JOSEPH CLAY

(828) 412-7800
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 both large and small organizations. Creative thinker committed to delivering continuous improvement through rigorous research and testing procedures to effectively assess vulnerabilities and perform exploits in a safe and repeatable manner. Communicates findings in clear, concise language, and offers actionable recommendations to assist clients in managing risk.

Known as a democratic, assertive leader who cultivates high-performing teams and optimizes security technologies while maintaining policies and standards. Volunteers to train individuals new to the industry and those trying to obtain entry-level cybersecurity positions. Constantly sharpening skills to remain up to date with the latest breaches and vulnerabilities discovered to stay relevant in the ever-evolving information security landscape.

PROFESSIONAL EXPERIENCE

FLEXENTIAL PROFESSIONAL SERVICES | 2021 - PRESENT
Penetration Tester

Providing penetration testing and consulting services for over one hundred clients to help them maintain compliance, manage risk, and enhance the confidentiality, integrity, and availability of resources.

- Assuming an increased responsibility on the penetration testing team of three members since joining.
- Responsible for the internal network testing “dropbox” machines; redesigning connectivity for reliability and efficiency utilizing an Amazon Web Services (AWS) instance hosting an OpenVPN server for dropbox connectivity at remote client sites.
- Conducting internal and external infrastructure, web application, wireless penetration tests, and social engineering engagements for a variety of clients within strict deadlines.
- Delivering professional presentations and expert recommendations of vulnerability mitigation strategies to both technical and non-technical audiences in client organizations.
- Contributing to a team of three penetration testers and a project manager to ensure the highest level of professionalism, effectively managing time, and ensuring the highest client satisfaction.
- Navigating tight deadlines, holding/leading client and internal meetings, and training, while writing, reviewing, and delivering reports.
- Developing Bash and Python scripts [as well as maintaining various internal tools] that automate testing procedures which save time, enhance consistency, and increase testing efficiency.

CIRCADENCE CORPORATION | 2020 - 2021
Information Security Engineer

Provided operational cybersecurity expertise and worked with developers to create immersive, gamified, and realistic cyber training environments marketed as Project Ares.

- Created, developed, and refined Project Ares scenarios by simulating real-world attacks used by Advanced Persistent Threats (APTs) to train cybersecurity professionals to recognize indicators of compromise, resulting in the highest quality and most realistic training environment.
- Used Python, YAML, and SaltStack to create and manage training scenarios in complex Microsoft Azure cloud-based environments.
- Routinely resolved bug reports, at times over ten per week (approximately 200% over average).

2U | 2020 - 2021
Cybersecurity Bootcamp Tutor

Assisted cybersecurity bootcamp students struggling with technical concepts in areas such as Linux fundamentals,

Windows fundamentals, networking, Python and Bash scripting, penetration testing, digital forensics, and preparing for the CompTIA Security+ exam.

- Substantially increased student retention while supporting a 90% pass rate in the cybersecurity bootcamp program.
- Achieved promotion to senior tutor based on session volume and glowing student reviews.
- Developed Python and Google API scripts to increase efficiency in online job tasks.

GLOBAL LINKING SOLUTIONS | 2020
Network Operations Center Technician

Monitored and managed network and service delivery to identify, analyze, and resolve service impacting issues.

- Reduced escalations by using the command-line interface on enterprise-grade Cisco switches and routers to remediate tickets while meeting or exceeding service-level agreement requirements.
- Identified root cause of faults by monitoring networks and troubleshooting connectivity issues with carriers, technicians, and client sites.
- Mapped out network topologies and performed moderate device configuration.

EDUCATION, CERTIFICATIONS, & TRAINING

CYBERSECURITY BOOTCAMP PROGRAM (GPA: 4.0) | UNIVERSITY OF NORTH CAROLINA - CHARLOTTE, 2020

- Gained valuable skills to earn the CompTIA Security+ certification.
- Architect a virtual network hosting an Ansible Docker container running Damn Vulnerable Web Application (DVWA), monitored using an ELK (Elasticsearch, Logstash, and Kibana) stack server, along with Filebeat and Metricbeat to process system and application logs.
- Received multiple recommendations from the lead instructor and teaching assistants leading to both teaching assistant and tutor positions within the bootcamp.
- Completed a CTF competition to compromise a vulnerable banking application to surreptitiously move funds from one account to another.

BACHELOR OF ART IN PSYCHOLOGY (GPA: 3.6) | UNIVERSITY OF NORTH CAROLINA - ASHEVILLE, 2017

Practical Network Penetration Tester (PNPT) certification | TCM Security, 2021

Junior Penetration Tester (eJPT) certification | eLearnSecurity, 2021

Security+ certification | CompTIA, 2021

Pursuing Offensive Security Certified Professional (OSCP) | Dec 2021 - Present

Pursuing Burp Suite certification | Dec 2021 - Present

TCM Academy: Practical Network Penetration Tester (PNPT) training | Oct 2021

- Practical Ethical Hacking
- External Pentest Playbook
- Open-Source Intelligence Fundamentals

Cyber Ranges: Hack The Box, TryHackMe, VulnHub, Capture the Flag (CTF) competitions | 2019 - Present

- Placed 5th in the SecureCodeWarrior BSides Charlotte 2020 CTF competition.
- Participating in various cyber ranges such as HackTheBox, TryHackMe, and VulnHub to sharpen exploitation and penetration testing skills.
- Built a home lab with Kali Linux, various VulnHub VMs, and an Active Directory network including Windows Server 2019 and two Windows 10 workstations to practice Linux and Windows system exploitation, Active Directory compromise, password cracking, and other penetration testing skills.

- Wrote a walkthrough for a VulnHub VM named “NullByte” available at the following link: https://docs.google.com/document/d/1kLV9AQw5yTLLbm4Z7KfrGO7rpgjGkK8VoUP2LoeAZbg/

RELEVANT SKILLS

Penetration Testing: Kali Linux, Nessus, OpenVAS, Metasploit, Merterpreter, MSFVenom, Nmap, Hashcat, SQLMap, Nikto, Dirbuster, Burp Suite, John the Ripper, netcat, Bloodhound, Aircrack-ng, eaphammer, Pyrit, Impacket’s toolkit, CrackMapExec, Kerberoasting, NTLMv2 hash capture/relay, password spraying, and credential stuffing

Programming & Scripting: Python, Bash, YAML, Ansible, PowerShell, Azure DevOps, Git, and VSCode

Networking: Wireshark and general packet analysis, router and switch configuration, SSH, Uncomplicated Firewall (UFW), iptables, FoxyProxy, Splunk, DNS, DHCP, and OpenVPN

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