and nmap [33]. I would consider it a best practice to use at least two sets of such tools in order to compare and correlate their results. What one may miss the other may catch and they can confirm the others findings. One obvious advantage of the tools available from the Internet is that they are free. You can't beat that. A number of freeware and commercial vulnerability scanners were tested and rated by Network World [9] and no single product passed all of their tests. Nessus and ISS Internet Scanner rated the highest by missing the fewest number of vulnerabilities that existed on their test systems. Another way of looking at it is that no single product was able to discover all of vulnerabilities present, but a combination of two or more should give a higher level of assurance in the assessment. I use one commercial set of tools and one freeware set of tools because they tend to complement each other nicely. There are other types of attacks possible that must also be considered and can include physical attacks, trusted user escalation of privilege, remote internal or internal network attacks, denial of service or simple insider misuse of access.

Penetration testing may in fact give you a false sense of security because it might not address all of the areas of your networks and systems that could possibly be vulnerable. Scanners are not commonly able, or configurable, to scan for homegrown applications problems buffer overflows for example. While convenient to use scanners they cannot be the only method of vulnerability assessment used. Actually walk over to some servers and poke around [12]. Run spot checks on a sampling of every type of network device and system in your environment.

A thorough vulnerability assessment would have to include all of the areas where you could be attacked, which is not accomplished through just running scanning software. Some of the many types of network or system vulnerabilities to look for are: software bugs, buffer overflows, incorrect systems or services configurations, poor administration practices, poor password management, sniffing, protocol, network devices and systems design flaws, or social engineering [32]. I find the scanners most helpful in helping narrow down specific technical areas to further investigate. It just is not possible for any automated tool to always be absolutely up to date. In order to be thorough, custom scripts you write yourself or in the wild '0 day sploits' have to be downloaded, tested and run. This brings about another interesting point, how far should you go? Is it enough to believe there may be a vulnerability or do you actually have to run the exploit to prove it is there? Downloaded hacker/cracker tools are fine, and fun, in isolated test labs, but may have unexpected consequences on production environments. There is no single answer here. To a certain extent it depends on how much you want to know and how far you are willing to go. The client expectations of the results and their desire not to impact live servers will likely influence this decision. In fact, these points should all be clarified and negotiated in advance with full knowledge of the risks.

There just is no excuse for running a port scan, a single vulnerability scanner, and sending the results directly to the client without any analysis. The methodology to use for external penetration tests is beginning to be well defined. The team has to look at your publicly accessible systems the way an intruder would. What systems of yours could be attacked, how could they get in, when are attacks likely to occur, who might want to attack you and why? 'Who?', is another question to consider carefully. If you are evaluating your internal security you have to face the possibility you may also be defending against someone who is already inside the walls and trusted as well [3].

The internal testing should be done by an internal group for a number of reasons. One being that it is easier for management to ensure that procedures will be followed properly and controls can be placed on their assessments if they are your own staff. The inside team may lack the capability of 'thinking like attackers' and may not be independent however they will have intimate knowledge of how and where to look for problems within their own environment. The external penetration team should be independent and look inwards from the outside like true attackers, with limited insider knowledge. A contracted firm with a good reputation and confirmed expertise in penetration testing should do the external assessment.

Keep archived logs of the scans and compare them for trends over time. In order to make the scanning analysis results most meaningful you need something to compare them against [5]. A good practice to follow would be to perform an initial assessment on a specific set of targets. Develop a plan to implement recommended changes to address the problem areas. Make the changes and then do a second assessment that matches the first. You should be able to clearly see improvements. Decide on a reasonable interval to perform periodic penetration testing and vulnerability assessments on both the internal and external systems. Now that you have a working baseline for comparison purposes. This will assist you in identifying weaknesses in the internal and external defenses as seen by an attacker. Periodic testing is required in order to ensure newly discovered exploits will not open the infrastructure to new potential intrusions. This process will give you an opportunity to evaluate the security of your infrastructure on an ongoing basis and engage in continuous improvement. The design and implementation of proper security controls is aided by having detailed knowledge of the baseline configuration.

