# 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, Spike Reply ha consolidato la propria esperienza nell'applicazione di metodologie di Vulnerability Assessment e Penetration Testing internazionalmente riconosciute, approcciando il problema da diversi possibili punti di vista ed arrivando rispondere a tutte le esigenze poste dai Clienti in questi ambiti.

## OBIETTIVI

Le attività di Vulnerability Assessment e Penetration Test offerte da Spike Reply 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 Spike Reply 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.

**VULNERABILITY ASSESSMENT VS PENETRATION TEST.** Per raggiungere tali obiettivi, la metodologia seguita da Spike Reply adotta due diverse tipologie di verifiche tecniche: Vulnerability Assessment e Penetration Test. Queste due tecniche si differenziano tanto per i risultati che permettono di raggiungere quanto per le risorse necessarie alla loro conduzione.

Un'attività di Vulnerability Assessment (VA) permette al Cliente di avere una fotografia dello stato di esposizione dei propri sistemi a tutte le vulnerabilità note. A questo scopo, vengono utilizzati alcuni tool automatici, i quali, effettuando una lunga serie di controlli su ogni singolo sistema o applicazione, permettono di conoscere dettagli riguardanti la loro configurazione e l'eventuale presenza di vulnerabilità. La velocità con la quale questi software effettuano le verifiche necessarie permette di testare in breve tempo un perimetro estremamente ampio, fornendo allo stesso tempo una visione di notevole dettaglio. Di contro, utilizzare strumenti automatici porta da un lato all'impossibilità di estendere il controllo oltre le vulnerabilità per le quali il tool è stato programmato e dall'altro a non verificare l'effettiva possibilità che un attaccante avrebbe di sfruttare tali vulnerabilità.

Al fine di fornire al Cliente la possibilità di effettuare analisi più precise ed approfondite di quelle permesse da un VA, Spike Reply offre la propria esperienza anche nel campo dei Penetration Test (PT). Durante un Penetration Test vengono infatti effettuate delle vere e proprie simulazioni di intrusione, ipotizzando diversi scenari di attacco e combinando tecniche manuali all'utilizzo degli strumenti automatici. In questo modo è possibile analizzare innanzitutto l'esposizione a vulnerabilità non verificabili dai software automatici, ma ancora più importante è la possibilità di mostrare come, anche laddove le vulnerabilità presenti, se considerate singolarmente non portino ad una reale situazione di rischio, un loro sfruttamento combinato possa invece esporre a conseguenze di notevole impatto.

Infine, operando manualmente su sistemi ed applicazioni, è anche possibile sfruttare le vulnerabilità riscontrate, portando a termine la simulazione di attacco, così da mostrare quali siano le reali conseguenze a cui questo potrebbe portare in un caso reale.

**PERIMETRI DI APPLICAZIONE.** I paradigmi generali descritti in precedenza assumono contorni ben diversi a seconda del loro campo di applicazione. In questo senso, è possibile delineare principalmente tre diversi ambiti:

- VA / PT infrastrutturali: riguardano tutte le verifiche a livello di configurazione della rete wired, dei server ed eventualmente dei client.
- VA /PT applicativi: riguardano tutte le verifiche effettuate sulle singole applicazioni.
- PT infrastruttura wireless: riguardano tutte le verifiche specifiche per le reti senza fili.

## VA/PT INFRASTRUTTURALE

La metodologia utilizzata da Spike Reply 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 che compongono la metodologia applicata vengono sinteticamente rappresentate nel diagramma in figura.


Le fasi principali 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.

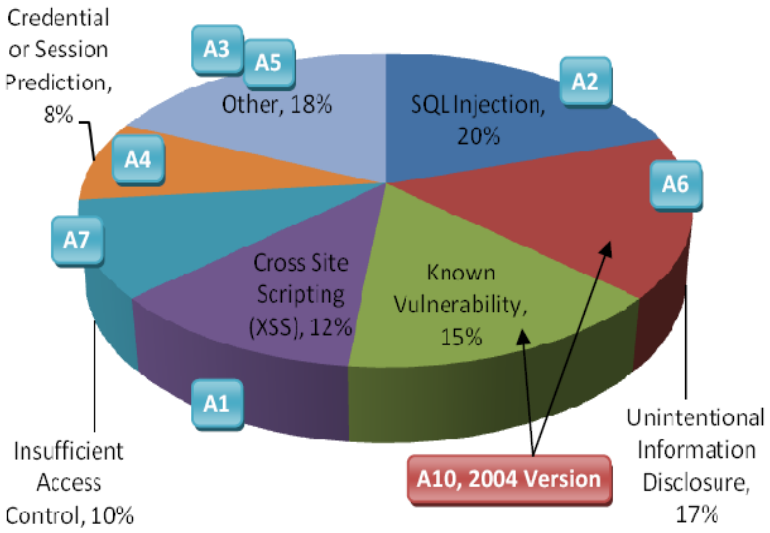
**EXPLOIT EFFETTIVO.** Nei casi in cui venga realizzato un penetration test completo (e comunque sotto espressa richiesta del cliente) l'attività di sfruttamento delle vulnerabilità riscontrate viene portata a termine nell'ottica di comprendere quali siano gli effettivi impatti, sui sistemi e sui dati,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

