

Università degli Studi di Salerno



Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Regole di Ingaggio su un Asset Reale

Arcangelo Castiglione
arcastiglione@unisa.it

Regole di Ingaggio

Asset Reale

Regole di Ingaggio

Con la presente, si definiscono le condizioni contrattuali tra il sottoscritto [redacted], nato a [redacted], il [redacted], CF. [redacted], residente in [redacted] (d'ora in poi "Il beneficiario"), e [redacted], nato a [redacted], il [redacted], CF. [redacted] (d'ora in poi "Il cliente"), facente le veci di [redacted] (d'ora in poi "il contraente"), titolare dell'attività [redacted] in piazza [redacted], riguardanti l'analisi della sicurezza (d'ora in poi "Penetration Testing") del relativo sistema informativo (d'ora in poi "asset"), a scopo puramente didattico-formativo.

Con la presente, si autorizza [redacted] ad effettuare attività di Penetration Testing al fine di valutare la sicurezza dell'asset ivi specificato, condotto tra il giorno 30/06/2019 e il giorno 9/07/2019 (d'ora in poi "periodo di Penetration Testing").

Le attività di Penetration Testing verranno effettuate seguendo la metodologia black box/double blind^[1].

Lo scope^[1] del Penetration Testing, coperto dal presente contratto, comprende l'indirizzo IP:

93.146.63.6

E tutti gli host, di competenza del cliente, collegati durante il periodo di Penetration Testing coperto da questo contratto.

Regole di Ingaggio

Asset Reale

Con la presente:

- Il cliente riconosce che tutte le azioni del beneficiario relative all'adempimento degli obblighi contrattuali ivi presentati non hanno intenzioni malevole e/o nocive per il contraente e il cliente, né minano l'integrità, la confidenzialità o la disponibilità delle informazioni raccolte, intenzionalmente e non, durante l'attività di Penetration Testing.
- Il beneficiario si occupa di minimizzare, nei limiti delle sue possibilità, i periodi di downtime del sistema derivanti dall'utilizzo di tecniche aggressive o da eventuali effetti collaterali imprevedibili.
- Il cliente riconosce che tutte le azioni del beneficiario relative all'adempimento degli obblighi contrattuali ivi presentati abbiano come fine il miglioramento della sicurezza dell'asset del cliente.
- In particolare, al fine di verificare la validità delle vulnerabilità scoperte dell'asset e al fine di valutare il potenziale rischio derivante dall'utilizzo di esse (exploiting), il beneficiario riceve dal cliente l'autorizzazione ad effettuare le seguenti:
 1. Scoprire, analizzare ed utilizzare le vulnerabilità scoperte per avere accesso all'asset del cliente
 2. Utilizzare tecniche di password cracking per valutare la sicurezza delle password utilizzate nell'asset.
 3. Nel caso in cui il beneficiario dovesse ottenere con successo l'accesso all'asset:
 - Utilizzare tecniche di postexploitation per ottenere accesso agli altri sistemi interconnessi
 - Utilizzare tecniche di privilege escalation per ottenere accesso ad informazioni riservate
 - Cercare di ottenere informazioni critiche per le politiche di business in modo da dimostrare i rischi effettivi dell'asset.

Regole di Ingaggio

Asset Reale

L'autorizzazione s'intende comprendente di tutti i sistemi informativi specificati nello scope del progetto di Penetration Testing.

Una volta terminato il periodo di Penetration Testing, verrà stilato un documento (report) relativo all'attività svolta, con indicazioni sulle contromisure da prendere per migliorare la sicurezza dell'asset.

Le informazioni collezionate durante il periodo di Penetration Testing verranno divulgate solo ed esclusivamente al prof. Arcangelo Castiglione, docente del corso di Penetration Testing & Ethical Hacking per l'A.A. 2018/2019 all'Università degli studi di Salerno, ai fini delle attività d'esame.

Il Beneficiario



Il Cliente

