

## Ronald Bowes

604-870 Cambridge Street

Winnipeg, Manitoba

R3M 3H5

Phone: (204) 960-4345

Email: [ron@skullsecurity.net](mailto:ron@skullsecurity.net)

---

### Profile

---

- Bachelor of Computer Science (Honours), graduation date of April 2006
  - Reverse engineered and implemented security checks and libraries for dozens of undocumented software platforms at Tenable Network Security, considerably expanding their security scanner's capabilities
  - Helped improve the Government of Manitoba's security posture by installing and maintaining leading edge security tools and training developers
  - Generated record amounts of press coverage by expanding Symantec's Internet Security Threat Report
  - Achieved two GIAC certifications: GPEN (96% on the certification exam) and GCIH (98% on the certification exam)
  - Developed open source scripts for the Nmap Scripting Engine with a wide range of purposes, including vulnerability and backdoor detection
- 

### Certifications

---

- (ISC)<sup>2</sup> Certified Information Systems Security Professional (CISSP)
  - GIAC Certified Incident Handler (GCIH) (Silver)
  - GIAC Penetration Tester (GPEN) (Gold)
  - Arcsight Certified Security Analyst (ACSA)
  - Arcsight Certified Integrator/Administrator (ACIA)
  - Bachelor of Computer Science (Honours) (University of Manitoba)
    - Specialized in networks and security
- 

### Work Experience

---

November, 2010 - Present

Winnipeg, MB

#### **Vulnerability Research Engineer**

#### **Tenable Network Security**

- Reverse engineered and implemented undocumented network protocols used by Enterprise software (such as Microsoft, HP, Citrix, Red Hat, and others)
- Implemented complicated network protocols based on specifications, often on short timelines
- Wrote audits to validate that the most recent version of software was installed on customers' networks (with minimal false positives/negatives)
- Performed detailed analysis of software patches for a variety of software platforms, especially Microsoft's Patch Tuesday patches
- Implemented several protocol libraries that are actively used by other developers

January, 2010 - March, 2010

Winnipeg, MB

**Mentor (Instructor)**

**The SANS Institute**

- Taught SANS Security 560 (Penetration Testing and Ethical Hacking) to a group of local students
- Covered the same material as a full SANS course, but in half the time due to the Mentor format
- Helped students work through labs, demonstrations, and the final hands-on workshop
- Averaged a 100% ranking from the students, was asked to run another class in the future

November, 2007 – October, 2010

Winnipeg, MB

**Senior Security Analyst**

**Information Protection Centre**

**Government of Manitoba**

- Performed security analysis and penetration testing of Web applications, mostly ASP.net, Java, and PHP
- Trained and directed developers on best security practices for coding
- Installed, configured, monitored, and maintained a security event management system (ArcSight)
- Developed tools and scripts to identify unpatched or vulnerable hosts on our network
- Mentored six students per year from the University of Manitoba Computer Science Co-op program. Participated in all aspects of the Co-op program, including interviewing, selection, mentorship, supervising, and reviewing

January, 2007 – October, 2007

Calgary, AB

**Security Analyst / Editor**

**Symantec Corp**

- Helped expand Symantec's Internet Security Threat Report to cover new regions and organizations
- Built tools to monitor black-market transactions, such as credit card sales
- Edited corporate blog posts for grammar and content

May, 2006 – December, 2006

Winnipeg, MB

**Programmer / Project Manager**

**Great White North Software Solutions**

- Developed and maintained applications written in PHP and MySQL
- Wrote an extensive PHP application that interfaces with AutoCAD, automatically generating material lists, costs, and reports for a building company
- Helped maintain and customize "Global Office," which is an office-manager suite.

