Robert J. Neel

SUMMARY

- Masters degree in Computer Science and 1700+ documented hours of CS training beyond degree
- GCIH, GPEN, and GWAPT certification
- NSA Network Exploitation/Vulnerability Analyst, USAA's Red Team founder/lead, and owner of PEN Consultants
- 20 years in Information Technology, 13 years in Information Security/Cybersecurity
- Experience with 28 programming languages; written complex programs for both offense and defense in 17 of them
- Six patents pending
- Top Secret / SSBI clearance (2008-2019)

RELEVANT CAREER HISTORY

PEN Consultants, LLC **San Antonio, TX** **2013 - Present**

- Founder and owner of the Information Security & Cybersecurity testing firm, PEN Consultants
- Conduct in-depth automated/manual application and security and penetration testing, red teaming, document and present discovered vulnerabilities and confirmed attack vectors to the client, provide detailed mitigation steps, etc.
- More details: https://PENConsultants.com
- Sample testing report: https://penconsultants.com/home/sample-security-testing-report/

USAA **San Antonio, TX** **2014 - 2019**

- Founded and led USAA's first: red team, hunt team, and weekly brown bag training sessions
- Discovered hundreds of vulnerabilities in USAA and vendor systems, recommended mitigations and created detections
- Served as the SME in: red/attack, malware analysis, hunt, EDR, detections, active defense, training, etc.
- Wrote/created hundreds of programs and scripts to find/detect evil and to automate processes
- Created thousands of signatures/rules (snort, yara, openIOC, various vendor formats, etc.), behavior based detections/IOAs, custom detection frameworks, etc.
- Interacted with teams at every level across the enterprise and participated in various invitee-only intel channels
- Accolades: 6 patents pending, 19 innovation awards, 3 spot awards, performance bonuses

National Security Agency **Fort Meade, MD and San Antonio, TX** **2008 - 2014**

- Toured in eight offices within NSA (6-9 months each) as part of a structured development program, including defensive tours in the NSA/CSS Threat Operations Center (NTOC) and offensive tours in Tailored Access Operations (TAO), as a Global Network Exploitation and Vulnerability Analyst (GNEVA), followed by a permanent assignment in San Antonio
- Provided NSA with new exploitation capabilities and defensive mitigations by analyzing (both white/black box approaches) computer systems, source code, network systems, computer protocols to exploit and/or protect by designing, demonstrating, and implementing exploitation techniques and/or mitigations
- Performed assessments against various COTS software, hardware and web services and produced/delivered executive summaries and detailed reports to customers which were used to protect systems throughout the DoD and .gov
- Created computer algorithms, protocols and software prototypes in response to customer requests and collaborative requirements review meetings which gave NSA six new capabilities, four of which eventually became corporatized
- Served as lead developer and DBA for a new corporate SIGINT tool where my individual contribution was 16,175 lines of PHP/HTML/JavaScript/CSS, 575 CSS, 2,049 JavaScript, 686 of Perl, 7,804 of Python, 6,954 of MySQL, all code reviewed by colleagues that provided a capability which was utilized throughout the Intelligence Community
- Accolades: 2 Performance Bonuses, Discovery Award, Individual Cost Savings/Productivity Award, Special Achievement Award

Various full-time Technology positions **TX and CO** **1999 - 2008**

- Hardware Engineer at Lockheed Martin, Net/Sys Admin for Red Oak ISD, and Tech Director at DeSoto AG Church
- Performed information/cybersecurity/app pen testing, system and network administration, DISA compliant hardening, computer forensics/investigation, data retrieval, incident response, system integration, system/network troubleshooting/repair/installation/configuration, VoIP and VPN installation/repair, automation, security and surveillance, SatCom, etc.

