

Global Information Assurance Certification Paper

Copyright SANS Institute Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering "Security Essentials: Network, Endpoint, and Cloud (Security 401)" at http://www.giac.org/registration/gsec Security Life Cycle - 1. DIY Assessment

By Lee Wan Wai, Version 1.0 13 November 2001

Introduction

60

Ever wondered where do you stand in term of IT security readiness? Is there a way to get a feel on the level of security with what you have without incurring additional cost on the already tight budget? What would be more saddening to realize that your server was taken over by hackers and had partaken in a DDOS (distributed denial of service) attack on the CIA? The best course of action, prevention by performing regular vulnerability assessments/reviews and treat those problem areas.

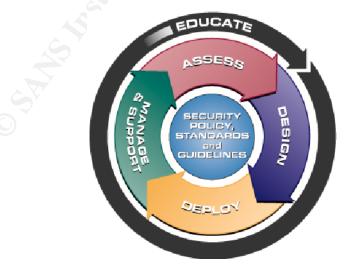
Here's one way that can provide a simple and up to date DIY assessments. What follows is a simplified and comprehensive way to get a quick self-assessment.

This paper covers one phase of the Security Life Cycle, Assessment.

Background

There are process cycles that many businesses are based upon. The process of buying and selling is a cycle, application development and SDLC (System Development Life Cycle) follow a process cycle. In the critical field of IT Security a Security Life Cycle process can effectively guide and covers the stages leading to a successful secured operations and business.

As a basis for understanding, the Security Life Cycle will be briefly discussed.



Security Life Cycle

*Policies, Standards and Guidelines- (BS ISO17799:2000 BS7799-1:2000)

These are the cores that govern the four stages of the Security Life Cycle.

Policies will ensure that various important areas such as controls, legal and information classifications are sufficiently covered. Standards will ensure proper control over configurations of various component and software involved. Guidelines ensure practices and tasks are executed in an orderly and predictable manner.

1. Assessment-

Assessment is a critical event that determines the security bill of health for any system. Activities such as audits, penetration testing and reviews are to be conducted periodically or when the needs arise, e.g. Major changes. Normally, risk assessments are computed from the data gathered. A good guide to risk assessment can be found in NIST Computer Security Resource Center web site. (See reference sites below)

2. Design-

Designing a proper and effective security configuration based on organizational and industry standards is an important stage of the security life cycle. Designing also encompasses activities such as formulating process and improvement over existing design.

3. Deploy-

Deployment is to implement based on the developed design. Specialized and skilled personnel have to be employed for these activities.

4. Manage-

Managing and monitoring is crucial to ensure the system is functional and also serves as a problem detection mechanism.

* Continual Training

Training is continual within the entire Life Cycle as it extends to many different level of the organization. Proficiency and skills are raised within this on-going process.

Assessment

The principle of Security Assessment is to determine the state or bill of health in two main areas, technical and non-technical. Assessments can be carried out by either internal or external 3rd party organization.

Non-Technical (Policy Assessment)

Here are 4 major key areas in policy assessment:

• Information Control and Protection

These policies govern the control and classification of information assets. It also includes both review instructions as well as personnel related issues such as NDA (non disclosure agreement) and duties segregation.

• Virus, Malicious Code and Virus Prevention

These policies govern the protection on information assets. Specifying the control on periodic information screening and instructions to deter unintentional virus/trojan infection.

• Disaster Prevention

These policies govern the disaster prevention and preservation of information assets. Failover system, high availability and capacity planning are measures against natural or manmade disaster.

Business Continuity Management

These policies govern the continuity of business in the event of an intentional or unintentional breakdown. Presence of backup measures and sufficient exercise to ensure the DR (Disaster Recovery) plans are effective.

Questionnaires and interviews are an essential part of a Policy Assessments, it is essential to build a checklist to meet areas mentioned above that is acceptable to the business objectives. It is also important to ensure that all policies are endorsed by management and are up to date with the current business needs.

(A simple and comprehensive sample checklist can be found at <u>http://www.itc.virginia.edu/security/checklist/checklist_intro.htm</u>)

Technical Assessment

Technical assessments cover the A to Z of all technical areas. It should effectively cover the following areas with the principle specified in the corporate security policy in mind. (A simple and comprehensive sample checklist can be found at http://www.itc.virginia.edu/security/checklist/checklist_intro.htm)

• Physical Security

Are the machines physically secured with only authorized personnel having access to it? It is wise to secure all wires and switches/hubs to avoid sniffing or port scanning.

