

L'Ethical Hacking

Il test di intrusione per la verifica delle difese informatiche

Le attività di **Ethical Hacking** sono principalmente strumenti utili al management aziendale, poiché sono il risultato di competenze tecniche ed organizzative che consentono l'analisi e le scelte migliori per risolvere i problemi nell'ambito della sicurezza informatica.

Esse consentono ad un'azienda di poter verificare se il proprio sistema informativo è vulnerabile, tenendo presente che la vulnerabilità può essere sia di tipo organizzativo (dipende da scorrette procedure umane) che di tipo fisico (dipende dalle configurazioni degli apparati preposti).

NEST2 si occupa da sempre di sicurezza informatica e offre una serie di test atti a verificare le difese della rete informatica aziendale.

Una rete vulnerabile può portare danni economici, per questo è consigliabile sapere lo stato di vulnerabilità della propria rete informatica.

Attraverso il servizio di Ethical Hacking NEST2 sfrutta le proprie conoscenze e tecnologie tipiche di un hacker, ma con l'unico obiettivo di proteggere la rete e non di danneggiarla.

Premessa

Per accrescere il proprio business e velocizzare lo scambio di informazioni, le moderne aziende si sono attivate per consentire ai propri clienti e ai propri business partner, l'accesso alla propria rete informatica o quantomeno l'accesso ad informazioni (p.e. via web).

Questa necessità di accesso condiviso, se da un lato ottimizza la comunicazione e crea maggiori opportunità di lavoro, dall'altro può ledere l'integrità dei dati sensibili. L'accesso condiviso, se non eseguito con le dovute cautele e con le opportune politiche di sicurezza informatica, può diventare sinonimo di rischio informatico.

Sul mercato esistono sistemi automatici e applicazioni di scansione più o meno valide, sviluppate per verificare la presenza di eventuali "buchi" o configurazioni errate nelle reti e nei sistemi rifacendosi a modelli e vulnerabilità note, che sono di aiuto per una prima verifica delle vulnerabilità presenti sui sistemi analizzati.

Questi strumenti non sono però in grado di rivelare i problemi che solitamente emergono dopo i test manuali degli esperti di sicurezza, in cui la componente più pericolosa è l'intelligenza umana.

Investimenti anche ingenti nella sicurezza ICT con sistemi firewall o IDS, possono illudere di essere protetti: sfortunatamente non è sempre così! Il primo suggerimento quindi, al fine di ridurre al minimo i rischi derivanti da eventuali attacchi ad una rete, è quello di affiancare ai test automatici eseguiti con dei software di scansione (**vulnerability assessment, o test di vulnerabilità**), dei test manuali che possano simulare realmente un'intrusione (**penetration test, o test di intrusione**).

Semplificando, si potrebbe affermare che con il **test di vulnerabilità** viene scattata una fotografia complessiva e dettagliata del sito oggetto dell'attacco: la foto viene poi analizzata dal sistemista in sicurezza con la visione propria dell'hacker, per poter procedere con il tentativo di intrusione, ossia il **penetration test**.

Questa pratica prende il nome di "**ethical hacking**", in quanto si sfruttano conoscenze e tecnologia tipiche di un hacker, ma **finalizzate alla protezione della rete e non al suo danneggiamento**.

Obiettivi

Tramite il servizio di **Ethical Hacking**, NEST2 propone dei **test di intrusione** atti a creare un quadro attuale e non apparente della "effettiva" capacità di difesa di una rete o sistema.

L'Ethical Hacking consente quindi di:

- Verificare concretamente se il sistema informatico aziendale è a prova di hacker, cioè di intrusioni da parte di malintenzionati
- Testare l'infrastruttura informatica dell'azienda per verificare l'attendibilità delle configurazioni degli apparati che compongono la rete informatica
- Individuare i settori a rischio e vulnerabili del sistema di rete
- Bloccare la fuga di informazioni, cioè gli attacchi informatici

I test si possono avvalere di informazioni diverse, le quali identificano due categorie principali:

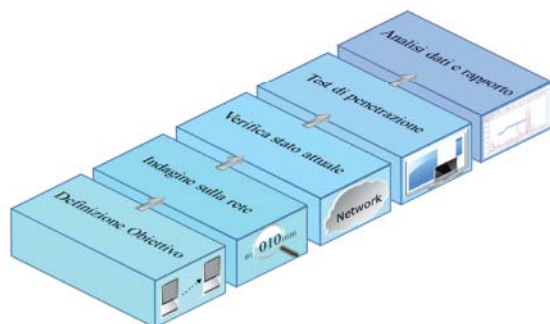
- **Black Box.** Quando non si hanno conoscenze della rete oggetto del test, fatto salvo quanto acquisito con il test di vulnerabilità
- **White Box.** Quando si ha una conoscenza completa della rete oggetto del test, con informazioni fornite anche dal cliente stesso, per mettersi nella situazione peggiore

La differenziazione in due tipologie si rende necessaria in quanto le tecniche e gli strumenti utilizzati per il tentativo di intrusione, variano come tempi e strumenti impiegati pur mantenendo una loro similitudine.

Particolarmente pericolosa è considerata la seconda tipologia di attacco (White Box), in quanto può includere la complicità di un dipendente o di un ex-dipendente dell'azienda, necessaria per poter disporre delle informazioni sensibili che difficilmente si riescono a reperire attraverso un test di vulnerabilità.

Nell'esecuzione dei test di intrusione, NEST2 segue alcuni processi fondamentali schematizzati nell'immagine sotto riportata.

Processi per l'esecuzione del test di intrusione



Vantaggi

Premesso che non esiste la sicurezza al 100% (diffidate di chi vi assicura il contrario), questa pratica consente comunque di prendere coscienza della capacità di difesa della propria rete o dei propri sistemi, rendendo visibili le eventuali debolezze che un hacker esperto potrebbe sfruttare, dando quindi la possibilità di difendere al meglio la rete, sia a livello di management interno, che di configurazione dei servizi erogati (server), garantendo quanto segue:

- Scoperta dei punti deboli attraverso il test di intrusione
- Riduzione del rischio di un attacco reale che potrebbe creare seri danni
- Identificazione dell'effettivo livello di solidità delle configurazioni dei sistemi di sicurezza
- Attenta valutazione delle singole caratteristiche dell'infrastruttura ICT
- Attenta valutazione degli investimenti effettuati in termini di sicurezza
- Simulazione di attacco perfettamente affidabile e reale

Applicazioni

Considerato che è l'evoluzione delle tecnologie, rapportata allo sviluppo economico odierno e alle norme legislative attuali, che richiede ad ogni azienda moderna, semplice o complessa, un elevato livello di sicurezza, l'attività di Ethical Hacking può essere applicata a tutte le realtà aziendali che trattano dati sensibili e non divulgabili, e più in generale per assicurarsi che la propria infrastruttura informatica non possa essere utilizzata per scopi illeciti o corrotta con perdita di produttività.

Per dare alcuni esempi esplicativi:

- Aziende dove avvengono transazioni bancarie
- Enti amministrativi dove risiedono informazioni personali
- Aziende che desiderano innalzare il livello di sicurezza della loro rete (o parte di essa) o comunque implementare un livello di sicurezza più elevato
- Aziende che necessitano di un controllo schedato sui loro apparati pubblicati in Internet, verificando di avere ogni sistema sempre aggiornato contro le più recenti tipologie di attacco

