

# Security Assessment Service

## *Security ? Anyone?*

The past three decades have introduced many new factors in the Information Technology (IT) world that have changed the security landscape many times. Introduction of UNIX has triggered the sprouting of multiple computers in a single location and introduction of Personal Computer (PC) has introduced the computing power on each desktop be it at home or at the office. The fact of the matter is that PC's have become so popular, that it is hard to imagine world without them today. Naturally, as with any technological advancement, the good came mixed with the bad. Enter, hackers, crackers, mischievous script kiddies, disgruntled employees, evil people and their uncles.

To make things worse again (yes, only from the security perspective), they were all given wide-open road to drive on. The road that has no limits or pre-defined routes, the road where every kid with a computer has the same power as any corporate CEO, where dangerousness of a person is measured in kilobits per second and megabytes of network traffic. Enter Internet in all of it's capable-of-surviving-nuclear-attack glory. Just like in good old west days: "Have a PC, willing to hack".

## *Block all, allow specific*

Today, it is safe to assume that everyone has a computer, or at least access to one. It could be at home, at work, in internet cafe or at the library. Knowing human nature and it's inclination towards hurting others, this brings the potential for evil-doing to just about every human being in the world. Scary thought! In reality, every security expert should keep this in mind. The whole world is The Enemy. Assuming less, is a guarantee for a failure. What you are trying to safe guard IS important to someone. Whatever it is, SOMEONE will have interest in it, to either have or destroy, so you don't have it either. That is why the most important rule of the Security of Whatever for Whomever is that you should always guard whatever was for you to protect with one rule in mind:

### *"Block all, allow specific"*

No one should be allowed to see, touch, or take anything unless you know who they are and are allowed to do so. Days of anonymous this or public that are gone up in the smoke of the flower power, when the network on the campus was referred to as Internet (Internal Network).

Let's review the need for security and security assessments as it stands today.

## *What is it?*

- Security Assessment is a process that consists of number of procedures to gather and examine information and/or objects (resources) related to a specific target information or object.
- Security Assessment takes in account all imaginable scenarios to acquire such resources but within the pre-determined, legal owner approved, scope.
- Security Assessment is non destructive in nature and will only point to a possible destructive effects, without actually taking advantage of them.

## *What is it NOT?*

- Security Assessment is not a product or a button that can be pressed.
- Security Assessment is not an open invitation for someone to hack or destroy your valuables.
- Security Assessment is not an embarrassment, regardless how bad the results are. It is a good and responsible step in a right direction towards safer environment.
- Security Assessment does not provide the security. It only points out the currently known deficiencies.

## *Who needs it?*

Every individual or organisation that safe guards information or objects (resources), of specific value, to itself or other individuals or organisations, should assess security employed to accomplish the task of safe guarding successfully.

## *Who does NOT need it?*

Owners of Useless-Objects-To-Be-Scrapped and Information-That-Nobody-Needs-Or-Wants. Also, People-Who-Don't-Care.

## *Who should do it?*

Security Assessment should always be done by a non-interested party. Non-interested party constitutes of one or more individuals that have no vested interest in any obtained information or objects from their legal owner.

## *Who should NOT do it?*

Security Assessment should never be done by legal owner of the guarded information or objects or any other individual or organisation that has a direct or vested interest in such information or objects. Why? Because you can't test yourself on a drivers exam.



# Security Assessment Service

## When should it be done?

Security Assessment should be done on a regular, random basis. Oxymoron? Not really. Regular, meaning, anywhere between every week to every year, based on the importance and the characteristics of the guarded resources and their environment.

Random, meaning, the Security Assessment should be done in stealth mode, with as few people knowing about it as possible.

## When it should NOT be done?

Security Assessment should not be done before major business and/or personal changes (for example, there is no point in assessing security (other than for the integration purposes) of the business that is going to be merged with another business in two weeks).

Security Assessment should not be done if the legal owner of the guarded resource has an agenda that is different from the ethical task at hand (for example, business owner hires a security expert to hack his employees private files).

## How should it be done?

Security Assessment should be done following the Security Assessment Methodology. In order to start the process, it is necessary to fulfill all the requirements in the first step:

- Customer signed Security Assessment Consulting Services Agreement
- Customer signed Limitation of Liability
- Consultant signed Non-Disclosure Agreement
- Consultant signed Letter of Action Intent
- Consultant signed Code of Ethical Conduct
- Customer supplied target site physical address, address (IP number(s) or domain name(s) and/or telephone number(s))
- Project plan outlining tasks to be done
- Customer and Consultant signed Statement of Work outlining expected deliverables

## How it should NOT be done?

Security Assessment should not be done as an ad-hoc process, as lack of methodical approach, information organization and consistency over time can not guarantee results any better than guessing.

