VA/PT LIGHT

it’s time to rethink the security concept!

A great cyber security and development company

Vulnerability Assessment/Penetration Test LIGHT

VA/PT

Vulnerability Assessment/Penetration Test LIGHT

VULNERABILITY ASSESSMENT E PENETRATION TEST

Una corretta gestione della sicurezza si basa innanzitutto su un'adeguata conoscenza dell'attuale livello di protezione dei propri sistemi. Partendo da questo presupposto, SEC4U ha consolidato la propria esperienza nell'applicazione di metodologie di Vulnerability Assessment e Penetration Testing, approcciando il problema da diversi possibili punti di vista.

OBIETTIVI

Le attività di Vulnerability Assessment e Penetration Test offerte da SEC4U hanno il comune obiettivo di fornire al cliente una conoscenza dettagliata sullo stato di sicurezza dei propri sistemi informatici.
In particolare, attraverso diverse fasi di analisi, effettuate simulando differenti scenari di intrusione, le metodologie adottate da SEC4U le permettono di:
verificare che le informazioni sulla rete del Cliente visibili da Internet siano ridotte al minimo;
verificare che non sia possibile ottenere accessi non autorizzati a sistemi ed informazioni;
valutare se per un utente interno sia possibile accedere ad informazioni o ottenere privilegi per i quali non ha l'autorizzazione necessaria;
verificare che una Web Application non contenga vulnerabilità che permettano ad un attaccante di ottenere accessi non autorizzati a dati riservati, in particolare impersonificazione di altri utenti, privilege escalation, accesso interattivo alla rete target, attacco all'utente dell'applicazione, Denial of Service.

VA/PT LIGHT

SEC4U mette a disposizione l'innovativo servizio VA/PT LIGHT. Si tratta a tutti gli effetti di un Vulnerability Assessment e Penetration Test che va a testare la corretta postura difensiva di un'organizzazione, la cui particolarità è però quella di essere rivolto in modo specifico alle piccole imprese, che spesso utilizzano tecnologie "di massa" e per le quali quindi SEC4U ha costruito una checklist di controlli facilmente ripetibili. Questo consente di ottimizzare i nostri servizi e soprattutto consente di abbassare notevolmente i costi che devono sopportare i nostri clienti.

Stiamo parlando di attività quali studi tecnici (geometri, architetti, ingegneri), studi notarili, studi legali ed in generale le piccole attività, le cui risorse tecnologiche di base a disposizione spesso si possono riassumere nelle seguenti:

- router internet
- file server
- stampanti
- workstation
- dispositivi mobile

Nelle attività di dimensioni poco superiori possono poi comparire:

- server voip
- server di dominio
- dispositivi Internet of Things

Questa omogeneità di risorse ci permette di rendere semi-automatici alcuni dei test che normalmente necessiterebbero di molta più attività manuale per raggiungere risultati equiparabili in realtà medio/grandi.

In ogni caso le attività di Vulnerability Assessment e Penetration Test, anche nella loro versione LIGHT, mantengono sempre una perfetta aderenza allo standard che impieghiamo quanto andiamo ad effettuare VA/PT di dimensione maggiore. Questo per mantenere un'elevatissima qualità dell'attività e soprattutto per rendere completamente ripetibili i test in un momento successivo.

Abbiamo messo a punto questa tipologia di VA/PT per consentire alle piccole attività di potersi rendere facilmente compliance con quanto stabilito dal General Data Protection Regulation (GDPR).

Le singole operazioni effettuate durante un VAPT Light vengono descritte nel documento **VAPT Light – Operations**.

GDPR COMPLIANCE

Un VA/PT periodico permetterà di essere compliance con quanto stabilito in materia dal General Data Protection Regulation (GDPR), che all'articolo 32 cita:

1.Tenendo conto dello stato dell'arte e dei costi

di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

…

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

VA/PT A CADENZA REGOLARE

Nel punto d) di quanto espresso dall'articolo 32 del GDPR esprime enorme importanza l'espressione "***valutare regolarmente***", per cui risulta fondamentale applicare ai VA/PT una cadenza periodica.
SEC4U, nella versione base del servizio VA/PT LIGHT, fornisce una **verifica trimestrale** della postura difensiva dell'organizzazione, che viene descritta in un apposito report, che viene consegnato al Cliente al termine dell'attività e che viene redatto seguendo i consigli descritti nel documento NIST SP 800-115.

VA/PT INFRASTRUTTURALE

Il servizio di VA/PT, nella sua versione LIGHT, verte soprattutto sulla parte infrastrutturale, anche se a richiesta SEC4U può ovviamente valutare anche gli altri ambiti (VA/PT applicativo, pentest sulle reti wireless, valutazione fattore umano attraverso tecniche di Social Engineering,…).
La metodologia utilizzata da SEC4U per l'attività di VA/PT infrastrutturale è conforme all'Open Source Security Testing Methodology Manual di ISECOM, standard internazionale de-facto in materia.

Le fasi principali del VA/PT infrastrutturale riguardano:

HOST IDENTIFICATION

La rete viene analizzata al fine di determinare i sistemi attivi ed ognuno di questi sistemi viene sottoposto a tecniche di fingerprinting attivo (inviando richieste ai sistemi stessi) e passivo (ottenendo le informazioni da server pubblici quali DNS o i database WHOIS), in modo da determinare, con la massima precisione possibile, la versione del Sistema Operativo installato.

ENUMERAZIONE DEI SERVIZI E IDENTIFICAZIONE DELLE VULNERABILITÀ

Tutti gli host attivi vengono esaminati per scoprire quali porte risultino essere aperte e quindi quali servizi risultino essere in ascolto. Per ogni servizio rilevato si tenta di identificare la versione del software ad esso associato.
Questa identificazione permette di effettuare test di verifica della presenza delle vulnerabilità che potrebbero essere sfruttate per ottenere un accesso non autorizzato ai sistemi. I test utilizzati combinano tecniche manuali e strumenti automatizzati, in modo da disporre della velocità e dell'esaustività delle scansioni automatiche, unite all'efficacia e alla precisione di un esperto hacker qualificato.

EXPLOIT EFFETTIVO

Nei casi in cui venga realizzato un penetration test completo (e comunque sotto espressa richiesta del cliente) l'attività di sfruttamento delle vulnerabilità riscontrate viene portata a termine nell'ottica di comprendere quali siano gli effettivi impatti, sui sistemi e sui dati, di una potenziale intrusione.

PERSONALE CERTIFICATO

SEC4U esegue le attività di Vulnerability Assessment e di Penetration Test avvalendosi di personale altamente qualificato e certificato CEH (Certified Ethical Hacker) e eCPPT (eLearnSecurity Certified Professional Penetration Tester).