

Exhibit A - Security Assessment Service - Package 5 - Total Organization Security Assessment Statement of Work (SOW)

Engagement Overview

WidgetCo Inc. (Widget) has approached BackGround Software Inc. (BackGround) regarding the potential security issues surrounding Widget's network infrastructure. Widget has asked BackGround to perform the Security Assessment Service - Package 5 - Total Organization Security Assessment. During this project, BackGround consultants will attempt to discover as much as possible about the Widget's infrastructure and potential security weaknesses, from the outside and inside of the Widget's network (i.e. internet and intranet/LAN access), as well as assess the site and organization of the Widget's security infrastructure, people and processes in place.

This project is based on BackGround's unique Security Assessment Methodology and during this project the following phases of the Security Assessment Methodology will be performed:

- 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 Organization Assessment
- Phase 7 - Documentation

Based on the requirements gathered through initial review of information provided by Widget, BackGround will help Widget by staffing the following resources for the project:

- System Administrator - Security Specialist for a period of 152 (one hundred and fifty two) hour(s) at the BackGround and Customer site.
- Technical Writer for a period of 40 (fourty) hour(s) at the BackGround and Customer site.
- System Architect for a period of 64 (sixty four) hour(s) at the BackGround and Customer site in the Greater Toronto Area
- Application Architect for a period of 64 (sixty four) hour(s) at the BackGround and Customer site in the Greater Toronto Area
- Project Manager for a period of 128 (one hundred and twenty eight) hour(s) to oversee all aspects of the project management throughout the duration of the project.

BackGround Software Inc. - Professional Services
Non-managed Services
Statement of Work

Scope of the Engagement

During this BackGround managed, fixed price, fixed timeline, fixed deliverable engagement, BackGround will assign listed resources to work on a project of Security Assessment Service - Package 5 - Total Organization Security Assessment.

The following Widget's infrastructure will be examined (based on Widget supplied information):

- One physical location
- 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)

For general guidance on this assignment, the activities that will be performed by BackGround consultants will be the following:

Phase 1 - Security Assessment Engagement

- Gathering of target site physical address, address (IP number(s) or domain name(s) and/or telephone number(s)
- Project plan outlining tasks to be done

Phase 2 - Reconnaissance from the Outside

Process 1 - Public Information

- Gather publicly available information about given IP/ranges and/or domain name(s) such as
 - All domain names for a given customer
 - All blocks of IP addresses for a given customer
 - Network (Internic) information
 - Search results for customer IP(s) and/or domain(s) on newsgroups and www related to any system information (network, system and application)
 - Search results for all email addresses from a given domain on newsgroups and www.
- Gather publicly available information about given telephone number(s) or search for customers telephone numbers in white and yellow pages, newsgroups and www.

Process 2 - Site Footprint

- DNS interrogation
- Network route tracing
- Port scanning (TCP and UDP)
- ICMP queries
- Telephone access scanning

BackGround Software Inc. - Professional Services
Non-managed Services
Statement of Work

- SNMP probing

Process 3 - System Footprint

- OS detection
- SNMP probing
- Shared resource enumeration
- Dial-in services probing
- Windows specific actions:
 - TCP 139/445 null session probe
 - NetBIOS probing
 - Registry probing
 - User id enumeration (system, AD and LDAP)
- UNIX specific actions
 - User id enumeration (system and LDAP)
- Network device specific actions
 - Firewall probing
 - BGP route enumeration

Process 4 - Application Footprint

- Application enumeration (based on known ports and probe responses)
- User id enumeration (application, DB and LDAP)
- HTTP/SSL web site analysis

Process 5 - Wireless LAN Footprint

- Search for Wireless Access Points (WAP) in the proximity of the customer premises (both data centre and user locations)

Phase 3 - Hacking from the Outside

Process 1 - Public Information Attacks

- Attempt to perform a public information attack on customer data (i.e. changing the DNS entries, or contact information).

Process 2 - Network Attacks

- Attempt to attack default routers and/or switches
- Denial of Service (DoS) threshold attack (if applicable)
- 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

BackGround Software Inc. - Professional Services
Non-managed Services
Statement of Work

Process 3 - System Attacks

- Windows specific actions/exploits
- UNIX specific actions/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

Process 4 - Application Attacks

- 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
- Data based attacks (malformed data, data validation attacks, etc.)
- xterm based attacks (UNIX)
- User id exploits including default and vendor user ids and passwords
- User id exploits including dictionary and brute force user id and password hacking

Process 5 - Wireless LAN Attacks

- Various WAP and WEP attacks (if applicable)

Phase 4 - Reconnaissance from the Inside

Process 1 - Site Footprint

- DNS interrogation
- Network route tracing
- Port scanning (TCP and UDP)
- ICMP queries
- Telephone access scanning
- SNMP probing

Process 2 - System Footprint

- OS detection
- SNMP probing
- Shared resource enumeration
- Windows specific actions:

BackGround Software Inc. - Professional Services
Non-managed Services
Statement of Work

- TCP 139/445 null session probe
- NetBIOS probing
- Registry probing
- User id enumeration (system, AD and LDAP)
- UNIX specific actions
 - User id enumeration (system and LDAP)
- Network device specific actions
 - Firewall probing
 - BGP route enumeration

Process 3 - Application Footprint

- Application enumeration (based on known ports and probe responses)
- User id enumeration (application, DB and LDAP)
- Application specific probes for MS Terminal Services, Symantec PCAnywhere and Citrix