In conclusion, vulnerability assessments play an important role in a coherent security program. Without them you are essentially running blind. Obviously, while a useful exercise, they also cannot be the only security measure implemented. Just as a firewall or an IDS is not a magic solution, neither is penetration testing. I really think you cannot live without vulnerability assessments of some sort; you just have to be careful with them and make certain they are properly thought out.

References and bibliography:

[1] Beck, David F. “A Review of Cybersecurity Risk Factors”. January 16, 2001. SANS Institute Information Security Reading Room. URL: http://www.sans.org/infosecFAQ/securitybasics/risk.htm (14 June, 2001)

[2] Berg, Al. “Secure Strategies - Part 2 ‘Audits, Assessments & Tests (Oh, My)’”. August 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/august00/features4.shtml (14 June, 2001)

[3] Boyd, Ida Mae. “The Fundamentals Of Computer HACKING”. December 3, 2000. SANS Institute Information Security Reading Room. URL: http://www.sans.org/infosecFAQ/hackers/fundamentals.htm (14 June, 2001)

[4] Brooks, Greg. “Nessus - Get on Board”. February 15, 2001. SANS Institute Information Security Reading Room. URL: http://www.sans.org/infosecFAQ/audit/nessus2.htm (14 June, 2001)

[5] Conner, Gary L. “Process for Performing, Evaluating and Documenting Host Vulnerability”. May 31, 2001. SANS Institute Information Security Reading Room. URL: http://www.sans.org/infosecFAQ/audit/host_vulnerability.htm (14 June, 2001)

[6] Cutler, Ken. “Hitting the Bull’s Eye”. August 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/august00/columns5_logoff.shtml (14 June, 2001)

[7] Farmer, Dan and Venema, Wietse. “Improving the Security of Your Site by Breaking Into it". 1995. URL: http://pulhas.org/docs/improve_by_breakin.txt (14 June, 2001)

[8] Fennelly, Carole. “Audits from Hell”. February 3, 1999. URL: http://www.soa.fau.edu/friedberg/audits-from-hell.htm (14 June, 2001)

[9] Forristal, Jeff and Shipley, Greg. “Vulnerability Assessment Scanners”. Network Computing January 8, 2001. URL: http://www.networkcomputing.com/1201/1201f1b1.html (14 June, 2001)

[10] Galvin, Peter. “Do you need a penetration test?” Sun World Feb 1997. URL: http://sunsite.nstu.nsk.su/sunworldonline/swol-02-1997/swol-02-security.html (14 June, 2001)

[11] Genusa, Angela. “12 Keys for Locking Up Tight”. March 01, 2001. CIO Magazine. URL: http://www.cio.com/archive/030101/keys.html (14 June, 2001)

[12] Gula, Ron. “Broadening the Scope of Penetration Testing Techniques - The top 14 things your ethical hackers for hire didn't test.” July 1999. URL: http://www.network-defense.com/papers/pentest.html (14 June, 2001)

[13] Heiser, Jay. “Beware the Red Herring”. August 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/august00/features3.shtml (14 June, 2001)

[14] Herman, Ben. "Routine External and Internal 'Hacking', An Important Part of Information Assurance". April 19, 2001. SANS Institute Information Security Reading Room. URL: http://www.sans.org/infosecFAQ/attack/routine.htm (14 June, 2001)

[15] Herzog, Pete. "Open Source Security Testing Methodology Manual". May 5, 2001. URL: http://uk.osstmm.org/osstmm.htm (14 June, 2001)

[16] Keith, Lynn. "Steps to a Secure Network". May 16, 2001. SANS Institute Information Security Reading Room. URL: http://www.sans.org/infosecFAQ/policy/steps.htm (14 June, 2001)

[17] King, Nathan A. "Penetration Testing, Sweeping Changes for Modem Security". June 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/june00/features1.shtml (14 June, 2001)

[18] Kurtz, George and Prosise, Chris. "Penetration Testing Exposed - Part 3 'Audits, Assessments & Tests (Oh, My)'". September 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/september00/features3.shtml (14 June, 2001)