## VA/PT APPLICATIVO

Ad oggi un ruolo particolarmente importante all'interno delle diverse attività di verifica tecnica è assunto dai test sulle applicazioni web. Il motivo di questa attenzione è da ricercarsi nelle statistiche dei vettori di attacco: il 70% degli attacchi informatici sono resi possibili da errori di programmazione.

Per svolgere le attività di Penetration Test sulle applicazioni web Spike Reply utilizza una metodologia ormai consolidata nella comunità scientifica internazionale e riassunta all'interno dell'Open Web Application Security Project (OWASP), organizzazione di riferimento per la sicurezza delle web application. Questa analisi è costituita da una serie di tentativi d'attacco che coinvolgono i protocolli e le logiche di comunicazione utilizzati dagli utenti finali per interagire con le applicazioni (attacco ai web server, alla struttura applicativa, ai sistemi di autenticazione ed autorizzazione, alle interfacce di gestione, ai sistemi client, …). Nel caso specifico delle applicazioni web, tali attacchi sono basati su manipolazioni dei pacchetti HTTP che vengono scambiati fra i browser degli utenti ed il web server.

I test vengono condotti sia in modalità anonima che in "user-mode", utilizzando un account creato tramite le usuali procedure di attivazione, al fine di permettere al penetration tester l'accesso come utente autorizzato. In questo modo è possibile testare la robustezza dei sistemi di autenticazione e di contenimento sia per utenti anonimi che per normali utilizzatori autorizzati.




L'attività comprende quindi l'analisi dell'applicazione in termini architetturali, nonché l'esame delle configurazioni delle macchine interessate, sia a livello di sistema operativo che a livello applicativo.

Particolare attenzione viene riservata, in fase di testing, alle classi di vulnerabilità rientranti tra le 10 vulnerabilità più importanti come diffusione e impatto sui sistemi, facenti parte della OWASP Top 10. In questo modo è anche possibile mantenere un costante riferimento per valutare la gravità delle situazioni riscontrate.

## PT INFRASTRUTTURA WIRELESS

Lo spettro delle attività di verifiche tecniche di sicurezza viene completato dalle analisi riguardanti l'infrastruttura di rete wireless. Le analisi riguardano principalmente la famiglia di reti 802.11 ed il relativo security assessment ha l'obiettivo di verificare la presenza di punti d'accesso autorizzati e non autorizzati e la loro copertura, nonché la loro consistenza e le vulnerabilità ad essi riconducibili.

L'attività è suddivisa principalmente in due macro-fasi. La prima fase è dedicata esclusivamente alla rilevazione di segnali radio all'interno degli stabili identificati come perimetro di analisi ed è condotta adottando strumentazione hardware e software specifica per ogni tipo rete. In questo modo è possibile stabilire quali siano le reti wireless presenti, determinare se i livelli di sicurezza di queste reti siano conformi alle policy aziendali e alle best practice in materia e verificare l'assenza di reti non autorizzate.La seconda fase è invece dedicata alla perlustrazione dei perimetri esterni, al fine di valutare, in particolare per le reti più critiche, se il livello del segnale radio permetta la connessione anche in zone ad accesso pubblico.

La metodologia segue i passi specificati nell'Open Source Security Testing Methodology Manual (OSSTMM), già utilizzata per le attività di VA e PT infrastrutturale.

Reply
spike

All'interno del Gruppo Reply SpA, Spike Reply è la società specializzata sulle tematiche relative all'area della Sicurezza e della tutela dei Dati Personali.

Spike Reply ha definito un'offerta completa, integrata e coerente per affrontare ogni aspetto del rischio associato ad un sistema informativo: dall'individuazione delle minacce e delle vulnerabilità, alla definizione, progettazione e di implementazione delle relative contromisure tecnologiche, legali, organizzative, assicurative o di ritenzione del rischio.

Spike Reply
www.reply.eu