Kevin Watson

contact@watsonkp.com · Phone Number · Street Address · Mailing Address

Experience

TD - Information Security Analyst II (September 2017 - November 2019)

- Completed more than 80 penetration tests of web, API, mobile, thick client, ATM, and mainframe applications and infrastructure focusing on authentication, authorization, session management, and business logic.
- Communicated with stakeholders from business risk management, Agile development, and change management teams to set the scope, threat model, requirements, and timeline for a penetration test.
- Monitored the progress of requirements and timelines for multiple staggered tests during their lead time to maximize my time and minimize development delays. My time was successfully used for testing in more than 90% of cases.
- Created and executed test cases tailored to the application's threat model, covering its scope, and meeting a standard. Manual testing was the focus with scripting used for efficiency and the output of automated tools used for insight. All findings were validated manually before reporting. Testing was logged for accountability.
- Written reporting of testing accommodated multiple audiences (executive, PM, developer, colleagues) using style and vulnerability severity standards. Findings were entered into multiple vulnerability/issue management systems.
- Contributed to the remediation process of findings by demonstrating their impact to application owners, providing detailed technical documentation with proof of concept exploits and verbal clarification to developers, and validating the effectiveness of fixes and mitigations.
- Presented and documented technologies, techniques, and tools for colleagues. Documented the testing process and taught it to new colleagues during their on-boarding. Supported colleagues through testing and technology difficulties.

Community

- Open source projects published at `github.com/watsonkp` using a variety of languages and frameworks. The projects cover automation scripts as well as tools for security testing and life more broadly.
- Technical writing available at `watsonkp.com` where I explore creating a security testing process from scratch and establishing the foundations of iOS application development for a DevOps environment.
- Volunteered for local DEFCON meetups and attended local OWASP meetups.
- Competed as a part of a team in the Symantec 416 live capture the flag event.
- RingZer0 Team Capture the Flag
  - Top 50 of more than 40000 players with 181 challenges completed at ringzer0team.com

Education

- B.Eng. in electrical and biomedical engineering completed at McMaster University
- Immunity: Wide Open to Interpretation / Java Exploitation three day training course at the Infiltrate conference.
- Program Analysis with the Binary Ninja API four day training at the REcon Montreal conference.
- Evil Mainframe Hacking two day training course at the NorthSec conference.
- Bug Hunting Millionaire: Mastering Web Attacks with Full Stack Exploitation two day training course at the CanSecWest conference.

Certification

- Offensive Security Certified Professional (OSCP)
  - Earned based on the quality and completeness of penetration testing reports covering a lab environment, and 24 hours of access to an exam environment where neither vulnerability scanners nor Metasploit were permitted.
- 5000 hours of French study, including ten high school credits where French was the language of communication.

Skills and Familiar Tools

- Security testing web applications and APIs using Burp Suite manually and with custom developed extensions.
- Testing REST APIs using PostMan and SOATest, SOAP web services using SoapUI, and other network services using Scapy.
- Reverse engineering, instrumenting, and debugging iOS, Android, Windows, and Linux applications with Binary Ninja, frida, IDA Pro, gdb, WinDbg, x64dbg, IntelliJ IDEA, and radare2.
- Programming in Python, Swift, JavaScript, C, Java, Go, Ruby, and Clojure.
- Automating tasks with Python, PowerShell, and Bash including data analysis and visualization using Python libraries NumPy, SciPy, and Matplotlib.

- Using and conducting security testing in numerous Linux distributions, many new and old Windows Desktop and Server versions, MacOS, and mainframe z/OS.
- Security testing in Active Directory, ACF2, and Oracle Identity directory environments.
- Queried PostgreSQL, Microsoft SQL Server, MySQL, Oracle, and SQLite databases as well as XML with XPath.
- Created, deployed, used, and debugged Docker containers as well as virtual machines in Hyper-V and VMware ESXi.
- Familiarity with project management tools including Microsoft Project, Confluence, ServiceNow, and Jira.