[19] Kurtz, George and Prosise, Chris. "Penetration Testing: Myth vs. Reality". September 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/september00/features4.shtml (14 June, 2001)

[20] Norton, Stephen. "Circle of Security". November 13, 2000. SANS Institute Information Security Reading Room. URL: http://www.sans.org/infosecFAQ/securitybasics/circle.htm (14 June, 2001)

[21] NSA Glossary of Terms Used in Security and Intrusion Detection URL: http://www.sans.org/newlook/resources/glossary.htm (14 June, 2001)

[22] Rude, Thomas. "Knockin' At Your Backdoor - A Guide to Penetration Testing". October 2000. URL: http://www.crazytrain.com/penetration.html (14 June, 2001)

[23] Spitzer, Lance. "Know Your Enemy." 21 July, 2000. URL: http://project.honeynet.org/papers/enemy/ (14 June, 2001)

[24] Spitzer, Lance. "Auditing Your Firewall." 12 December, 2000. URL: http://www.enteract.com/~lspitz/audit.html (14 June, 2001)

[25] Swanson, Dan. "Avoiding IS Icebergs - Part 4 'Audits, Assessments & Tests (Oh, My)'". October 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/october00/features3.shtml (14 June, 2001)

[26] Symantec. "Enterprise Security Strategy". September 2000. URL: http://enterprisesecurity.symantec.com/article.cfm?articleid=354 (14 June, 2001)

[27] The MIS Corporate Defence Solutions Ltd., Network Security Team. "An overview of Network Security Analysis and Penetration Testing". 1 August, 2000. URL: http://www.mis-cds.com/services/spirit/test/wp-over-pentest.pdf (14 June, 2001)

[28] Torres, Efrain. "Penetration Testing Methodology - For Fun and Profit". v1.2 19 February, 2001. URL: http://www.securityfocus.com/data/library/pen.pdf (14 June, 2001)

[29] Winkler, Ira. "Audits, Assessments & Tests (Oh, My)". July 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/july00/features4.shtml (14 June, 2001)

[30] Winkler, Ira. "The 'Ethical Hacker' Debate" July 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/july00/features4a.shtml (14 June, 2001)

[31] Winkler, Ira. "Security Strategies for E-Companies, a Crisis in Confidence" February 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/february00/columns_logoff.shtml (14 June, 2001)

[32] Wilson, Zachary. "Hacking: The Basics". April 4, 2001. SANS Institute Information Security Reading Room. URL: http://www.sans.org/infosecFAQ/hackers/hack_basics.htm (14 June, 2001)

Tools:

[33] Fyodor. Nmap. 11 June, 2001. URL: http://www.insecure.org/nmap/index.html (14 June, 2001)

[34] Max Vision's White Hats. "Penetration Testing Assessment Tools". URL: http://www.whitehats.com/tools/assessment.html (14 June, 2001)

[35] PGP Security Products. CyberCop Scanner. Network Associates Inc. URL: http://www.pgp.com/products/cybercop-scanner/default.asp (14 June, 2001)

[36] Security Assessment. Internet Scanner. Internet Security Systems Inc. URL: http://www.iss.net/securing_e-business/security_products/security_assessment/internet_scanner/ (14 June, 2001)

[37] Talisker. "Talisker's Network Security Tools: Vulnerability Scanners". URL: http://www.networkintrusion.co.uk/scanners.htm (14 June, 2001)

[38] The Nessus Project. Nessus. URL: http://www.nessus.org/intro.html (14 June, 2001)

Services:

[39] Elytra Enterprises Inc. "Security Consulting". URL: http://www.elytra.com/services.htm (14 June, 2001)

[40] En Garde Systems Inc. "Remote Penetration Testing" URL: http://www.engarde.com/consulting/pentest/onsite.php (14 June, 2001)

[41] En Garde Systems Inc. "Onsite Penetration Testing by EGS". URL: http://www.engarde.com/consulting/pentest/onsite.php (14 June, 2001)

[42] eSecurityOnline, "Overview of Vulnerability Scanning Service". URL: http://www.esecurityonline.com/services/vss/overview.asp (14 June, 2001)