• Network & Security Design

Are there traffic filtering, monitoring and segregation of network traffic with consideration based on least privilege rule? The presence of a logging system and IDS (intrusion detection system) would help identify a fair amount of potential intrusion. Choosing switches over hub enhances both security and performance. Ingress and egress firewall filtering rules should be verified.

• Skills matrix

Are personnel handling the system capable of detecting, responding and escalate any incident? Are there sufficient training and awareness in IT security among staffs?

The next stage of the technical assessment requires full authorization from management and system owner as it deals directly with probing and penetration testing of the intended system.

There are several tools designed for simple technical assessments. Some are freeware while some are commercial products. Two products are covered in this paper, one from each category, namely ISS and Nessus. Both were highly rated software from Network Computing review <u>http://www.networkcomputing.com/1201/1201f1b1.html</u>. Note that War-dialing is not covered in this paper but it is highly recommended that authorized personnel should perform it.

• ISS Internet Scanner

This is the leading commercial industry tool that is highly rated for assessing either a single IP device or a range of IP devices on various operating platform. The unregistered version only scan the loop-back machine it is installed on. ISS will run on WinNT 4.0 and Win2000 series with 80Mb RAM with 180Mb of hard disk space.

1. Acquire ISS Internet Scanner Ver 6.2(36Mb) evaluation from <u>http://www.iss.net</u>. Installing ISS Internet Scanner is a breeze by executing ISSNT.exe (pre-scan file for malicious code before installing) and everything will go right through without much difficult question.

2. While connected to the Internet, apply X-Press update to get the lasted test signatures from ISS themselves. This may takes a while depending on the amount of new updates since the software release date. When updated, there will be 980 exploits available on database.

×uX-Press Update - Internet	Scanner 6.2	
Installing X-F	ress Updates	
Status: Creating bac	kup package XPressUpdate5_1.xpu.uninstall	
	< Back Next > Cancel	Help

3. ISS operates in several security detection Levels. It is advisable to have this run sequence order: (Recommended to disable all DOS related checks unless all precaution and recovery measures are ready on standby)

- L1 Inventory
- L2 Classification
- L3 Router/Unix/NT(Basic Penetration)
- L4 Router/Unix/NT(Enhanced Penetration)
- L5 Unix/NT(Expert Penetration)

SISS Internet Scanner - [Session]		⊻indow <u>H</u> elp	×
1 🛍 📽 🖬 🕹 🗕 🤹 🔍 🛙	🔨 隆 👘		
- Hosts to be scanned	Host	Status	Time
2 127.0.0.1 [lww]	🔍 127.0.0.1	Scanning	NA
TELESCE [IIII]	£	TCP Services Scan	Fri Nov 09 13:2
	£	Telnet banner	Fri Nov 09 13:2
	£	HTTP port scan	Fri Nov 09 13:2
	1	HTTP port 80 not active	Fri Nov 09 13:2
	12 C	HTTP port 8080 not active	Fri Nov 09 13:2
	教教教教教教	smtp check	Fri Nov 09 13:2
O 🎭 🕵		SNMP check	Fri Nov 09 13:2
	Properties	Status 😟 Vulnerabilities	Services 🥵 Accounts
Scanning 1 Host(s) Scanning Host: 127.0.0.1			
General A Session2 A S	ession2[1]/		
-	L5 NT V	Veb Server	1 Host(s)

4. The results are fairly straightforward to locate under the "Vulnerabilities" tab, right clicking on each item allow further explanations and remedy on that vulnerability. Reports can be generated based on the interest of the reader via the "Reports" menu. Furthermore, custom exploit checks can be built and added to the list of exploits supplied.

Nessus

Nessus had attained a very good reputation as the most valuable vulnerability tool available under the open-source category. It is also by far the most preferred tool for commercial environment. Nessus consist of two components, the server that perform the assessment and a client GUI (Graphical User Interface) client and they operate as a client/server model. However, Nessus server is Unix based that can only be installed onto a Unix like system such as Linux. Etc.

