SEC588.1: Discovery, Recon, and Architecture at Scale

Topics
•Cloud Assessment Methodology
•Infrastructure Cloud Components
•Terms of Service and Demarcation Points
•Domains and Certificates for Enumeration
•Host Discovery with MassCAN and Nmap
•Git Mirroring
•Services and Databases in the Cloud
•Recon and Discovery through Visual Tracking

SEC588.2: Mapping, Authentication, and Cloud Services

•APIs
•Cloud SDKs
•AWS IAM and Privileges
•Building and Using Powerful Wordlists
•Turning Tokens into Access
•Persistence through AWS IAM

SEC588.3: Azure and Windows Services in the Cloud

•Azure Active Directory
•VHD and Volume Shadow Copies
•SAML and Microsoft ADFS
•Windows Containers
•Azure Roles
•Microsoft Graph API
•Office365

SEC588.4: Vulnerabilities in Cloud Native Applications

•Backdooring CI/CD
•Discovering Routes and Hidden Consoles
•SSRF Impacts on Cloud Environments
•Command Line Injections
•SQL Injections
•Peirates for Container Escape
•Injecting Functionless Environments Using LambdaShell

SEC588.5: Exploitation and Red Team in the Cloud

•Red Team and Methodologies
•Heavy and Lite Shells
•Data Smuggling
•Avoiding Detections

SEC588.6: Capstone