Process 4 - Wireless LAN Footprint

- Results of the search for Wireless Access Points (WAP) inside the customer premises (both data centre and user locations)

Phase 5 - Hacking from the Inside

Process 1 - Network Attacks

- Attempt to attack default routers and/or switches
- Denial of Service (DoS) threshold attack (if applicable)
- 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

Process 2 - System Attacks

- Windows specific actions/exploits
- UNIX specific actions/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

Process 3 - Application Attacks

- Various buffer overflow based attacks
- Telnet, ftp, tftp, ssh specific attacks
- SNMP specific attacks
- RIP spoofing

BackGround Software Inc. - Professional Services
Non-managed Services
Statement of Work

- 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
- Data based attacks (malformed data, data validation attacks, etc.)
- xterm based attacks (UNIX)
- User id exploits including default and vendor user ids and passwords
- User id exploits including dictionary and brute force user id and password hacking

Process 4 - Wireless LAN Attacks

- Various WAP and WEP attacks (if applicable)

Phase 6 - Site and Organization Assessment

Process 1 - Architecture Assessment

- Review infrastructure architecture including network, backup and management
- Review application architecture

Process 2 - Physical Security Assessment

- Review data centre physical security, server access policies, procedures and practice
- Review physical location for all infrastructure pieces
- Review physical security for all data (input, current and backups)

Process 3 - Public Information Assessment

- Review customer publicly available information for potential security exposures

Process 4 - Network Assessment

- Review firmware level on network devices
- Review IOS level on Cisco devices
- Review MD5 hashes for all system commands
- Assessment of system security policies
- Assessment of system administrator (privileged) user id's and passwords
- Network traffic sniffer analysis

Process 5 - System Assessment

- Review of OS level
- Review of system patch/service pack levels
- Review of MD5 hashes for all system commands

BackGround Software Inc. - Professional Services
Non-managed Services
Statement of Work

- Search for known tools by name and/or footprint
- Search for unnecessary services that can be stopped or eliminated through a server hardening process
- Internal system port scan for known trojan ports
- Assessment of system security policies
- Assessment of system administrator (privileged) user id's and passwords
- Enumerate files that are writable by public
- Enumerate root files that are SUID/SGID

Process 6 - Application Assessment

- Review of application patch/service pack levels
- Review of application setup and internet/intranet client facing interfaces for potential vulnerabilities
- Review of application access of the data for potential vulnerabilities
- Assessment of application administrator (privileged) user id's and passwords

Process 7 - Staff Assessment

- Assess system administration, system security, application development, support and maintenance staff and end-users for ability to perform their daily tasks from the point of security.

Deliverables

Following documentation will be delivered to Widget either at the end of the project or as the discovery is made, in case of the finding critical for the Widget security:

Phase 7 - Documentation

- 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 (if applicable)
- 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)

Statement of Work

- 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)
- Infrastructure architecture assessment
- 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.

BackGround Software Inc. - Professional Services
Non-managed Services
Statement of Work

Widget's Responsibilities

Widget will assign a Project Manager to act as a single point of contact for all issues related to the engagement, and be responsible for:

- ensuring availability of information and other resources needed by the BackGround team to complete their assignments;
- receiving BackGround deliverables created as a result of this engagement.

BackGround's Responsibilities

BackGround will manage the project and work with the Widget Project Manager to ensure completion of all deliverables as defined in this SOW, and:

- resolve all issues relating to this engagement in a timely and professional manner;
- secure and coordinate all BackGround resources required to meet BackGround's obligations under the terms of this SOW.

Change Control

Should Widget determine that additional Time & Materials or different resources are required to achieve additional or different results than those described above, BackGround will implement the BackGround Change Order process where the BackGround Project Manager submits a Change Order Request to the Widget Project Manager for approval. The Change Order Request will describe any changes to project resources, schedule, and cost. Widget will authorize any such changes in writing to BackGround prior to BackGround implementing the changes.

BackGround Software Inc. - Professional Services
Non-managed Services
Statement of Work

Assumptions

The following assumptions were made to create this SOW:

- Widget will provide BackGround's project staff with adequate workspace, including office desk, access to telephone, copier, fax, conference room, and printing facilities;
- Widget will provide BackGround's project staff with Widget's standard desktop workstation for office related work and network access to the Internet;
- Widget will assign a Project Manager for the duration of this engagement;
- All BackGround project deliverables will be received by Widget Project Manager and deemed as accepted upon delivery;
- BackGround project work will be performed at BackGround and Customer facilities in Greater Toronto Area;
- The engagement will begin up to two weeks after receipt of a valid purchase order and signed agreement, or at on another, mutually acceptable date.

Should any of these assumptions prove to be incorrect or incomplete, BackGround reserves the right to modify the rates or schedules described in this SOW.

Project Start Prerequisites

- Customer signed Security Assessment Consulting Services Agreement (CSA)
- Customer signed Limitation of Liability (LOL)
- Consultant signed Non-Disclosure Agreement (NDA)
- Consultant signed Letter of Action Intent (LOI)
- Consultant signed Code of Ethical Conduct (CEC)
- Customer supplied target site physical address, address (IP number(s) or domain name(s) and/or telephone number(s)
- Customer and Consultant signed Statement of Work (SOW) outlining expected deliverables
- Customer issued Purchase Order in the full amount of the service to be performed