1. There are two way to get the binaries, one way is to launch a script "nessus-installer.sh" downloaded from any of the listed ftp sites on <u>www.nessus.org</u>. The safer way is to acquire Nessus binaries simply by downloading 4 files from <u>www.nessus.org</u>. (Note that x represent version numbering)

i. nessus-libraries-x.x.tar.gz ii. libnasl-x.x.tar.gz iii. nessus-core.x.x.tar.gz iv. nessus-plugins.x.x.tar.gz

A Nessus GUI client for windows can be found on the site for download. Alternative Java GUI client is also available for download. As Nmap can be plug-in for Nessus for added depth of scanning, install Nmap before installing Nessus. Nmap can be obtained at <u>www.nmap.org</u>.

2. Installing NMAP is straight forward, as it only requires a single command for e.g. in Mandrake Linux:

rpm -i nmap-253-1.i386.rpm

Installing Nessus requires a little more effort and time, as these are source code that required compilation and linking. Hence the development options have to be present before compiling these 4 binaries. In the even of a compilation error, please refer to <u>www.nessus.org</u> for further help in the FAQ or Installation guide.

In the order listed above, perform the following (preferably with all 4 files in the /tmp directory):

cd /tmp tar -zxf nessus-libraries-x.x.tar.gz *cd nessus-libraries* ./configure make make install vi /etc/ld.so.conf <Ensure a line /usr/local/lib is in the file, add if neccessary> ldconfig *tar -zxf libnasl-x.x.tar.gz* cd libnasl ./configure make make install cd /tmp tar -zxf nessus-core.x.x.tar.gz cd nessus-core ./configure make make install tar -zxf nessus-plugins.x.x.tar.gz cd nessus-plugins ./configure make

This will install all the libraries and binaries needed for operating with Nessus.

3. Since Nessus operates like a client/server model, a user has to be created on the server.

make install

Add a user by issuing the command:

nessus-adduser

Supply a login name, one time password and choose cipher as the authentication for now. Issuing the command can start Nessus daemon:

nessusd –D

Nessusd will computes it's own key pair when started for the first time, this key pair are used for authentication as well as providing a encryption channel between Nessusd and the client.

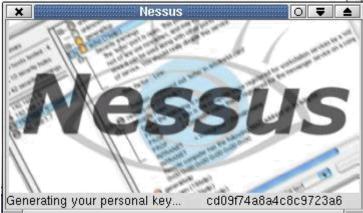
4. Posix, windows or java clients has the similar interface and the main difference is on the platform of the running OS. Start X windows and fire up Nessus by issuing the command:

nessus &

Windows based Nessus are started via an executable named nessus.exe.

It is not recommended to use Java clients as it had not be further developed for almost a year and hence lacking in many functionality.

Once Nessus fires up for the first time it will compute it's own key pair for authentication and encryption. Be ready to set and remember a new password for this personal key.



Using Nessus requires some practice and understandings on the switches and options available. Hereby will provide a simplified to access a machine within the network. However do be ready to have these information for Nessus to operate.

i. The nessus user and password, Login is required ii. If dangerous plugins testing are required iii. Nmap scan technique (options available from reading nmap manuals or at site www.nmap.org) iv. Scan options for additional features. (Suggested to check Nmap option for starter)

