Research Assistant- Preliminary Forensic Analysis of Amazon Echo Research Assistant- Preliminary Forensic Analysis of Amazon Echo CEH | CCNA | BS ISO 27001:2013 LA Baltimore, MD Insightful, results-driven IT Security professional with notable success in directing a broad range of corporate IT security initiatives while participating in planning, analyzing, and implementing solutions in support of business objectives. Highly focused with an ability to meet deadlines and deliver results with flexibility and a hunger to learn. Excels at implementing Information Security Management policies, deploying network devices, finding vulnerabilities, performing risk analysis and monitoring a network. Sponsorship required to work in the US Work Experience Research Assistant- Preliminary Forensic Analysis of Amazon Echo Johns Hopkins University - Baltimore, MD February 2017 to Present ? Obtained the firmware information, analyzed it, and determined potential vulnerabilities. ? Reverse engineered APK s and binaries stored in .bin file. ? Changed Alexa s voice easily by changing the Echo s mp3 files in /local/share/earcon directory. ? Documented and submitted this paper to get published in IEEE Conference, UK. IT Security Analyst PC Solutions - New Delhi, IL July 2015 to May 2016 ? Key Member of the VAPT team, tasked with identifying vulnerabilities in the internal applications. ? Spearheaded a campaign to implement Cisco s Cloud Web Security and further establishing the policies. ? Established TACACS+ protocol to support authentication, authorization and accounting services for network device access control. ? Liaised with a team to implement HP Archsight SIEM in the company. Associate Consultant QGS PVT Ltd - New Delhi, Delhi February 2013 to June 2014 ? Evaluated the potential effects to critical business operations with the help of BIA. ? Implemented Security Controls in accordance with ISO 27001:2013 and developed the SoA. ? Collaborated with teams to prepare the Information Asset list. Education MS in Security Informatics Johns Hopkins University December 2017 B. Tech in Information Technology NorthCap University July 2015 Skills C (4 years), C++ (4 years), Python (2 years), Javascript (3 years), Linux (3 years), Cloud Computing, Penetration Testing (2 years) Links https://www.linkedin.com/in/prerit11 Certifications/Licenses CEH September 2018 ISO 27001 Lead Auditor July 2019 Additional Information PROJECTS 1. Threat Modeling of an open source browser extension- DTA: ?Identified the valuable assets that the system must protect and created

the architecture of the application. ? Decomposed the application to create the security profile, identified and rated all the threats associated with it. 2. Reverse Engineering of an open source application- BitchX: ? Compiled the binary, dumped the headers, identified the shared library dependencies, listed the symbols from object files, dumped the vm tables, and statistically analyzed the binary. 3. Implemented a client for the JMessage encrypted instant messaging service ? Developed a client that uses 3 cryptographic primitives, namely RSA, DSA and AES encryption. ? Implemented key lookup, key fingerprints, read receipts and obtained undelivered messages from the server. 4. Implemented a buffer overflow and arbitrary write exploits- DevToDo: ? Used a format string vulnerability to implement an Information leak exploit. ? Implemented a buffer overflow by copying into a buffer without checking bounds. 5. Implemented a stack smashing exploit that uses shellcode injection and arc-injection- Eatmemory: ? Altered the address of the return pointer of the vulnerable function and pointed it to the injected shellcode. ? Implemented return-to-libc by passing the address of the env variable as the argument to the system call. 6. Attacked the messaging client by replaying and modifying (decrypt) messages sent between two clients: ? Implemented a program that intercepts and decrypts the messages sent between two clients. 7. Created a twitter-bot detection system using various API s and Zerofox cloud platform: ? Built a utility to detect bots on Twitter, with the help of Tweepy, Google s Safe Browsing API, Open Source Truth Project and Zerofox Cloud Platform. ? Used skew rate, retweet count, content of the tweet, Geo Location to differentiate between bots and humans.

Name: Joshua Wu

Email: parsonsbrooke@example.net

Phone: (518)714-7810x368