Programming/Computer Skills and Miscellaneous:

- Develop/architect development projects from scratch
- Test myself by coding on paper, then test compilation errors/syntax
- Optimize/refactor/inline to condense the number of lines of code in modules/subroutines, for less overhead (cpu cycles)
- In depth knowledge of Linux
- In depth knowledge of C/Java/PHP/JQuery
- root/Linux exploits (bypass regular user shell and spawn a root shell, ie kernel fd race condition)
- keygens
- patches
- zero days
- shellcode
- assembly x86
- Linux kernel modules
- Virtual Machines/Hypervisors (VirtualBox, VMWare, Qemu)
- Speed-reading
- Typeracing
- Fast researching/resourcing literature and documents
- Attention to details (detail oriented)
- Built my own computer (medium tower with window, Fan Tower Heatsink, no water cooling loop), knowledge of computer hardware/components and the IPC
- Implementing in subsequent development projects: Kubernetes, Docker, CAAS (container orchestration), Vagrant
- Debugging/troubleshooting: stack traces, segmentation faults, core dumps, kernel/system logs, dev/proc pseudo-filesystems
- Subversioning (repository): subversion, git, gitlab, mercurial
- Developed Linux desktop GUI application using: gtk and qt4
- asymetric vs symetric key encryption (ie: SSH2 protocol, SSH keygen)
- run Linux on bootable USB key (modify boot order in BIOS/UEFI) using Yumi/unetbootin
- derriks DBAN software (securely deletes all data/partitions/formatting and writes 0s to all sectors of the HD in multiple rounds, using a large cost coefficient)
- knowledge of powershell/command prompt/regedit in Windows (ie: netsh, all command prompt builtins)
- magic jellybean (retrieve Windows product key)
- raspberry pi and arduino (breadboard/GPIO/LED/PWM etc)
- Server side game predictions/collision detection

Other Software

- xfire
- ventrillo
- teamspeak
- discord
- slack
- skype

- yumi
- vlc
- cpuz
- cantordust
- putty
- cygwin
- exiftool
- portablewincdemu
- audacity
- VAC (virtual audo cable)

Text Editors/IDEs (no particular order)

- Sublime Text 2
- Notepad++
- Notepad
- Wordpad
- Bluejay
- Sun Java Studio One
- Netbeans
- TextEdit
- Kate
- Kwrite
- Vim
- Gedit
- JetBrains PHPStorm/IntelliJ
- Atom
- Eclipse
- Nano
- Emacs
- Dreamweaver Studio
- Microsoft Office Suite
- Libre Office

Live Streaming Websites Used:

- stickam.com
- justin.tv
- blog.tv
- blab.im
- twitch.tv
- dlive.com
- mixer.com
- youtube.com (live streaming)

Linux Distros Used (distrowatch.org):

- Blackarch
- QubesOs
- Arch Linux
- Gentoo
- Fedora
- CentOS
- Puppy Linux
- LFS
- Mandriva
- OpenSuSe
- Slackware
- FreeBSD
- Openbox
- Fluxbox
- Kali Linux (Formerly BackTrack)
- Debian
- Ubuntu
- Lubuntu
- Kubuntu
- Raspbian
- Xebian
- ArchBang

Linux Tiling/Window Managers Used (scripts/configs: dotshare.it)

- Awesome
- Xmonad
- dwm
- wmfs
- enlightenment
- cinnamon
- Gnome
- KDE
- LXDE
- XFCE

P2P software used (Gnutella p2p network):

- Kazza
- Limewire
- Shareza
- DC++
- BearShare
- FrostWire
- iMesh

Areas of specialization:

- Dynamic Memory Management (Heap/Stack)
    - valgrind (identify memory leaks/performance bottlenecks

  Data Structures
    - Memory maps, depicting address/references/values in memory (Java/C)
    - Big (O) n!, 2^n,n^2,nlogn,n,logn,1 (worst to best, respectively)
    - Knowledge of: Trees, B-Trees, Linked Lists, Doubly Linked Lists, Matrix, Array Lists, HashMaps, qsort, bsearch
    - Recursion, recursive functions
- Operating Systems
    - Created LearnLinuxLive VM including an internal (lower resource WM) VM, watch users “break” into a “limited shell” using non blacklisted Linux builtin commands, winner receives congratulation animations (prolog) Essentially, users are able to witness this live as it happens. They can choose to participate, or learn from more experienced users. (more info: twitch.tv/learnlinuxlive)
    - Win32 API interfacing/programming
    - Win32 DLL (__cdecl/__stdcall) hooks/injection (Read/WriteProcessMemory)
    - GNU/Linux monolithic/micro kernel/modules/pseudo-filesystem study/development
    - Windows ASLR (Address Space Layout Randomization), built into windows 7+
        - ASLR not implemented in early version of Windows (< XP)
        - Modify values at specific memory addresses to activate cheats (ie. CheatEngine)
- Game Development
    - Created 2 game clones of Space Invaders in C++/Java
        - C++ (win32 API interfacing)
    - Networked (C sockets) Tic-Tac-Toe game in C using Gtk UI
- Networking
    - network attacks (smurf/arp poisoning)
    - C raw sockets (Frame injection, Layer 2 OSI Model)
    - NIC Packet Injection/monitor mode
    - Wireless 802.11 a/b/g/n network forensics/scanning/probing
    - Java IRC client clone RFC1459
    - Java Anonymous email sender (fake/spoofed emails using free SMTP server)
    - Worked with AP (Routers): 2Wire, Linksys, TP-Link, D-Link, Hitron
    - Worked with industry network devices/equipment at college to perform practical exams (subnetting, configuring devices, firewalls (iptables), physical cabling)
    - Interfaced with computer lab laserjet printer, to modify the LCD display text using C in conjunction with PJL protocol (Printer Job Language)
    - P2P/Anonymizer protocols: Gnutella, I2P, Tor
    - Network encryption protocols knowledge: WEP, WPA, WPA2-PSK, CCMP
    - Flashed Linksys router (AP) with DD-WRT firmware (homebrew: unlocked all features)

