**Joseph Clay**

(828) 412-7800 | Huntersville, NC

[clayjoseph1994@gmail.com](mailto:clayjoseph1994@gmail.com) | [linkedin.com/in/clayjoseph1994](https://www.linkedin.com/in/clayjoseph1994/) | [github.com/skollr34p3r](https://github.com/clayjoseph1994) | [clayjoseph1994.com](https://clayjoseph1994.com/)

**Penetration Tester**

Skilled **Penetration Tester** respected for assessing physical, technical, and administrative controls to improve the security posture of an organization. Capable of conducting Internal and External Infrastructure tests, Web Application tests, Wireless Tests, and tests involving Social Engineering and Physical testing. Effectively communicates findings and recommendations to other technical professionals as well as laymen. Known as a democratic, assertive leader who cultivates high-performing teams to optimize security technologies and maintain policies and standards. Certified in PNPT, eJPT, CompTIA Security Plus, and Cybersecurity. Out-of-the-box thinker committed to delivering continuous improvement through rigorous research and testing procedures to identify and exploit vulnerabilities and to provide recommendations to mitigate the risk that these vulnerabilities pose. Constantly sharpening skills and working to stay up to date with the newest breaches and vulnerabilities discovered in order to stay abreast the ever-evolving technological landscape.

**CAREER HIGHLIGHTS**

* Reviewed, troubleshot, and made edits to a scenario to address 11 customer complaints/bugs in 5 days.
* Ranked 5th in the B-Sides Charlotte SecureCodeWarrior CTF Challenge.
* Passed the eJPT exam in under 7 hours with a 90%.
* Completed the Cybersecurity Bootcamp with a 4.0 GPA leading to a recommendation for a TA position at UNC.
* Wrote a walkthrough for a box named NullByte from VulnHub.

**Skills & Expertise**

|  |  |  |
| --- | --- | --- |
| * Penetration Testing | * Incident Response | * User Training |
| * Red Team Exercises | * Patching | * Endpoint Attack Techniques |
| * Application Design | * Vulnerability Remediation | * Network Security Infrastructure |
| * Threat Detection | * Secure Development Training | * Cloud Services |

**Professional Experience**

**FLEXENTIAL PROFESSIONAL SERVICES | REMOTE – BOULDER, CO | 2021 TO PRESENT**

**Penetration Tester**

Providing penetration testing and consulting services to over a hundred clients to help them maintain security compliant status and keep their data safe.

* Assumed a great deal of responsibility on the penetration testing team as the lead of the team left shortly after I was hired.
* Claimed ownership of the internal infrastructure testing machine procedure and redesigned the process to be more reliable and efficient.
* Conducted internal and external infrastructure, web application, wireless, and social engineering penetration tests for a variety of clients with strict deadlines.
* Authored, co-authored, and modified scripts in bash and Python to automate testing procedures in order to save time and allow multi-tasking during engagements.

**CIRCADENCE CORPORATION | REMOTE - BOULDER, CO | 2020 - 2021**

**Information Security Engineer**

Provide operational cybersecurity expertise and work with developers to create immersive, realistic cyber training environments integrated into a gamified platform.

* Delivered operational cybersecurity expertise by cultivating Python and YAML skills creating scenarios for Project Ares, a gamified cybersecurity training platform.
* Reviewed, troubleshot, and made edits to a scenario to address 11 customer complaints/bugs in 5 days.
* Created immersive, realistic cyber training environments by navigating a complex infrastructure hosted in Azure and getting acquainted with a plethora of technical tools.
* Utilized SaltStack to make run-time configuration changes to the services and states of VMs used by scenarios.

**2U | REMOTE - CHARLOTTE, NC | 2020 TO PRESENT**

**Cybersecurity Bootcamp Senior Tutor**

Promoted to Senior tutor for consistently helping students achieve positive outcomes during high volume sessions.

