Rob Pratt

Phone | Location

rob.pratt@tutanota.com | https://rpriven.github.io/ | https://github.com/rpriven

Passionate Offensive Cyber Operator with a strong interest in Penetration Testing, Red Teaming, Ethical Hacking, Vulnerability Analysis and Network Security. Hard-working, energetic, personable, and technical-minded individual with exceptional customer service, communication skills, and ability to multitask. Dedicated to continual training and certification courses as well as home lab experience.

Experience in scripting languages including Python and Bash, and Security tool-kits such as Kali Linux, Metasploit, and Burp Suite. Excellent task management and ability to handle multiple projects.

Certifications

TCM Security	**PNPT**	Practical Network Penetration Tester (testing January 2023)
Cyber Ranges	**CEPP**	Certified Exploitation & Post-Exploitation Professional
ZeroPoint Security	**CRTO**	Certified Red Team Operator (in progress, estimated March 2023)
Offensive Security	**OSCP**	Offensive Security Certified Professional (estimated Spring 2023)
Hack The Box	**CPTS**	Certified Penetration Testing Specialist (estimated February 2023)
APIsec	**ACE**	API-Security API Certified Expert (upon test release)
Hack The Box	**CBBH**	Certified Bug Bounty Hunter (estimated Spring 2023)
PortSwigger	**BSCP**	Burp Suite Certified Practitioner (estimated early 2023)
CompTIA	**Security+**	(testing early 2023)
freeCodeCamp	**Responsive Web Design**	

Penetration Testing Experience

Active Directory Hacking Lab

- Setup and configured an Active Directory home lab with a Domain Controller and several user machines to practice initial attacks such as LLMNR poisoning, SMB Relay and IPv6 attacks.
- Used various TTPs such as Pass the Pass/Hash, Token Impersonation, Kerberoasting and Golden Ticket attacks and gained shell on Kerberos and took control of the entire Domain.

Penetration Testing Lab

- Created and maintained a virtual Hacking lab using Kali Linux in order to conduct vulnerability scans and practice various types of exploits and attacks on Systems, Networks, and Web Apps.
- Proficient in using Metasploit as well as a range of other Pentesting tools and frameworks for recon, scanning, exploitation, post-exploitation, analysis and exploit development as needed.
- Skilled in network mapping with tools such as Nmap, with the ability to identify open ports, determine which services are running and vulnerable, and identify effective points of entry.
- Automated tasks with Bash/Python in order to scan, document and organize gathered Intel.
- Write detailed Reports with Executive and Technical Summary, description of vulnerabilities, risk, tools used, NIST or OWASP references, evidence and remediation recommendations.
- Constantly research CVEs, exploits, payloads, malware, pivoting and privilege escalation skills.

Bug Bounty / Web Application Testing Lab

- Deployed Docker containers and Web Apps including Juice Shop, DVWA, crAPI and vAPI.
- Tested for OWASP Top 10 Security Vulnerabilities: Authorization, Authentication, Injection, Insecure Design, Security Misconfiguration, Data Exposure, Cryptographic Failures and more.

Security Events & Affiliations

- Active participant in Cyber Ranges, Hack The Box, TryHackMe, PicoCTF, Snyk, VulnHub, etc.
- OSINT researcher interested in Trace Labs crowd-sourced CTF investigation of missing persons.
- Blog: Actively post about Cybersecurity, Privacy and CTF write-ups (website coming soon).

Professional Experience

Bug Bounty Hunter / Security Researcher 2022 – Present

BugCrowd, HackerOne

- Test the security of APIs and Web Applications for a variety of companies using tools including Burp Suite, Postman, Zaproxy, Nuclei, SQLmap, Wfuzz as well as custom-built tools and scripts.
- Search for common bugs, vulnerabilities and exploits in the OWASP Top 10 and CWE Top 25.
- Document and report any findings and recommend techniques for mitigation and prevention.

Manager / Xactimate Expert 2021 – 2022

Company – Location

- Provided hands-on IT Support to local office as well as other locations for 30+ employees.
- Wrote Xactimate estimates, submitted and negotiated with Insurance companies which lead to an increase in company profits by 60% for approximately $750k throughout one season.
- Developed and produced multiple reports and Excel Spreadsheets for bi-weekly meetings in order to track updates, job status, incoming checks, A/R, profit increases, job costing, etc.

Projects

Purple Team Projects

- Configured an Ubuntu VM to capture and monitor network traffic using Snort, forwarding the logs to a Splunk server in the cloud to practice stealth and evasion techniques and detection.
- Developed and implemented security procedures to harden and secure home networks.
- Captured packets with Wireshark to practice analysis, detection, encryption and decryption.

Raspberry Pi Projects

- Experienced in WiFi security and hacking, using AI, bettercap and hashcat. Built a pwnagotchi to gain experience with de-authentication attacks, capturing and cracking secure handshakes.

Miscellaneous Projects

- Skilled system and network administrator managing Linux, Windows and Android devices.
- Configured BashBunny and Rubber Ducky to improve scripting with PowerShell, Bash, Python and Duckyscript to bypass authentication to machines, export passwords or other data, open programs or files to improve understanding and gain hands-on experience in ethical hacking.
- Persistently adapt and improve in order to stay current with the latest tools and technologies.

Education & Additional Training

TCM Academy	Practical Ethical Hacking, External Pentest Playbook Linux Privilege Escalation, Windows Privilege Escalation Open-Source Intelligence (OSINT) Fundamentals
APIsec University	API Penetration Testing
TryHackMe	Red Team Operations, Junior Penetration Tester Intro to Cyber Security, Pre-Security
Dr. Severance (Michigan State University)	Python for Everyone
Splunk	Intro to Splunk
Udemy	Linux System Administration, Bash Scripting