Reiss Romoli

top-ix
WE DO CONNECTIONS

Introduzione al Security Testing (VA/PT)

Un *Security Assessment* è l'analisi della superficie d'attacco che una azienda espone e permette di capire se un attaccante è in grado sfruttare delle vulnerabilità o errori implementativi di un servizio per effettuare un attacco. Un'azienda, attraverso l'esecuzione di un *Security Assessment*, può comprendere le carenze di sicurezza che potrebbero essere sfruttate per ottenere l'accesso non autorizzato a componenti di rete critici e applicare le necessarie tecniche di difesa.

Agenda (3 gg)

Introduzione al Security Assessment

- Tipologie e modalità di esecuzione di un *Security Assessment*
  - Analisi della superficie d'attacco
  - *Vulnerability Assessment / Penetration Test*
  - *Social Engineering Attack Simulation*
  - *Infrastructure Assessment*
  - *Security Awareness Audit*
- Linee guida per lo svolgimento di un *Security Assessment*
- Preparazione delle regole di ingaggio per un *Security Assessment*

Metodologia di base per lo svolgimento di un *Security Testing*

- Tecniche e strumenti per l'analisi OSINT
- Tecniche e strumenti per il *Vulnerability Assessment*
- Tecniche e strumento per il *Penetration Test*
  - Utilizzo dei programmi Open Source per l'esecuzione di un *Penetration Testing*
- *Dark reading*

Esecuzione dei principali step di un Vulnerability Assessment (VA)

- *Planning and Preparation*
  - Autorizzazione
  - Criticità, finestra di manutenzione
- Esecuzione
  - *Information Gathering / Mapping* di una rete
  - *Vulnerability Scanning*
  - Velocizzare o rallentare l'*assessment*
- Analisi aggiuntive
  - Tecniche di rilevazione delle vulnerabilità di un sistema
  - *Penetration test*: quando e come

Analisi delle vulnerabilità trovate

- Classificazione e priorità delle vulnerabilità rilevate
- Probabilità, impatto, rischio
  - Scenari di attacco / *Attack Vector*
  - MITRE
  - *Business Impact Analtysis* (cenni)

Gestione delle vulnerabilità

- *Vulnerability Management*
- *Patch Management*
- *Remediation Plan*

Tecniche di sfruttamento delle vulnerabilità rilevate in un VA

- Struttura di un *exploit*

Architettura e protocolli utilizzati dai web server

Principali vulnerabilità di una Web Application

- Metodologia OSWAP e analisi dell'OWASP Top 10 relativa alle principali vulnerabilità
- Tecniche di attacco attraverso strumenti open source e commerciali

Obiettivi

Fornire a un *security engineer* i principi fondamentali per la realizzazione di un'attività di *security testing* in termini di *Vulnerability Assessment* e *Penetration Testing*. Durante lo svolgimento del corso, oltre ai fondamenti teorici, saranno svolte diverse esercitazioni.

Destinatari

IT Auditor, Consulenti informatici, Responsabili di Sistemi Informativi, Forze dell'Ordine, Responsabili della Sicurezza Informatica, Sistemisti e operatori del settore ICT.

Prerequisiti

Conoscenza dei principali sistemi operativi, fondamenti di *networking*, conoscenza dei principi e strumenti di sicurezza informatica.