* Contributed to a substantial increase in student retention and pass rate by preparing students to succeed in Cybersecurity and Security Plus certification.
* Improved workflow efficiency by creating and utilizing Python and Google API scripts to assist in online job tasks.
* Provided subject-matter guidance to colleagues during the training planning phase and implementation.

**GLOBAL LINKING SOLUTIONS | CHARLOTTE, NC | 2020**

**Network Operations Center Technician**

Monitored and managed network and service delivery to facilitate the identification, analysis, and resolution of service impacting issues.

* Reduced the escalation frequency to improve service satisfaction by using CLI on Cisco Systems to remediate tickets in queue within established SLAs.
* Isolated and identified root cause of faults by monitoring networks and troubleshooting connectivity issues with carriers, technicians, and sites.
* Restored services to customers more quickly by mapping out network topologies, configured subnets, and learned about various networking devices.
* Fostered relationships with vendors including Cisco, Fortinet, Adtran, Juniper, and Palo Alto.

**Projects**

**Cyber Ranges | HacktheBox, TryHackMe, VulnHub, Project Ares, CTFs | 2019 to Present**

* Placed 5th in the SecureCodeWarrior B-Sides Charlotte 2020 CTF Competition.
* Joined HacktheBox by hacking the website to complete five user and five system owns.
* Set up my lab with Kali Linux and various VulnHub boxes to practice Pentesting skills.
* Wrote a walkthrough for a box named NullByte from VulnHub.

**Udemy Courses | Web Developer Bootcamp, Python Bootcamp, Practical Ethical Hacking | 2020 to Present**

* Completed approximately 50% of the Python Bootcamp created by Colt Steele.
* Built some of my simple tools through hands-on experience with a lot of common tools.
* Finished the Practical Ethical Hacking course provided by TCM Security, teaching the core concepts of penetration testing methodology, as well as Active Directory penetration testing and how to prevent these attacks

**INE eJPT Course for Junior Penetration Tester Certification | 2021**

* Developed essential penetration testing skills and methodologies, network and WebApp vulnerability assessment, exploitation with Metasploit, OSINT, information gathering and recon, TCP/IP knowledge, etc.
* Passed the exam in less than 7 hours with a score of 90%.

**Cybersecurity Bootcamp Program (UNC Charlotte) | 2019 to 2020**

* Built and configured a virtual network hosting an Ansible Docker container of DVWA, monitored using an ELK stack server set up with FileBeat and MetricBeat to log system and application information.
* Compromised a site called Shadow Bank by enumerating the website and injecting payloads/exploiting SQL vulnerabilities to route money to your account from another account.

**Education & Certifications**

**Cybersecurity Bootcamp Program (GPA: 4.0)** | University of North Carolina - Charlotte, Charlotte, NC: 2020

**Bachelor of Arts in Psychology (GPA: 3.6)** | University of North Carolina - Asheville, Asheville NC: 2017

|  |  |
| --- | --- |
| * **Practical Network Penetration Tester (PNPT)** | TCM Security, 2021 * **Junior Penetration Tester (eJPT)** | eLearnSecurity, 2021 * **Security+ ce Certification** | CompTIA, 2021 | * **Cybersecurity Certificate** | UNC Charlotte, 2020 * **Javascript Fundamentals** | SoloLearn, 2019 * **Learn HTML5 and CSS3 to Build a Website from Scratch** | BitDegree, 2019 |

**Technical Skills**

**Penetration Testing**: Kali Linux, Nessus, OpenVAS, Metasploit, NMAP, Hashcat, SQLMap, Nikto, Dirbuster, BurpSuite, John the Ripper, MSFVenom, Merterpreter, netcat

**Programming & Scripting**: Python, bash, zsh, YAML, Ansible, PowerShell, Azure DevOps, Git, VSCode, and Sublime Text

**Networking**: Packet analysis, Wireshark, router and switch configuration, protocols, SSH, firewalls, iptables, proxies, SIEM, DNS, DHCP, VPN, and VLAN

**Systems**: Windows and Linux Administration/Hardening, Docker, VMWare, VirtualBox, and System Configuration, nxlog, auditd, and Sysmon