Service Definition

Security Testing of Cloud Infrastructure

Azure/AWS as required

External testing of cloud-based environments and infrastructure as unauthenticated and anonymous user to identify flaws and vulnerabilities in configuration.

Testing includes examination of the configuration of accounts to provide clarity about issues including:

- IAM setup
- Security Groups
- Block storage
- VPC configuration
- Encryption and data at rest.

Cloud application security training

Course outline

Introduction

- Vulnerability landscape for IaaS, SaaS and PaaS
- Current threats

Microservices and Serverless

- Monolith to microservice to serverless
- Removing expensive and redundant servers

Securing infrastructure

- Securing access to your cloud environments including effective use of IAM technologies, certificates and secrets
- Understanding least privileged access in cloud environments
    - Effective IAM policies, roles & groups
    - Container security
    - Defence in depth
    - Security by design

Finding vulnerabilities

- Understanding flaws
- Scanning infrastructure
- Automating vulnerability scanning

Logging

- Effective logging techniques
- Retention policies
- How, what and where to log

Tools to help

- Use of technologies to provide oversight to the cloud environment including automating protective actions
- Working with solutions including:
- AWS Config
- Shield
- GuardDuty

Authentication & Authorisation

- Exploration of Authentication and Authorisation methods and technologies
- Use of cloud specific systems including: Cognito, OAUTH2 and JWT
- Preventing lateral movement

Threat modelling serverless applications

- Discovering critical paths
- Reducing reliance and increase resilience
- Building Security Redundancy into your architecture
- Importance of Application layer threat modelling
- Discovering and building data flows

Threat Modelling & Security Testing For Web Applications

Course outline

Introduction

- Why does security matter?
- Examples of successful compromises
- The frequency and severity of attacks
- Cataloguing your data and how it is stored
- Threat Modelling – the basic concepts.

Fundamental Concepts

- The components of a deployed web app
- Considerations specific to internal & external applications
- Cloud deployment as a special security context.

Threat Modelling – an Introduction

- Introducing Threat Modelling Tools
- Creating Data Flow Diagrams using Threat Modelling Tools
- Advantages of performing threat risk modelling
- How threat modelling is used to define and understand application flaws
- The threat categories identified by *STRIDE*
- Categorising the different kinds of attacker
- Driving effective testing through your threat model.

How Attackers Identify Targets & Perform Reconnaissance

- How to proxy HTTP traffic and understand weaknesses using Burp Suite
- Examples of readily accessible flaws in requests.

The OWASP Top 10 (Part I)

A highly practical section, in which concepts are introduced using **demonstration** and **discussion** around real life compromise examples.
Demonstrations are followed by relevant exercises using a number of vulnerable applications at **varying levels**.
The relevance of the learning opportunities to developers and testers working with APIs which may well have little to no user interface is strongly considered. Items which can be compromised easily using fuzzing and brute force techniques and which are of the greatest relevance receive the greatest focus.
After each exercise, relevant additional elements are **added to the Data Flow Diagram** to illustrate and expand the Threat Model and provide understanding of the mitigations required.

- Introducing O W ASP and the ' Top 10'
- Overview of the ten top vulnerabilities

- How vulnerabilities have changed over time
- How to construct and run a SQL injection attack
- Different forms of SQL injection in Web Apps
- Automated testing of SQL injection with *SqlMap*
- How to mitigate SQL injection attacks
- Defining the concept of Cross Site Scripting (XSS)
- How XSS can be used to compromise a Web Application
- Methods of mitigating various kinds of XSS attacks
- Chaining attacks to compromise applications.

The OWASP Top 10 (Part 2)

In this continuation of Part I, concepts are introduced using **demonstration** and **discussion** around real life compromise examples for the remaining sections of the OWASP Top 10. After each exercise, relevant additional elements are **added to the Data Flow Diagram** to illustrate and expand the Threat Model and provide understanding of the mitigations required.

- Common flaws in authentication and session management
- Choosing between whitelists and blacklists for validating input
- Identifying and fixing misconfigurations
- Guarding against sensitive data exposure
- Introducing function level access control
- Preventing cross site request forgery
- Avoiding components with known vulnerabilities
- Preventing unvalidated requests and forwards

Capture the Flag

- Comprehensive, guided and fast paced leader board session exploring practising penetration & security testing techniques.
- Use of relevant Capture the Flag software depending on audience
- Facebook CTF
- OWASP Juice Shop for developers and testers involved with Front End development.

