Rick Console | OSCP | CRTO

Cherry Hill, NJ 08003
856-470-6681
rick@rickconsole.com
rickconsole.com
github.com/RickConsole

EDUCATION

Drexel University, Philadelphia, PA — *Bachelor of Science in Computing and Security Technology*

Graduating June 2024

- Concentration in Computer Security
- Cumulative GPA: 3.84 - Dean's List

EXPERIENCE

Security Risk Advisors, Philadelphia, PA — *Penetration Tester*

September 2020 - Present

- Performed internal and external penetration tests to assess the security of various companies
- Lead purple team assessments by executing various test cases to simulate nation state threat actors
- Discovered and reported on various vulnerabilities in penetration tests

Unofficial College Course Professor, Drexel University

Summer 2022

- While taking IT Security II, I was asked to teach half of the course's classes and to design the final exam
- Developed a vulnerable Linux server from scratch to simulate a penetration test
- Worked with the director of IT to get instances of my machine on Drexel's vSphere servers
- Held weekly lectures and labs to walk my classmates through the penetration testing process
- My machine and labs were added to the official course curriculum

RedPhish, Cherry Hill, NJ — *Founder/Owner*

June 2017 - Present

- Created Security Awareness campaigns for multiple companies
- Launched phishing simulations to test for social engineering risks
- Provided weekly reports of security risks and phishing statistics to business owners

SKILLS

- Penetration Testing + Purple Teams
- Linux systems and CLI
- Tools: Cobalt Strike, Burp Suite, Metasploit, Bloodhound, Nmap, Hashcat, PowerView, impacket, etc.
- Operating Systems: Arch and Debian systems, Kali

PROGRAMMING LANGUAGES

- Go, Python, Bash
- HTML, CSS, JS

AWARDS

- 1st place HacktheBox x Uni CTF International
- 1st place National CPTC qualifiers
- 1st place Comcast Cloud Native Revolution CTF
- A.J. Drexel Scholarship

ACTIVITIES

- Drexel Cyberdragons 2019-Present
- Black Hat USA 2021
- Hackthebox (Pro Hacker Rank)
- National CCDC
- National CPTC

EXPERIENCE, COURSES & CERTIFICATIONS

Offensive Security Certified Professional (OSCP), Offensive Security

October 2022

- Compromised Linux and Windows machines in several lab environments
- Built a custom buffer overflow exploit script to obtain code execution on a windows target
- Pivoted through machines by creating SOCKS proxies to access different subnets
- Completed and passed the 24 hour exam by compromising 6 hosts and writing a full report

Certified Red Team Operator, Zero-Point Security

April 2023

- Simulated Adversaries such as nation-state threat actors and APT groups
- Compromised entire Active Directory domains from a command and control server
- Performed privilege escalation attacks and implemented persistence mechanisms
- Completed a 48 hour practical exam

Cybersecurity Club Leader, Drexel University

Spring 2020-Present

- Led meetings twice per week lecturing on various cybersecurity concepts
- Designed and hosted several Capture the Flag competitions and vulnerable machines
- Competed in international penetration testing competitions
- Managed a custom made lab environment in the cloud

Collegiate Cyber Defense Competitor, Online — *Linux Security*

March 2020, 2021, 2022

- Implemented audit rules to monitor applications and sensitive files
- Created hidden backups of application data
- Identified and blacklisted malicious IP addresses
- Restricted access on Debian and CentOS machines
- Removed backdoors and malicious processes on compromised systems

Advanced Application of Adversarial AI for Scenario Based Hacking, Black Hat USA

August 2021

- Developed methods to bypass authentication systems and evade spam filters
- Learned how to inject fake training data into an AI's API to change its behavior
- Studied the fundamentals of Artificial Intelligence and set up data ingestion processes

Introduction to Hardware Hacking and Reverse-Engineering, Advanced Security Training

July 2021

- Analyzed IoT hardware and identified crucial components

- Developed a custom version of UART to communicate with embedded systems

- Dumped the firmware of an IoT device over its Serial Peripheral Interface, then flashed a modified version of the firmware to the device

- Experimented with CPU debug protocols such as JTAG and SWD

Offensive IoT Exploitation, Attify

June 2021

- Unpacked and analyzed various IoT firmware files and discovered vulnerabilities and credentials

- Emulated IoT firmware for analysis without having the physical device tampered with

- Backdoored firmware files and sent them to the IoT device as a malicious update

- Performed Bluetooth Low Energy (BLE) attacks on various IoT devices

- Decompiled Android applications for IoT devices to determine its functionality