## What are the phases that we are talking about?

- Phase 1 - Security Assessment Engagement
- Phase 2 - Site Reconnaissance from the Outside
- Phase 3 - Hacking from the Outside
- Phase 4 - Site Reconnaissance from the Inside
- Phase 5 - Hacking from the Inside
- Phase 6 - Site and Organisation Assessment
- Phase 7 - Documentation

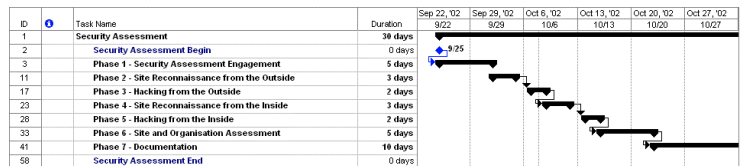
## What infrastructure will be examined?

Whatever you have and want assessed. We usually use the example module for our fixed price offering based on the following:

- One domain name
- Up to 5 (five) machines (one DNS, one web server, one web application server, one database server, one firewall)
- Up to 3 (three) network devices (one router, one switch and one load balancer)

## How long will it take?

Depending on the complexity, but for our given example infrastructure, all seven phases will take about 30 days (elapsed project time)



## How much will it cost?

For a sample infrastructure mentioned above there are five available service packages:

Service Package	Man days	Time line	US\$	CAN\$
#1 - Assessment from the Outside	16	15 days	\$24,000	\$36,000
#2 - Assessment from the Inside	16	15 days	24,000	\$36,000
#3 - Assessment from the Outside and Inside	23	20 days	\$34,000	\$51,000
#4 - Site and Organization Assessment	42	15 days	60,000	\$88,000
#5 - Total Organization Security Assessment	56	30 days	\$80,000	\$120,000



## *What are you going to get for your money?*

### **Service Packages 1, 2 and 3 sample deliverable list:**

- Results of the attempt to perform a public information attack on customer data (i.e. changing the DNS entries, or contact information).
- Results of the attempt to attack default routers and/or switches
- Results of the effects of the Denial of Service (DoS) threshold attack
- Results of the DNS poisoning attack (limited scope)
- Results of the Telephone access exploits
- Results of the User id exploits including default and vendor user ids and passwords
- Results of the User id exploits including dictionary and brute force user id and password hacking
- Results of the Windows specific actions/exploits
- Results of the UNIX specific actions/exploits
- Results of the various buffer overflow based attacks
- Results of the telnet, ftp, tftp, ssh specific attacks
- Results of the SNMP specific attacks
- Results of the RIP spoofing
- Results of the SMTP/POP/sendmail specific attacks
- Results of the DNS/bind specific attacks
- Results of the HTTP/SSL specific attacks (including specific attacks for MS IIS, Apache, NES, Cold Fusion, PHP, Perl, SSI, WebSphere and WebLogic)
- Results of the database specific attacks
- Results of the various data based attacks (malformed data, data validation attacks, etc.)
- Results of the various xterm based attacks (UNIX)
- Results of the various WAP and WEP attacks (if applicable)
- Assessment of system security policies
- Assessment of system administrator (privileged) user id's and passwords
- Writable file report
- SUID/SGID file report
- Application assessment
- Application data access recommendation
- Assessment of application administrator (privileged) user id's and passwords
- System administration, system security, application development, support and maintenance staff assessment report.

### **Service Package 5 sample deliverable list:**

All of the above (Packages 1, 2, 3 and 4)

## *Ready to start?*

Please contact us to discuss your needs and how we can help you. Your security is our business.

### **Service Package 4 sample deliverable list:**

- Application architecture assessment
- Physical data centre security assessment
- Server access policies, procedures and practice assessment
- Physical data security assessment
- Customer publicly available information assessment
- Network device assessment
- System security policies assessment
- Network traffic sniffer analysis
- System assessment
- Report on tools with high security risk
- Server hardening recommendation
- Trojan scan report

For more information, please contact:

BackGround (BGD) Software Inc.

900 Steeles Ave West, Suite 608

Thornhill, ON L4J 8C2 CANADA

Tel: (416) 917-0130

Toll-Free: (888) 230-8320

EEmail: sales@bgdsoftware.com

WWW: <http://www.bgdsoftware.com>

November 2002, © All Rights Reserved.