Threat Modelling

This section builds on the above practical learnings with a new application to model, participants are provided with a whiteboard, a copy of the Microsoft Threat Modelling tool.

- Conducting a threat risk modelling workshop
- Producing effective lists of threats and mitigations through incremental and speedy threat modelling.
- Producing a Data Flow Diagram that visualises key interactions

Automated Security Testing

- Benefits of automating your security tests
- Options for automating the tools used on the course
- Adding automated security tests to the nightly build
- Automated testing and Continuous Integration in Agile

Additional Common Flaws

- Different forms of brute force attack
- Hacking login by force using *Hydra* and understanding of wordlists

- Mitigating brute force attacks
- Designing a RESTful API with security in mind
- Restricting particular HTTP verbs by user role
- Verifying and manipulating metadata given in H T TP headers
- Validating information early and often
- Safe usage of public cloud infrastructure:
- Correct usage of Security Groups
- Implementing a secure, redundant infrastructure with automation
- Security considerations around images
- Routing & network security

Assessment of Wireless Security

£1000 per person per day (Excl. of VAT)
Our Assessment of Wireless Security service meticulously evaluates the security of your wireless networks, detecting potential risks and vulnerabilities that could be exploited by cyber adversaries. We simulate real-world attacks to test the strength of your WEP, WPA, and WPA2 security protocols, along with assessing your network's susceptibility to common threats.

Infrastructure Assessments

£1000 per person per day (Excl. of VAT)
Our Infrastructure Assessments provide a comprehensive examination of your existing IT infrastructure to uncover vulnerabilities and recommend optimisation strategies. We analyse the configuration of your systems, network design, and operational procedures, aligning them with industry standards and best practices.

Web Application & Mobile Application Penetration & Security Testing

£1000 per person per day (Excl. of VAT)
Our Web and Mobile Application Penetration & Security Testing services ensure the robustness of your applications against cyber threats. Employing a variety of testing techniques such as static and dynamic analysis, we scrutinise application code, functionality, and backend systems to identify security weaknesses. We have provided this service to e-commerce platforms and many other organisations, where our penetration testing uncovered and rectified critical security issues, significantly improving their resilience against online attacks.

Open Source Intelligence and Social Engineering

£1000 per person per day (Excl. of VAT)
The Open Source Intelligence and Social Engineering service we offer leverages publicly available information to simulate social engineering attacks, assessing your organisation's susceptibility to information leakage and human factor breaches. Our operations have helped companies understand the ease with which sensitive data can be obtained and used maliciously. For a financial institution, we conducted a campaign that resulted in a fortified awareness and response plan against such social engineering tactics.

Cyber Essentials Plus

£1000 per person per day (Excl. of VAT)
Cyber Essentials Plus is our certification service that not only ensures compliance with the Cyber Essentials scheme but also includes an additional layer of hands-on technical verification. We conduct thorough tests on your systems and processes, providing a higher level of assurance in your cybersecurity practices. For instance, we have guided multiple SMEs through the certification process, significantly elevating their security standards and enabling them to meet contractual obligations with confidence.

Network & Infrastructure Penetration Testing

£1000 per person per day (Excl. of VAT)
Our Network & Infrastructure Penetration Testing service is a robust security measure that identifies and exploits vulnerabilities within your network infrastructure. It involves simulated cyber-attack scenarios crafted to assess the resilience of your network's security controls. Our certified experts utilise cutting-edge tools and methodologies to thoroughly evaluate physical devices, network hosts, services, and firewalls. As an example, for a major financial institution, we carried out a penetration test that exposed security flaws and led to significant security enhancements, thus fortifying their network against actual cyber threats.

Web Application Security Reviews

£1000 per person per day (Excl. of VAT)
Our Web Application Security Reviews are in-depth analyses aimed at identifying and mitigating security vulnerabilities in your web applications. By reviewing your application architecture and codebase, we provide actionable insights and recommendations for improving your security posture. We've assisted healthcare providers in strengthening their patient data portals, enhancing their protection against data breaches and cyberattacks.