Kevin Watson

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

Experience

TD - Information Security Specialist (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, development, and change management teams to set and manage the scope, threat model, requirements, and timeline for multiple staggered penetration tests concurrently. My time was successfully used for testing in more than 90% of cases.
- Executed test cases tailored to the application's threat model while meeting standards. Manual testing was the focus with scripting used for efficiency and the output of automated tools used for additional insight. All findings were validated manually before reporting. Testing was logged for accountability.
- Written reporting of test results for multiple audiences while complying with style and vulnerability severity standards. Findings were logged in multiple vulnerability/issue management systems.
- Contributed to the remediation process of findings by justifying 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 infrastructure 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.
- Volunteered for local DEFCON meetups.
- Top 50 of more than 40000 players with more than 180 challenges completed at `ringzer0ctf.com`

Education

- B.Eng. in electrical and biomedical engineering completed at McMaster University
- 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.
- 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.
- Implemented then exploited vulnerabilities in hashing, PRNG, public, and private key cryptography in 41 challenges at `cryptopals.com`.
- 5000 hours of French study, including ten high school credits where French was the language of communication.

Skills and Familiar Tools

- Web, mobile, and API security testing using Burp Suite with custom extensions I wrote.
- 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, Clojure, and assembly.
- iOS and Android mobile application development.
- Automation with Python, PowerShell, and Bash scripting. Data analysis and visualization using NumPy, SciPy, and Matplotlib. Microsoft Word document generation with PowerShell.
- Using and conducting security testing in numerous Linux distributions, 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 and virtual machines in Hyper-V and VMware ESXi.
- Reproducible builds and container images for controlled proof of concept development and testing using Nix.
- Deploying and using CI/CD tools including Jenkins Pipelines and Git.
- Cisco IOS network configuration including IPv4 and IPv6 routing, addressing, subnets, VLANs, NAT, and firewalls.
- Project management tools including Microsoft Project Gantt charts, Confluence, ServiceNow, and Jira.