PUBLIC WORKS

- Presenter: at HackWest, BSides SATX, BSides Austin, and the Executive Women's Forum; also presented to NSA director ADM Mike Rogers, Commander Army Cyber Command LTG Ed Cardon, and Deputy Commander Army Cyber Command GEN Paul Nakasone
- Published dozens of articles (ex. https://penconsultants.com/blog)
- Active on Gitlab (ex. https://gitlab.com/users/J35u5633k/projects), although most teams and projects are private
- Twitter (@redeemedHacker), LinkedIn (@RNeel)

FORMAL EDUCATION

- MS in Computer Science from The University of Texas Arlington with a specialization in Computer Networking and Security - 2007
- Graduate from The National Security Agency's Computer Network Operations Development Program as a Global Network Exploitation and Vulnerability Analyst with a specialization in Computer Network Protection and Exploitation – 2012

FORMAL TRAINING

- Security Testing: SANS Network Penetration Testing and Ethical Hacking (SEC560), Web App Penetration Testing and Ethical Hacking (SEC542), Foundstone's Ultimate Hacking, Foundstone's Ultimate Hacking - Expert, Foundstone's Ultimate Hacking - Windows, Foundstone's Ultimate Hacking - Wireless, Art of Exploitation - Bootcamp, EC-Council's Ethical Hacking and Countermeasures
- Intrusion Detection/Security: SANS Intrusion Detection In-depth (SEC503), SANS Perimeter Protection In-depth (SEC502), ANRC's Cyber Threats Detection and Mitigation, Red Hat's Kernel Security (RHD351), Red Hat's Enterprise Security: Network Services (RHS333), Network Security and Cryptography
- Analysis: Intermediate and advanced Software Analysis Laboratory, ANRC's Network Traffic Analysis, Intermediate Protocol Analysis, ANRC's Malicious Network Traffic Analysis
- Neworking/Tech: Cisco's Interconnecting Cisco Network Devices Part 1 (ICND1), Global Knowledge's IPv6 Foundations, Global Knowledge's Wireless Networks I (Integration/Troubleshooting) and II (Security/Analysis), Bill Gatliff's Embedded Linux, Microprocessor Laboratory
- Malware: Linchpin Labs Malware (LPL2003), ANRC's Basic Malware Analysis
- Certs: GPEN (2015), GCIH (2016), GWAPT (2019)

LANGUAGES / TECHNOLOGIES

- Security Testing: Nessus, OpenVAS, Qualys, NMAP, masscan, Metasploit, Netcat, Helix, Auditor, BackTrack/Kali, DISA Gold Disk, SysInternals, IDAPro, OllyDbg, WinDbg, IDA Pro, Nikto, JohnTheRipper, Cain/Abel, Paros/OWASP ZAP, Burp, Squid, WEP/WPA auditing, coWPAtty, Aircrack suite
- Network Administration and monitoring: VLAN, 802.1x, iptables, routes, firewalls, IDS/IPS, VPN, VoIP, Wireshark/TShark suite, Ettercap, TCPDump/WinDump, NS2, NetWitness Investigator, Snort, Netflow, SiLK
- System Administration and monitoring: Windows Server 2k3/2k8 R2, Active Directory, Group Policy, registry/regedit, Unix, Various Linux Desktop/Server, macOS, Android, plist, Antivirus
- Programing: Network programming in Python, PowerShell, Perl, Ruby, VB[A][.net], AppleScript, Batch, Bash, awk, flex, sed, C/C++, Objective-C, c# .net, Java, Go, R, Swift, x86 Assembly; MySQL, Oracle; HTML, JavaScript, ASP, PHP, CSS, SSI, XML, SOAP
- Protocols: ARP, DHCP, DNS, FTP, HTTP, IMAP, ICMP, IP, POP3, SIP, SMB, SMTP, SSL, SSH, TCP, TELNET, UDP
- Technology/Misc: 802.11abgn, wireless backhaul, VoIP, fiber, IDAPro, xxd, XVI32, regex, yara, Fireeye HX/EX/NX, Cylance Optics