v. Target IP address or range

	Nessus S	etup	0 🔻 🔺	×		Nessu	is demp	
lessusd host Plug	gins Prefs. Scan	options Target selection	on User Credits	Ne	ssusd	host Plugins Prefs. Scan	options Target selection	User Credits
New session setu	чр			F	Plugin	selection		
9	Nessusd Host : Port :	localhost			Win Gair Bac CGI	jer abuses dows n a shell remotely kdoors abuses		
	Encryption :	twofish/ripemd160:3				/IP lote file access less services		
	Login :	nessus			Usin SME SME SME SME	Able all Enable all Enable all Enable all Enable all Enable all big NetBIOS to retrieve inform: 3 log in Enable registry Baccessible registry Permissions of W 3 Registry : permissions of will Registry : permissions of will Bacgistry : permissions of will Bacgistry : permissions of kells	inVNC's key nlogon	
		Log in			SME SME	3 Registry : value of SFCDiss 3 Registry : NT4 Service Pac 3 Registry : permissions of So 8 Registry : permissions of ke	k version chedule	
					Sta	int the scan L	.oad report	Quit
	gins Prefs. Scan	s Setup options Target selectio		₹ ≜	: ×	Ne essusd host Plugins Prefs.	ssus Setup	
	gins Prefs. Scan	options Target selectio			: ×	Ne	ssus Setup	
essusd host Plug Plugins preferenc	gins Prefs. Scan ces Ping the			▼ ▲	: ×	Ne essusd host Plugins Prefs Scan options	ssus Setup Scan options Target se	
Plugins preferenc	gins Prefs. Scan ces Ping the	options Target selectio			: ×	essusd host Plugins Prefs. Scan options Port range :	ssus Setup Scan options Target se	
Plugins preferenc	gins Prefs. Scan ces Ping the ping P ping	options Target selectio		▼ ▲	: ×	essusd host Plugins Prefs. Scan options Port range : Max threads :	ssus Setup Scan options] Target se [1-15000 8 /cgi-bin	
Plugins preference Plugins preference Do a TCP p Do an ICMF TCP ping	gins Prefs. Scan ces Ping the ping source port :	options Target selectio		₹ 4	: ×	te essued host Plugins Prefs. Scan options Port range : Max threads : Path to the CGis :	ssus Setup Scan options] Target se [1-15000 8 /cgi-bin	
Plugins preferenc Plugins preferenc T Do a TCP p TCP ping TCP ping c	gins Prefs. Scan ces Ping the ling P ping source port : destination port :	options Target selection e remote host: 60 80		₹	: ×	essusd host Plugins Prefs. Scan options Port range : Max threads : Path to the CGIs : Do a reverse lookup on	ssus Setup Scan options] Target se [1-15000 8 /cgi-bin	
Plugins preferenc Plugins preferenc T Do a TCP p TCP ping TCP ping c	gins Prefs. Scan ces Ping the ling P ping source port : destination port :	options Target selectio		₹	: ×	Ne essued host Plugins Prefs. Scan options Port range : Max threads : Path to the CGIs : Do a reverse lookup on Optimize the test TCP Ping the remote host	Scan options) Target so [1-15000 8 /cgi-bin the IP before testing it	election User Credit
Plugins preferenc Plugins preferenc T Do a TCP p TCP ping TCP ping c	gins Prefs. Scan ces Ping the ping source port : destination port : of retries :	options Target selection e remote host: 60 80		Ţ Ţ	: ×	The essued host Plugins Prefs. Scan options Port range : Max threads : Path to the CGis : Do a reverse lookup on ■ Optimize the test TCP Ping the remote host Ping the remote host Nmap	Scan options) Target so [1-15000 8 /cgi-bin the IP before testing it	election User Credit
Plugins preferenc Plugins preferenc T Do a TCP p TCP ping TCP ping c	gins Prefs. Scan ces Ping the ping source port : destination port : of retries :	options Target selections a remote host: 60 60 10		₹ 4	: ×	I te essusd host Plugins Prefs. Scan options Port range : Max threads : Path to the CGIs : Do a reverse lookup on ■ Optimize the test TCP Ping the remote host Ping the remote host Nimap Nimap top connect() scan FTP bounce scan	Scan options) Target so [1-15000 8 /cgi-bin the IP before testing it	election User Credit
Plugins preferenc Plugins preferenc T Do a TCP p TCP ping TCP ping c	gins Prefs. Scan ces Ping the ping source port : destination port : of retries :	options Target selection e remote host: 80 80 10 Nmap:			: ×	Ke essusd host Plugins Prefs. Scan options Port range : Max threads : Path to the CGIs : _] Do a reverse lookup on F Optimize the test TCP Ping the remote host Ping the remote host Nmap to connect() scan	Scan options) Target so [1-15000 8 /cgi-bin the IP before testing it	election User Credit
Plugins preference Plugins preference TO a TCP p TO an ICMF TCP ping TCP ping c Number r	gins Prefs. Scan ces Ping the ping source port : destination port : of retries :	options Target selection e remote host: 80 80 10 Nmap:		· · ·	: ×	I te essusd host Plugins Prefs. Scan options Port range : Max threads : Path to the CGIs : Do a reverse lookup on ■ Optimize the test TCP Ping the remote host Ping the remote host Nimap Nimap top connect() scan FTP bounce scan	Scan options) Target so [1-15000 8 /cgi-bin the IP before testing it	election User Credit
Plugins preference I Do a TCP p I Do a TCP p I Do an ICMF TCP ping c Number of A connect()	gins Prefs. Scan ces Ping the ping source port : destination port : of retries :	options Target selection e remote host: 80 80 10 Nmap:		3	: ×	I te essusd host Plugins Prefs. Scan options Port range : Max threads : Path to the CGIs : Do a reverse lookup on ■ Optimize the test TCP Ping the remote host Ping the remote host Nimap Nimap top connect() scan FTP bounce scan	Scan options) Target so [1-15000 8 /cgi-bin the IP before testing it	election User Credit
Plugins preference Plugins preference III Do a TCP p III Do an ICMF TCP ping c Number of A connect() \$\sciences SYN scan	gins Prefs Scan ces Ping the ping P ping source port : destination port : of retries : TCP scan	options Target selection e remote host: 80 80 10 Nmap:			: ×	I te essusd host Plugins Prefs. Scan options Port range : Max threads : Path to the CGIs : Do a reverse lookup on ■ Optimize the test TCP Ping the remote host Ping the remote host Nimap Nimap top connect() scan FTP bounce scan	Scan options) Target so [1-15000 8 /cgi-bin the IP before testing it	election User Credit
Plugins preference Plugins preference IF Do a TCP p IF Do an ICMF TCP ping c Number of A connect() SYN scan FIN scan	gins Prefs Scan ces Ping the ping P ping source port : destination port : of retries : TCP scan	options Target selection e remote host: 80 80 10 Nmap:			: ×	I te essusd host Plugins Prefs. Scan options Port range : Max threads : Path to the CGIs : Do a reverse lookup on ■ Optimize the test TCP Ping the remote host Ping the remote host Nimap Nimap top connect() scan FTP bounce scan	Scan options) Target so [1-15000 8 /cgi-bin the IP before testing it	election User Credit

