Sydney S Leigh | Nashua, NH, 03062|
603-521-0458 | Sydney.S.Leigh@gmail.com |
https://www.sydney-leigh.com

PROFESSIONAL SUMMARY

Practiced for more than 10+ years experience in cybersecurity for the federal government, engaging in various roles from auditing, to penetration testing, to system administration, to being a project manager and liaison, I've been well rounded with a few particular specializations. Having attained a (CISSP) certificate in 2017, I have been actively pursuing a goal towards being a Chief Security Officer (CSO). My ideal role would position me as the CSO/CISO or potentially lead a smaller team taking on high impact responsibilities such as simplifying and refining complex security policies or assisting with internal and external audits.

PROFESSIONAL EXPERIENCE

DOD, US ARMY CORPS OF ENGINEERS, Computer Scientist, Vicksburg, MS, Sep 2012 - Present
- Acted as a liaison between two major agencies, translating technical jargon into laymen terms among dozens of people in order to fund multi-million dollar projects
- Performed multiple DIACAP compliance audits across the USA interfacing with customers, helping them understand the DoD requirements they have to meet, doing SCAP scans, and working with my team to revise verbiage on the reports we needed to send to get them approval to operate
- Administered and ran honey pot to collect attack data from the world wide web
- Wrote a small command and control based botnet in C++ for a virtual laboratory
- Performed Windows administrative work on a Virtual Desktop Environment (VDI) with VMWare
- Created Powershell Script for automating user entry into Active Directory (AD) to save hundreds of hours of labor instead of entering it manually through the GUI
- Information Assurance Technician II (IAT II) assisted senior admin with software installs for VMWare ESXi
- Ensured access to export controlled codes and data was kept private by use of file permissions and handled by DOD and Army Regulation standards

BOWHEAD, Engineer/Scientist I, Vicksburg, MS, Mar 2012 - Sep 2012
- Created a virtual laboratory involving an Apache, IIS, a DNS server, and a web application firewall (WAF) called Mod Security for IDS research

DOD, DEFENSE INFORMATION SYSTEMS AGENCY (DISA), Red Team, Chambersburg, PA, Jun 2011 - Aug 2011
- Helped plan missions and procedures for Red Team
- Built a web application with web2py for organizing attack tools.
- Trained on Certification and Accreditation (C&A). Information Assurance (IA) Policy, Personally Identifiable Information (PII), Continuity of Operations (COOP), and Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)

MSU IT DEPARTMENT, Compliance Officer, Mississippi State, MS, Jun 2010 - Aug 2010
- Made shell scripts to automate the examining of abnormal DNS servers to look for malware & SSH brute force attacks.
- Programmed proof of concepts for XSS bugs found on campus websites by vulnerability scanners to demonstrate security vulnerabilities to CSO

- Did vulnerability scanning of many machines on campus with Nexpose

EDUCATION

- Masters of Science in Computer Science from Mississippi State University, graduated 2011
- Bachelor of Science in Computer Science with a minor in Software Engineering from Mississippi State University, graduated 2009

CERTIFICATIONS

- CompTIA Security Plus certified (Current)
- Certified Information Systems Security Professional (CISSP)
- SANS Global Information Assurance Certified Intrusion Analyst (GCIA)
- Sandia National Labs (SNL) Information Design Assurance Red Team (IDART) certified
- InfoSec Institute Certified SCADA Security Architect (CSSA)
- InfoSec DIARMF certified
- NIST 800-53B Control Baselines certified

PUBLICATIONS

- *HIPAA Violated by Wireless Access Points*, Published and presented at the International Conference on Information Security and Privacy 2010

PASSION PROJECTS

- Made my own version of Ubuntu Linux for Cryptocurrency cold storage offline. This included an air gaped laptop that was hardened to NIST hardening guidelines
- Written Buffer Overflow (BOF) exploits from scratch in labs in college using C and metasploit shell code for a C application using gdb
- Participated in many online hacking competitions such as Defcon, Hack.lu, DC3 digital forensics challenge, etc.

SKILLS

- Risk Management Framework (RMF), DIACAP, NIST 800-53, ISO 27001, PCI-DSS, HIPAA, Auditing, Windows, Windows Server, Linux, Linux Server, Governance Risk and Compliance (GRC), Information Security (InfoSec), Penetration Testing (Pen Testing), Incident Response (IR), Forensics, Digital Forensics, Honey pot, Cryptography, Apache, Internet Information Services (IIS), DNS, Web Application Firewall (WAF), Mod Security (Apache WAF), Red Team, Blue Team, Purple Team, Vulnerability Assessment, Risk Assessment, Nexpose, Malware Analysis, Packet Analysis, Secure Shell (SSH), Cross-site Scripting (XSS), Buffer Overflow (BOF), Exploits, OllyDbg, IDA Pro, GNU Debugger (gdb), Metasploit, Backtrack Linux, Helix Linux, Forensics Toolkit Imager (FTK Imager), Windows Sys Internals, Windows Event Viewer, Public Key Infrastructure (PKI), Asymmetric Cryptography, Symmetric Cryptography, Digital Signatures, RSA, Structured Query Language (SQL), SQL Injection (SQLi), Hashing, Hash Algorithms, MD5, md5sum, SHA, sha256sum, Rainbow Tables, Password Cracking, Brute force, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, Man-in-the-middle attacks, DNS Poisoning, Open Systems Interconnection (OSI) Model, Advanced Encryption Standard (AES), AES-256, SCAP, Secure Sockets Layer (SSL), SSL Certificates, Transport Layer Security (TLS), Tunneling, Virtual Private Network (VPN), Secure Hypertext Transfer Protocol (HTTPS), Ports and Protocols, Port Scanning, Port Knocking, Shell Code, No Operation Sledding (NOP Sledding), Social Engineering, Social Engineering Toolkit (SET), Physical Security, Rootkit, Poison Ivy, Remote Access Terminal (RAT), Windows Binaries, Portable Executable Header (PE Header)