---

## Volunteer and Opensource Work

---

### Hackerspace

- Founder and president of Winnipeg's first and only hackerspace - SkullSpace Winnipeg Inc.
- Handling all aspects of running a non-profit, including legal matters, running meetings, facilitating projects, public relations, handling relationships with related groups, securing funding, and more
- In its first year, SkullSpace Winnipeg has become Canada's largest hackerspace by membership size
- Ran a workshop on reverse engineering skills for over 20 members

### Nmap Security Scanner

- Wrote a collection of over 24 Nmap Scanning Engine (NSE) scripts, including several libraries
- Wrote a script to detect Conficker infections with a short and strict deadline, helping Nmap achieve a record number of downloads
- Implemented Microsoft's Server Message Block (SMB) and Remote Procedure Call (MSRPC) protocols in Lua through a combination of packet logging, reading books and whitepapers, and trial and error
- Helped security group from an American university scan networks for weak passwords and vulnerable systems; found hundreds of such systems, including a domain controller with blank administrative passwords
- Published several blogs on the subject, which frequently explain the intricacies protocol to a technical (but not specialized) audience
  - <http://www.skullsecurity.org/blog/?cat=9>
- Authored a paper titled Scanning Windows Deeper With the Nmap Scanning Engine:
  - [http://www.giac.org/certified\\_professionals/practicals/GPEN/00049.php](http://www.giac.org/certified_professionals/practicals/GPEN/00049.php)

### Battle.net Protocol Analysis

- Reverse engineered and implemented an open source version of Blizzard's Battle.net protocol, including version validation, encryption, and authentication. This included Blizzard's implementation of the Secure Remote Password (SRP) protocol and their enhanced "lockdown" protection:
  - <http://www.skullsecurity.org/wiki/index.php/SRP>
  - <http://www.skullsecurity.org/wiki/index.php/Lockdown>
- Generated reusable code whenever possible; has since been used in several successful projects, including Just Another Battle.net Login Service (JBLS), which handled over 1000 login requests per day

### Assembly language tutorial

- Wrote a tutorial on x86 assembly language and reverse engineering, due to interest generated by my Battle.net work:
  - <http://www.skullsecurity.org/wiki/index.php/Assembly>
- Targeted developers with a technical background, but not necessarily with a background in low-level languages

---

## Technical Skills

---

### Networking

- Firm understanding of scanning and penetration testing tools, including Nmap, Metasploit, Wireshark/Ethereal, Nessus, Foundstone, IBM AppScan, Paros, Burp Suite, Netcat, Hydra, John, Rainbow Crack, and many more
- Firm understanding of network security concepts, including threat and risk analysis, security event/incident monitoring, asset and risk management, and intrusion detection and prevention sensors
- Experienced with configuring both Windows and Linux networks
- Basic knowledge of SAP deployment and security

### Operating Systems

- Proficient with Linux-based systems
- Experienced with many versions of Windows (including Windows 7), UNIX, BSD, and Solaris

### Programming Languages

- Firm understanding of programming (and reading) C, C++, Java, PHP, Intel x86 Assembler, and Nessus Attack Scripting Language (NASL)
- Experienced with penetration testing and code auditing against ASP.net, Java, PHP, and C/C++
- Experienced with reverse engineering C/C++ and ASP.net code
- Working knowledge of Visual Basic, Javascript, Perl, and BASH Shell
- Working knowledge of reading and writing malicious C, Intel x86 Assembler, and Javascript code
- Basic knowledge of Motorola 68k, SPARC, MIPS, ARM, Ruby, DirectX, and Simple DirectMedia Layer (SDL)

### Reverse engineering

- Proficient with the use of disassemblers and debuggers
- Experienced with reverse engineering network protocols
- Working knowledge of reverse engineering cryptographic algorithms

---

## Interests

---

- Open Source Software development (especially the Nmap security scanner)
  - [http://www.skullsecurity.org/wiki/index.php/My\\_Projects](http://www.skullsecurity.org/wiki/index.php/My_Projects)
- Computer security, such as reading mailing lists and magazines and maintaining a blog and wiki
  - <http://www.skullsecurity.org/blog>
  - <http://www.skullsecurity.org/wiki>
- Reverse engineering and lock picking, out of general interest
- Outdoor activities, such as camping, hiking, and going to the cottage
- Computer, strategy, and role-playing games
- Indoor rock climbing
- Running
- Cycling
- Exploring