

# SCADA PENETRATION TESTING PER IL SETTORE ENERGETICO

I Sistemi di Controllo di Supervisione e Acquisizione Dati (SCADA) sono fondamentali per il monitoraggio e la gestione delle infrastrutture critiche in molti settori, ma sono particolarmente vitali nel settore energetico, dove controllano reti elettriche, centrali, raffinerie e altre infrastrutture chiave.

Un attacco a un sistema SCADA potrebbe portare a gravi interruzioni, perdite economiche e potenziali danni fisici.

## SCENARIO

Una compagnia energetica nazionale, "EnergeticaX", ha ampliato la sua rete di distribuzione e ha implementato nuove funzionalità nei suo sistema SCADA. Prima di portare i sistemi completamente online, desidera effettuare uno SCADA Penetration Testing per valutare potenziali vulnerabilità.

## STEPS

### 01/ SCOPING

Definizione degli obiettivi specifici del test, tenendo conto delle nuove implementazioni e delle aree critiche.

### 02/ RECONNAISSANCE

Raccolta di informazioni sui sistemi SCADA di EnergeticaX e sulla sua infrastruttura di rete.

### 03/ SCANNING

Utilizzo di strumenti specializzati per rilevare vulnerabilità nei sistemi SCADA.

### 04/ EXPLOITATION

Tentativo di sfruttare le vulnerabilità identificate per valutare l'effettivo impatto di un attacco.

### 05/ POST-EXPLOITATION

Analisi della superficie dell'area compromessa e valutazione delle potenziali implicazioni in caso di un vero attacco.

### 06/ REPORT

Elaborazione di un report dettagliato sulle vulnerabilità trovate, la loro gravità e le raccomandazioni per la loro correzione.

### 07/ REVIEW & REMEDIATION

Collaborazione con "EnergeticaX" per correggere le vulnerabilità identificate e rafforzare i loro sistemi.

## COME POSSIAMO AIUTARTI

### <sup>01/</sup> EXPERTISE SPECIALIZZATA

Aspisec possiede un team dedicato ai sistemi SCADA, con una profonda conoscenza delle sfide uniche e delle vulnerabilità tipiche di questi sistemi.

### <sup>02/</sup> STRUMENTI AVANZATI

L'utilizzo di strumenti specifici per SCADA assicura che le valutazioni siano accurate e pertinenti.

### <sup>03/</sup> APPROCCIO SICURO

I penetration test su sistemi SCADA sono delicati, data l'importanza critica di tali sistemi. Aspisec garantisce che tutti i test siano condotti in modo sicuro, evitando potenziali interruzioni o danni.

### <sup>04/</sup> FORMAZIONE E SUPPORTO

Post-test, Aspisec può offrire formazione al team di "EnergeticaX" su migliori pratiche di sicurezza, nonché supporto continuo per mitigare future minacce.

Attraverso un'efficace SCADA Penetration Testing offerto da Aspisec, "EnergeticaX" può garantire la sicurezza delle sue infrastrutture critiche, proteggendo l'energia e i servizi su cui si basa l'intera nazione.

L'esempio di use case fornito rappresenta solo una delle molte applicazioni possibili. Aspisec ha una consolidata esperienza in vari settori, tra cui Energy, Oil & Gas, Telco, Transport, Banking, Health, Insurance, Industry, Gov e Space.

Contattaci per una consultazione gratuita ad [info@aspisec.com](mailto:info@aspisec.com)