Once the Target IP address or range had been filled in, click on the "Start the scan" button and the progress windows will appear.

 10.1.1.1	Portscan : Attack :		Stop
	Security check :	Marconi ASX DoS	
9 10.1.1.2	Attack : 2 Security check :	ftp writeable directories	Stop
a			

5. When the tests are completed the test results screen will appear. Expanding each colorcoded (for severity) item will provide more information on that item and it's respective fixes.

		-
×	Nessus Report 💽 🔻	_
Summary	Er	A
Found 1 security holes Found 12 security warnings	Remote FTP server banner : Iww1 ftp server (version wu-2.6.1(1) tue oct 3 14:29:19 cest 2000)	
Found 8 security notes	Security warnings The FTP service allows anonymous logins. If you do not want to share data with anyone you do not know, then you should the anonymous account, since it can only cause troubles. Under most Unix system, doing : echo ftp >> /etc/ftpusers will correct this. Risk factor : Low CVE : CAN-1999-0497	
▶	Sort by port Save as Save as NSI Close	
(())		

The results can be saved into several nicely formatted reports:

- (i) .NSR nessus readable file
- (ii) .spiffy HTML format with pies and graphs
- (iii) .HTML format
- (iv) ASCII format
- (v) LaTex format

Conclusion

In conclusion, self-assessment is a good starting point before bringing in formal and external assessment agency to conduct independent tests for audit or further insurance purposes. What this paper has covered should provide a good Do-it-yourself guide on the assessment phase of the security life cycle.

As technology advances, new exploits and vulnerabilities are discovered at an alarming pace, the lifetime of a single security life cycle had significantly been shortened. Hence requiring a faster and swifter execution of every stage of the cycle. Security professionals need to be equipped with the know-how and the technology to keep up and minimize this increasing security gap. The cycle will keep going and will not stop till the machine is unplugged and switched off, leaving us with the most secured box (un-powered) ever.

References

Jett Forristal and Greg Shipley. "Vulnerability Assessment Scanners" URL: <u>http://www.networkcomputing.com/1201/1201f1b1.html</u> (8 January 2001)

NIST Computer Security Resource Center - CSD. "SP 800-26 Security Self-Assessment Guide for Information Technology Systems" URL: <u>http://csrc.nist.gov/publications/nistpubs/index.html</u>

(August 2001)

BS ISO/IEC 17799:2000 BS7799-1:2000. "Information Technology Code of practice for information security management" (15 February 2001)

Insecure.Org homepage. "Nmap release 2.53" URL: http://www.nmap.org

(1 November 2001)

Nessus homepage. "Nessus 1.0.9" URL: http://www.nessus.org

(2 November 2001)

Beau Spafford. "The Life Cycle of Security Administration" URL: http://www.sans.org/infosecFAQ/start/life_cycle.htm

(17 April 2001)

Stuart McClure, Scrambray Joel. "Hacking Exposed 3rd Edition: Network Security Secrets & Solution" (27 November 2001)



© SANS Institute 2000 - 2005