Hacking and Securing Cloud Infrastructure 2 Days

This 2-day course cuts through the mystery of Cloud Services (including AWS, Azure and G-Cloud) to uncover the vulnerabilities that lie beneath. We will cover a number of popular services and delve into both what makes them different, and what makes them the same, as compared to hacking and securing a traditional network infrastructure.

Whether you are an Architect, Developer, Pentester, Security or DevOps Engineer, or anyone with a need to understand and manage vulnerabilities in a Cloud environment, understanding relevant hacking techniques, and how to protect yourself from them, is critical. This class covers both the theory a well as a number of modern techniques that may be used to compromise various Cloud services and infrastructure.

Who Should Attend

Cloud Administrators, Developers, Solutions Architects, DevOps Engineers, SOC Analysts, Penetration Testers, Network Engineers, security enthusiasts and anyone who wants to take their skills to next level.

Prior Pen Test experience is not a strict requirement, however, some knowledge of Cloud Services and a familiarity with common command line syntax will be greatly beneficial.

Delegate Requirements

Delegates must bring their own laptop and have admin/root access on it. The laptop must have a virtualization software (virtualbox / VMWare) pre installed. A customized version of Kali Linux (ova format) containing custom tools, scripts and VPN scripts for the class will be provided to the students. The laptop should have at least 4 GB RAM and 20 GB of free disk space dedicated for the VM.

Course Takeaway

Our own customized version of kali linux with inhouse developed scripts and tools to help with hacking auditing and securing Cloud.

Course Outline

INTRODUCTION TO CLOUD COMPUTING
- Introduction to cloud and why cloud security matters
- Comparison with conventional security models
- Shared responsibility model
- Legalities around Cloud Pentesting

ENUMERATION OF CLOUD ENVIRONMENTS
- DNS based enumeration
- OSINT techniques for cloud-based asset

GAINING ENTRY IN CLOUD ENVIRONMENT
- Serverless based attacks (AWS Lambda / Azure & Google functions)
- Web application Attacks
- Exposed Service ports

ATTACKING SPECIFIC CLOUD SERVICES
- Storage Attacks
- Azure AD Attacks
- Containers and Kubernetes Clusters
- IAM Misconfiguration Attacks
- Roles and permissions-based attacks
- Attacking Cognito misconfigurations

POST - EXPLOITATION
- Persistence in Cloud
- Post exploit enumeration
- Snapshot access
- Backdooring the account

AUDITING AND BENCHMARKING OF CLOUD
- Preparing for the audit
- Automated auditing via tools
- Golden Image / Docker image audits
- Relevant Benchmarks for cloud

DEFENSE: IDENTIFICATION OF CLOUD ASSETS
- Inventory Extraction for AWS, Azure and GCP
- Continuous inventory management

DEFENSE: PROTECTION OF CLOUD ASSETS
- Principle of least privilege
- Control Plane and Data Plane Protection
- Financial Protections
- Metadata API Protection
- Cloud specific Protections
- Windows / Linux IaaS auditing

DEFENSE: DETECTION OF SECURITY ISSUES
- Setting up Monitoring and logging of the environment
- Identifying attack patterns from logs
- Monitoring in multi-cloud environment

DEFENSE: RESPONSE TO ATTACKS
- Automated Defense techniques
- Cloud Defense Utilities
- Validation of Setup

NotSoSecure part of claranet cyber security

For more information:

UK: +44 (0)1223 653 193
US: +1 (628) 200-3053/3052
Email: contact@notsosecure.com
Visit: notsosecure.com