

## ► CHE COS'È?



Un approccio graduale al pentesting dei prodotti con elementi digitali (PDE) in linea con il Cyber Resilience Act (CRA)

## ► A CHI È RIVOLTO?



Piccole e medie imprese (PMI) che producono prodotti con elementi digitali.

# METODOLOGIA DI PENETRATION TESTING ALLINEATA AL CRA



## CONFIRMATE

Il progetto finanziato nell'ambito dell'accordo di sovvenzione n. 101190193 è sostenuto dal Centro europeo di competenza per la sicurezza informatica.



Co-funded by  
the European Union



## ► PUNTI DI ATTENZIONE !!

La CRA non richiede test di penetrazione in sé, ma impone "revisioni e test efficaci e regolari" della sicurezza dei prodotti.

L'esercitazione di test può rafforzare la base probatoria per una dichiarazione di conformità ai requisiti essenziali di sicurezza informatica della CRA.

## ► È TUTTO NUOVO?



No, si basa sugli standard del settore: OSSTMM3, ETSI EN 303 645 e TS 103 701, OWASP Testing Guide, PTES e NIST SP 800-115.

## ►PASSO DOPO PASSO



### 1. Fase preliminare e pianificazione

Definizione dell'ambito, dei requisiti CRA, degli ambienti di test, delle autorizzazioni e allineamento delle parti interessate.

**Risultato:** piano di test, documenti legali, valutazione iniziale dei rischi.



### 2. Raccolta di informazioni e riconoscimento

Mappare la superficie di attacco, raccogliere OSINT e definire scenari di attacco realistici.

**Risultato:** profilo dell'avversario, informazioni iniziali sulle vulnerabilità..



### 3. Esecuzione e sfruttamento

Verifica delle vulnerabilità tramite strumenti e controlli manuali, simulazione di attacchi in laboratorio.

**Risultato:** rapporto completo sulle vulnerabilità.



### 4. Analisi dell'impatto e rendicontazione

Valutare la gravità, mappare il CRA, definire le azioni correttive.

**Risultato:** risultati mappati sul CRA, strategia correttiva.



### 5. Post-impegno e follow-up

Verificare le correzioni, ripetere i test, raccogliere feedback e preparare le comunicazioni, se necessario.

**Risultato:** rapporto finale sul test di penetrazione per la conformità CRA.

## ABOUTINFORMAZIONI SU CONFIRIMATE

Semplificare e automatizzare la conformità al Cyber Resilience Act (CRA). Attraverso lo sviluppo di strumenti open source, metodologie standardizzate e risorse formative, aiutiamo le PMI a districarsi tra i requisiti di sicurezza informatica con facilità ed efficienza. Il nostro obiettivo è creare un ecosistema dinamico in cui gli stakeholder possano scambiarsi le migliori pratiche, tenersi aggiornati sugli sviluppi normativi e contribuire al progresso dei prodotti digitali sicuri.

### VEDI ALTRO



[www.confirmate-project.eu](http://www.confirmate-project.eu)

[confirmate.project@gmail.com](mailto:confirmate.project@gmail.com)

[cyen-cybersecurity](#)