JOSEPH CLAY

(828) 412-7800 | Huntersville, NC
clayjoseph1994@gmail.com | linkedin.com/in/clayjoseph1994 | github.com/skollr34p3r | 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 Network Tests, Physical penetration tests, and Social Engineering. 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 risks. Constantly sharpening skills and working to stay up to date with the newest breaches and vulnerabilities discovered to stay relevant in an ever-evolving technological landscape.

CAREER HIGHLIGHTS

- Claimed the lead role for a full internal penetration test for a client with over eight thousand hosts in the internal network, leading all calls with the client, writing the entire report, and delivering all materials on time.
- Began volunteering to mentor individuals seeking to launch careers in Cybersecurity.
- Passed the Practical Network Penetration Tester (PNPT) exam over the weekend while working full-time.
- Passed the eJPT exam in under seven hours with a 90% score.
- Ranked fiftth in the B-Sides Charlotte SecureCodeWarrior CTF Challenge.
- Reviewed, troubleshot, and made edits to a scenario to resolve eleven customer-reported bugs in five days.
- Completed a Cybersecurity Bootcamp with a 4.0 GPA leading to a recommendation for TA and tutor positions.

SKILLS & EXPERTISE

- Penetration Testing
- Red Team Exercises
- Cloud Infrastructure
- Incident Response
- Patching
- Vulnerability Remediation
- User Training
- Endpoint Attack Techniques
- Network Security Infrastructure

PROFESSIONAL EXPERIENCE

FLEXENTIAL PROFESSIONAL SERVICES | REMOTE – BOULDER, CO | 2021 - PRESENT

Penetration Tester

Providing penetration testing and consulting services to over a hundred clients to help them maintain security compliant status, secure data, assess technical controls, and make expert recommendations for vulnerability mitigation.

- Assuming an increased load in responsibility on the penetration testing team when the lead of the team left, requiring more initiative and tasks outside what this role initially required.
- Conducting internal and external infrastructure, web application, wireless, and social engineering penetration tests for a variety of clients with strict deadlines.
- Functioning as a subject matter expert in a consulting environment, requiring presentations and recommendations of vulnerability mitigation strategies to both technical and non-technical leaders in client organizations.
- Communicating professionally with clients in verbal and electronic form, and during virtual meetings.
- Working with a team consisting of other penetration testers, supervisors, and project managers to ensure prioritization of client satisfaction.
- Navigating tight deadlines for penetration testing engagements, scheduled meetings, training, and writing, reviewing, and delivering reports.
- Claiming ownership of the internal infrastructure testing machine procedure and redesigning the process to be more reliable and efficient utilizing an OpenVPN server in AWS to connect the team to devices at client sites.
- Authoring, co-authoring, and modifying scripts in bash and Python to automate testing procedures to save time and allow multi-tasking during engagements thereby increasing the efficiency of work being done.
- Reconstructing a nessus2docx tool used to convert Nessus files into a more easily modifiable docx format used for validating Nessus findings manually during penetration tests.

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

Information Security Engineer

Provided operational cybersecurity expertise and worked with developers to create immersive, realistic cyber training environments integrated into a gamified platform called Project Ares.

- Delivered operational cybersecurity expertise by cultivating Python and YAML skills creating scenarios for Project Ares, a gamified cybersecurity training platform.
- Created immersive, realistic cyber training environments by navigating a complex infrastructure hosted in Microsoft Azure and becoming familiar with cloud infrastructure.
- Reviewed, troubleshot, and made edits to a scenario to resolve eleven customer-reported bugs in five days.
- Utilized SaltStack to make run-time configuration changes to the services and states of VMs used by scenarios.
- Refined the functionality of the Project Ares platform by playing through and improving scenarios involving webapp penetration testing using tools like Nikto, BurpSuite, Dirb, SQLMap, and Hydra.

2U | REMOTE - CHARLOTTE, NC | 2020 - 2021

Cybersecurity Bootcamp Senior Tutor

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

- Contributed to a substantial increase in student retention and a ninety percent pass rate by preparing students to succeed in Cybersecurity and achieve Security Plus certification.
- Improved workflow efficiency by creating and utilizing Python and Google API scripts to assist in online job tasks.
- Quickly earned a reputation for expertise in degree-level standards and practices across assigned portfolios.

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 the Command-Line Interface on Cisco Systems to remediate tickets in queue within established Service-Level Agreement timeframes.
- Isolated and identified root cause of faults by monitoring networks and troubleshooting connectivity issues with carriers, technicians, and client sites.
- Restored services to customers quickly by mapping out network topologies, configuring subnets, and learning about various networking devices.

TRAINING & PROJECTS

Offensive Security Training | Dec 2021 - Present

- Received access to the PEN-200 course and labs to train for the Offensive Security Certified Professional (OSCP) exam.
- Began studying for the OSCP certification exam.
- Successfully gained user and system level privileges on three Proving Grounds Practice machines.

PortSwigger Training | Dec 2021 - Present

- Registered for the Web Security Academy Learning Path offered by PortSwigger, the makers of BurpSuite.
- Purchased a voucher for the BurpSuite Certification exam provided by PortSwigger.

TCM Academy/Practical Network Penetration Tester Training | Oct 2021

- Completed the Practical Ethical Hacking course, teaching the core concepts of penetration testing methodology, as well as Active Directory penetration testing and how to prevent these attacks.
- Completed the External Pentest Playbook course, teaching fundamental concepts related to external penetration testing methodology and practical application of these skills.
- Completed the Open-Source Intelligence Fundamentals course, teaching the core concepts of performing reconnaissance and gathering information about targets from publicly available sources.
- Passed the Practical Network Penetration Tester (PNPT) certification, which consisted of applying the concepts of external penetration testing, exploitation, pivoting into an internal network, gaining a foothold into an Active Directory domain, moving laterally through the domain, fully compromising the Domain Controller, establishing persistence in the network, writing a professional penetration testing report including all relevant findings and recommendations for mitigation, and presenting the report to a well-respected, professional penetration tester.

 (828) 412-7800 | clayjoseph1994@gmail.com

Cyber Ranges | HacktheBox, TryHackMe, VulnHub, CTFs | 2019 - 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 a lab with Kali Linux and various VulnHub boxes to practice Penetration Testing skills.
- Wrote a walkthrough for a box named NullByte from VulnHub.

INE eJPT Course for Junior Penetration Tester Certification | May 2021

- Developed essential penetration testing skills and methodologies, network and WebApp vulnerability assessment skills, skills necessary for exploitation with Metasploit, Open-Source Intelligence knowledge, information gathering and reconnaissance skills, TCP/IP knowledge, and many other applicable skills related to penetration testing.
- Passed the exam in less than 7 hours with a 90% score.

Cybersecurity Bootcamp Program (UNC Charlotte) | Sep 2019 - Feb 2020

- Gained invaluable network, system, penetration testing, and other IT and Cybersecurity skills used to successfully pass the ComTIA Security Plus exam.
- Built and configured a virtual network hosting an Ansible Docker container of Damn Vulnerable Web Application (DVWA), monitored using an ELK (Elasticsearch, Logstash, and Kibana) stack server, set up with FileBeat and MetricBeat to log system and application information.
- Attended a CTF event where everyone was encouraged to compromise an intentionally vulnerable, fake web site called Shadow Bank, done by enumerating the site, exploiting SQL vulnerabilities, and injecting payloads to imitate the concept of routing funds from one bank account to another.

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, YAML, Ansible, PowerShell, Azure DevOps, Git, and VSCode
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, nxlog, auditd, and Sysmon