- Real Time Systems
    - QNX (Virtual Machine/Hypervisor) C multithreaded development (C pthreads, POSIX threads)
    - Multithreading
    - Backend server net code/architecture
        - edge triggered/level triggered
        - AWS backend architecture
        - remote command executor client/server model
        - remote backend trojan (desktop prank)
- Network Security/Pentesting/Cryptography
    - entropy (hardware interrupts, mouse/keyboard movements to generate the most random seed values)
    - aircrack-ng
    - nmap
    - Linux network commands builtins
    - metasploit (ruby with embeded shellcode)
    - Twitter deamon bot used to parse (HTML DOM) exploit-db.com and tweet out new (local, remote, papers, exploits and CVEs etc) links + other metadata
    - diffie-hellman algorithm
    - ssh2 protocol
    - smurf attack (arp poisoning)
    - SQL injection
    - DDOS attacks/prevention (kernel level, tcp_syncookies)
    - Session Hijacking, Session poisoning
    - TCP Handshake spoofing
    - TCP connection hijacking
    - firewalls (ICMP management, drop/allow ip/ports)
    - TCP Syn scanning
    - TCP Xmas attack (set 3 TCP opts: URG, PUSH, ACK)
    - netcat (reverse TCP backdoor shell)
    - sslstrip (decrypt SSL/TLS certificate stream data)
    - DVWA (Damn Vulnerable Web Application, web application riddled with exploits/CVEs, useful for pentesting your website)
- Reverse Engineering
    - ollydbg/java decompiler/ida pro decompiler/infinity debugger/gdb
    - Runescape (early 2000's, jar file decompilation/created my own runescape esq website, hosted on freewebs/ftp)
    - Skype (Protocol encryption/p2p network inspection)
    - MSN Messenger (early 2000's, protocol inspection, which was plain text)
    - Original Xbox, softmod splinter cell exploit to install xebian (xbox linux distro)
    - Samsung s3 rooted/jailbroken, installed busybox, cyanogen mod (modded android distribution), paranoid android, GNU/Linux
    - Original Ipod, installed Linux and ran game emulators (ie DOOM)
    - Xbox 360, installed firmware hardware mod (not JTAG) on DVD/R to autoplay burned game iso
    - Flashed custom DD-WRT firmware on Linksys router (AP) to unlock device

- Wired ADT DSC PC5010 alarm system with envisalink 4 microcontroller with embedded EEPROM and integrated RJ31 phone loop connection (enabled self monitoring)
- Ophcrack, rainbow tables, chntpwn, cain and able, brute force attacks
- PJL (Print Job Language) send commands (change display text, put printer in out of service mode, beep) to printer (port 9000)
- bypass anti cheat systems (punkbuster/VAC)

Comprehensive List of Projects

- small HTML websites (even one running the old school Runescape java applets)
- IRC (RFC 1459) express client
- MSN console client (utilizing the old protocols)
- java space invaders game clone
- java anonymous SMTP client
- Skype addon
- TicTacToe console client
- networked client/game server (utilizing WINSOCK)
- low level Linux code (change NIC MAC address)
- java Asteroids game
- java Chat Server
- java Nim game
- RoboCode
- reverse engineering (ASM, code caves, cracks, patches, keygens, self-keygens etc)
- WIN32 GUI programming
- MOSH (C my own shell)
- C memory address modifier
- CodeX scene decryptor for programming challenge
- IDA/ollydbg decompilers to view ASM
- HTTP download client, ICMP PING client
- jtvXpress (JTV movable windows)
- Python bot (scrape exploit website for list of exploits and tweet them out)
- Camcast.it (my own video streaming website)
- C IP is online check
- C live IPC (print details constantly)
- C network file downloader
- C raw sockets (send a custom frame over the wire)
- RCE_CONSOLE (remote command executor)
- C Linux wall command spammer
- C Linux mouse button logger/open CD rom
- WIN32 RCE (Remote Command Executor)
- TicTacToe network project
- C multithreaded (pthreads) client/server architecture utilizing dynamic memory allocation
- TwitchTerminal/LearnLinuxLive 2 Twitch.tv projects
- Intellishopper (NDA)