1100 - Microservices and FaaS for Offensive Security

Saturday at 11:00 in 101 Track

20 minutes | Demo

Ryan Baxendale

There are more cloud service providers offering serverless or Function-as-a-service platforms for quickly deploying and scaling applications without the need for dedicated server instances and the overhead of system administration. This technical talk will cover the basic concepts of microservices and FaaS, and how to use them to scale time consuming offensive security testing tasks. Attacks that were previously considered impractical due to time and resource constraints can now be considered feasible with the availability of cloud services and the never-ending free flow of public IP addresses to avoid attribution and blacklists.

Key takeaways include a guide to scaling your tools and a demonstration on the practical benefits of utilising cloud services in performing undetected port scans, opportunistic attacks against short lived network services, brute-force attacks on services and OTP values, and creating your own whois database, shodan/censys, and searching for the elusive internet accessible IPv6 hosts.

Ryan Baxendale

Ryan Baxendale works as a penetration tester in Singapore where he leads a team of professional hackers. While his day is filled mainly with web and mobile penetration tests, he is more interested developing security tools, discovering IPv6 networks, and mining the internet for targeted low hanging fruit. He has previously spoken at XCon in Bejing on automating network pivoting and pillaging with an Armitage script, and has spoken at OWASP chapter and Null Security group meetings. https://www.linkedin.com/in/ryanbaxendale

@ryancancomputer

https://github.com/ryanbaxendale

#defcon25/by_track/101/saturday

#defcon25/By_Day/_saturday