

Computer Security Analyst Computer Security Analyst Computer Security Analyst - Lockheed Martin Ashburn, VA Work Experience Computer Security Analyst Lockheed Martin - Ashburn, VA May 2014 to Present Research and respond to vulnerabilities related to the Lockheed Martin Flight Services Program. ? Manage, deploy, and update McAfee Products to systems and servers via McAfee e-Policy Orchestrator. ? Troubleshoot Windows and Linux server environments. ? Responsible for the maintaining and upgrading of all security based servers and devices. ? Ensure firewall configurations meet company policy. ? Review SIEM logs and investigate potential threats and hacks. ? Respond to intrusion detection alerts and mitigate threats as necessary. Sandia National Laboratories - Albuquerque, NM July 2013 to May 2014 Researched and developed tutorials to aid trainees in navigation through Tracer FIRE (Forensic Incident Response Exercise) an educational training for cyber security incident responders. ? Developed and hacked a model railroad train module as a part of a larger simulated city project used to educate children grades k-12. ? Reverse engineered Jython script to write Python scripts implementing PySerial in order to access serial USB ports to connect to a model railroad train. ? Developed cyber security lesson plans to assist teachers in walking through the cyber train module with students. ? Created and managed Linux virtual machines for the students to complete their cyber train modules. ? Researched mobile forensics using the Cellebrite UFED system to analyze data found on mobile devices (Android, iOS, Microsoft). IT LAN Services and System Administrator Dominion Resources - Norfolk, VA May 2011 to January 2013 Prepared and deployed hundreds of assets for new and existing employees and set up their user access profiles within Active Directory ? Responsible for the imaging and deployment of thousands of Windows 7 machines as a part of a companywide migration project which included over thirty thousand machines ? Connected hundreds of devices to the company's LAN network and had to troubleshoot issues surrounding network connectivity ? Actively managed the functioning of the enterprise by utilizing an online ticket system to translate user requests into technical diagnoses and apply the diagnoses into a solution that suited the user's needs PROJECTS ? Utilized the Software Development Life Cycle (SDLC) to design, develop, and test a unique Java based Android application prototype, which included file shredding for all

social media metadata, remote access to application, and implement encryption to blocks of the device's flash memory via the Bouncy Castle library ? Utilized the UFED Cellebrite Forensic Toolkit to extract data from mobile devices (iPhone, Android, and Microsoft) and analyze data pulled via EnCase to build an application that will securely overwrite and delete social media metadata on Android devices. ? Utilized open source penetration testing tools such as Nessus Vulnerability Scanner, Metasploit Framework, nmap, and John the Ripper to research vulnerabilities in a virtual competition environment (National Cyber League Fall 2013) ? Utilized Socket Layer for Android to port Python socket programming to Android platform and developed a script to connect to the Android application remotely ? Set up small LAN network to implement firewall rules and perform penetration testing which included utilizing Wireshark to dissect packets, sniff traffic via Snort IDS, and detect packets that contained keywords ? Researched the security implications of cloud computing in order to design, develop, and partially implement a cloud prototype for students to upload documents/media to share with classmates at Norfolk State University using a local server to host it using PHP ? Researched and analyzed Format Preserving Encryption in order to pose possible implementation for a database encryption scheme using an onion encryption method ? Utilized Backtrack 5 while participating in an Ethical Hacking workshop hosted by Norfolk State University to learn how to create spoof emails via spear phishing, exploit network vulnerabilities, and launch attacks to other virtual machines

RELEVANT COURSEWORK ? Network Defense, Computer Security, Education Master of Science in Computer Science Norfolk State University - Norfolk, VA May 2014 Bachelor of Science in Computer Science Norfolk State University - Norfolk, VA July 2012 Additional Information ? Operating Systems: Windows (user, system administrator), Mac OSX, Linux

Name: Deanna Morgan

Email: cynthia22@example.org

Phone: 001-504-695-4084x557