

BackGround Software Inc. Security Assessment Methodology

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
 - 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.

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
E-Mail: sales@bgdsoftware.com
WWW: <http://www.bgdsoftware.com>
November 2002, © All Rights Reserved.

Organized, documented, predictable approach to assessing organization security.

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.

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.

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

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 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

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)

What are you going to get for your money?

Service Packages 1, 2 and 3 sample deliverable list:

Results of the following actions:

- Attempt to perform a public information attack on customer data (i.e. changing the DNS entries, or contact information).
- Attempt to attack default routers and/or switches
- Effects of the Denial of Service (DoS) threshold attack
- DNS poisoning attack (limited scope)
- Telephone access exploits
- User id exploits including default and vendor user ids and passwords
- User id exploits including dictionary and brute force user id and password hacking
- Windows specific actions/exploits
- UNIX specific actions/exploits
- Various buffer overflow based attacks
- telnet, ftp, tftp, ssh specific attacks
- SNMP specific attacks
- RIP spoofing
- SMTP/POP/sendmail specific attacks
- DNS/bind specific attacks
- HTTP/SSL specific attacks (including specific attacks for MS IIS, Apache, NES, Cold Fusion, PHP, Perl, SSI, WebSphere and WebLogic)
- database specific attacks
- Various data based attacks (malformed data, data validation attacks, etc.)
- Various xterm based attacks (UNIX)
- Various WAP and WEP attacks (if applicable)