Weiheng Bai

Address : 2001 Fitzwarren Place. **Tel:** 443-224-8954. **City:** Baltimore, Maryland **E-mail:** wbai3@jhu.edu

Education

Johns Hopkins University, Baltimore, America

Master of Science in Information Security(GPA: 3.93) Aug.2019-

Beihang University, Beijing, China **(GPA: 3.3 Rank: 1/7)**

Bachelor of Mathematics Sep.2015-Jun.2019

Skills & Learning

- **Programming Languages: Python, Javascript, Matlab**
- **Tools: Kali, Linux, WireShark, VScode, MySQL, Django, MetaSploit, VMware, R Studio, Ghidra， Burp suite, XAMPP**

Security Experiences

University of Austin Capture the Flag Competition (Rank top 100 of 1000 teams)

Project Experiences

Develop and implement protocol stack similar to OSI model Aug. -Dec.2019

Keywords: TCP/IP, TLS protocol, C/S, OSI model, Python, Handshake, DH, AESGCM, X.509, Certification Chain, packet

- Implemented the mechanism of the **TCP/IP** and **TLS** protocols based on self-build environment similarly to OSI model.
- Implemented a client/server **interactive game** by python and used it as the application layer.
- Implemented **three-way handshake** including **Nonce,** which can ensure **Integrity,** to realize TCP protocol initialization.
- Used **asyncio** to determine the timeout and connection lost in TCP packet transform and used **packet slicing** and **hash** function to slice the application layer data into small slicing and encapsulated them into signal packet to realize TCP packet transform to ensure **Availability**.
- To implement TLS layer, I used **Diffie–Hellman algorithm** for key exchange between client and server and used **AESGCM** for data encryption and user authentication to ensure the **confidentiality**. Utilized **X.509** for signature and implemented a **Certification Chain** from professor to team member for security in order to avoid tampering with the contents of a certificate by man-in-the-middle attack.

Hacking the Parrot Bebop 1 Drone Jan.- March.2020

Keywords: penetration test, Netdiscover, nmap, Wireshark, Nessus, DoS, ARP, Python

- Led other 5 members to do **penetration test** on a drone named Bebop Parrot and find three zero-day vulnerabilities
- Used **NetDiscover** to find the certain host under the given network and used **nmap** to find the opening ports and use **Nessus**.
- Set up cloned controllers to test the maximum number of connections that exist. Got the AR Discovery Process in MDNS by **Wireshark.**
- Implemented a **python** script which sends numerous costumed **JSON** data initializing the connection to launch **flood attack.**
- Launched **DoS ARP attack** based on python against AR Discovery Process and break the connection between drone and its controller.

Used Metasploit shell reverse TCP with self-build payload to implement shell reverse attack Mar.2017-Jul.2016

Keywords: Assembly coding, C, Metasploit, payload, Kali (project: https://drive.google.com/file/d/10VYobZUsr8-sDDtX1EVbetVY_wZ3Kllu/view?usp=sharing)

- Used **assembly coding** to spawn a shell in Linux 64 and converted assembly code into shell code by **NASM** and **Objdump**.
- Implemented a **C** code to test this shellcode based on function pointer and used **GCC** to compile the C file into executable file to get shell.
- Modified the file named shell_reverse_tcp.rb file in **Kali Linux** by used self-build shellcode and used **msfvenof** to generate new **payload**.
- Opened **Metasploit** and used **Handler** for listening on the attack machine to get the reverse shell after the target machine which is a ubuntu VM downloaded this payload and executed it.

Course Security Analytics. Aug – Dec. 2019

- Finished the paper named Yelp Fake Review Detection Based on Deep Learning.
- Software Compared the results based on SVM, Bi-LSTM, Bi-LSTM embedded in BERT.
- Led the team of 4 to fulfill tasks and mainly responsible for the part of vectorization and Bi-LSTM and paper writing.

Intern, University of Illinois at Urbana-Champaign Summer,.2017

Intern, Institute of Software, Chinese Academy of Sciences. Aug.- Dec.2017

- Grasped skill to apply Python by learning A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers
- Learned a new method for the prevention of side channel attack and did simulation after reading the conference paper: CacheD: Identifying Cache- Based Timing Channels in Production Software
- Grasped taint analysis by learning the paper All You Ever Wanted to Know About Dynamic Taint Analysis and Forward Symbolic Execution

The Interpolation Theory and its Application Nov 2017 – Jun 2018

- Introduced almost all the basic interpolation theories in Banach Space, such as M.Riesz interpolation theory, Marcinkiewicz interpolation theory and so forth.
- Summarized the application of interpolation theories in theoretical and practical.

Identity Authentication of Satellite Network Based on Blockchain. Aug.- Dec.2017

- Led other 4 members to study on blockchain, and held group discussions about three times a week
- Took charge of the study on “Composition of Blockchain” and “Identity Authentication of Blockchain”
- Responsible for the thesis writing

MCM/ICM, Analysis of Terminal Inspection Flow Based on Queuing Theory and Petri Net Dec.2017

- Took charge of theoretical analysis, modeling, Matlab realization, and thesis writing
- Model one: proved the number of passengers arriving per unit time subject to
- Model two: introduced the concept of queuing theory and the main parameters of data, put forward the concept of optimization, and built a queuing model.

Patent

Weiheng Bai, A Kind of Computer Wire Clamp's Structure, Patent Number: 201720362458.0 April 09, 2017

Award

- Outstanding Graduate (8/120);
- First-class Scholarship
- China Excellent Student Leader (Academic year of 2017-2018)
- Student Committee President (2016, 2017, 2018)