Versione italiana

CONOSCERE LE PRINCIPALI
TECNICHE CYBER
TRA ASSESSMENT E TEST

DIFFERENZE E PUNTI DI ATTENZIONE TRA VULNERABILITY ASSESSMENT E PENETRATION TEST

ALESSANDRO SCARAFILE

« La sicurezza IT è come una promessa:
se ci tieni troverai un modo, altrimenti troverai una scusa. »

Alessandro Scarafile

VP Cyber Security & Operations
Syneto

SOMMARIO

INTRODUZIONE

Le persone parlano spesso di penetration testing, ma in realtà il richiedente si aspetta un vulnerability assessment. Altre volte, al contrario, in molti richiedono un vulnerability assessment, mentre ciò di cui hanno davvero bisogno è un penetration test.

Spesso è un problema di comunicazione, dal momento che — visti da lontano — i due termini sembrano molto simili e vengono spesso utilizzati in modo intercambiabile. Tuttavia, da vicino è tutta un'altra storia.

Essenzialmente, un vulnerability assessment è una scansione automatizzata utilizzata per identificare vulnerabilità, mentre un penetration testing mira a sfruttare tali vulnerabilità per ottenere una comprensione più profonda delle falle nelle difese.

1. COS'È UN VULNERABILITY ASSESSMENT?

Un vulnerability assessment è una **scansione**. Utilizza strumenti automatizzati per verificare la vulnerabilità dei sistemi. Immaginiamo un ladro che identifica un ingresso sul retro del vostro edificio, ma non entra. I risultati della scansione mostreranno come un'applicazione, un sito web o un altro sistema sia vulnerabile, ma non forniranno dettagli su cosa potrebbe accadere se tale vulnerabilità fosse sfruttata.

Molte organizzazioni effettuano vulnerability assessment per "spuntare una casella", di solito in ambito compliance. Tuttavia, ci sono limiti a un vulnerability assessment, poiché non è in grado di spiegarne l'impatto, la capacità di riadattare una vulnerabilità o usarne un'altra per compromettere un sistema. Esiste anche la possibilità di falsi positivi/negativi, quindi è importante verificare i risultati automatizzati con più strumenti o con l'aggiunta di metodi manuali.

2. COS'È UN PENETRATION TEST?

Il penetration testing è un metodo per identificare e **testare** vulnerabilità nella sicurezza IT, che potrebbero essere sfruttate in infrastrutture esterne o interne, lasciando un'azienda a maggior rischio.

Un penetration test di solito inizia con una scansione automatica delle vulnerabilità, ma va molto più in profondità. Nel nostro scenario di un ipotetico furto, questa volta i ladri stanno verificando un'entrata posteriore per poi effettivamente entrare nell'edificio (tranquilli, sono autorizzati!).

Questa modalità di test — che molte persone potrebbero considerare "hacking" — è un esame sistematico di una rete o di un sistema, effettuato da esperti di sicurezza qualificati e professionisti a cui è stato concesso il permesso di sfruttare le vulnerabilità e le configurazioni errate che troveranno strada facendo, per determinarne il potenziale impatto.

Gli esperti lavoreranno su una metodologia di prova predefinita, per entrare nella rete attraverso le lacune identificate (da cui il termine "penetrazione"), usando le loro conoscenze, informazioni Open Source e una vasta gamma di strumenti. Una volta identificate e testate le falle di sicurezza nei sistemi e nelle reti, forniranno una consulenza mirata per rafforzarne le difese.

3. VULNERABILITY ASSESSMENT VS. PENETRATION TEST

Proviamo a capire meglio cosa è incluso in ciascun servizio, attraverso questo pratico confronto tra un vulnerability assessment e un penetration test generico (ogni test dipenderà dal sistema in esame).

Immagine 1: **Categorie di Attività**

Description	VA	PT
Scoping call	✓	✓
Documenting of requirements and scope	✓	✓
Passive information gathering		✓
Active information gathering	✓	✓
Automated vulnerability scan	✓	✓
Exploit analysis		✓
Vulnerability confirmation		✓
Misconfiguration examination		✓
Vulnerability/misconfiguration exploitation		✓
Application/infrastructure exploit pivoting		✓
System restoration to pre-test state: removal of test files, software and account		✓
Vulnerability report (system generated)	✓	
Exploit reporting		✓
Detailed summary on overall security posture		✓
Customized remediation advice		✓

Immagine 2: **Tabella delle Attività**

Come si può osservare, un penetration test è significativamente più approfondito di un vulnerability assessment. Mentre un penetration test generalmente include una scansione automatica delle vulnerabilità iniziali, è lo sfruttamento manuale delle vulnerabilità che richiede una vasta gamma di competenze e tempi.

4. COS'È MEGLIO PER UN'AZIENDA?

4.1 VULNERABILITY ASSESSMENT

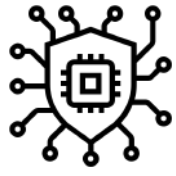
Pensiamo a un vulnerability assessment come ad una scansione automatizzata di alto livello, adattabile a pressoché qualsiasi contesto, che rileva le vulnerabilità più comuni. È più economico e più rapido, perché non richiede molte risorse e potrebbe essere considerato come un controllo dello stato di salute di una rete (come eseguire una scansione antivirus su un laptop, ma su un'intera rete).

Anche se un vulnerability assessment viene spesso condotto come attività obbligatoria nell'ambito del rispetto di specifici requisiti normativi (come ad esempio l'ISO 27001), si raccomanda vivamente l'esecuzione con una certa regolarità su tutti i nuovi dispositivi prima della loro distribuzione/attivazione, oltre che durante tutto l'anno (come fosse un'esercitazione antincendio).

4.2 PENETRATION TEST

Un penetration test è la differenza tra "spuntare una casella" ed essere sicuri di aver esaminato le vulnerabilità da ogni angolo. I test sono effettuati da professionisti che comprendono le sfumature di come funzionano le aziende. A differenza di un software di scansione automatica, possono porre domande quando qualcosa non sembra del tutto corretto.

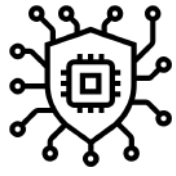
Proprio come l'esecuzione di un tagliando annuale su un'auto, si consigliano penetration test regolari per tutte le aziende, al fine di garantire una costante mitigazione del rischio.



5. COSA STIAMO VERIFICANDO?

Qualunque servizio si scelga, dipende dalla risorsa da testare; se la risorsa ha un valore basso (ovvero il compromesso non avrebbe un effetto devastante sulle operazioni o sulla reputazione), probabilmente un vulnerability assessment è adeguato.

Tuttavia, se la risorsa ha un valore elevato (ovvero una violazione o un blocco potrebbe causare interruzioni operative, perdite di entrate o danni alla reputazione), allora diventa un'attività primaria per professionisti delle minacce, che investono tempo nella ricerca di modi ingegnosi per compromettere e ottenere l'accesso.



6. RISULTATI

Entrambe le tecniche forniscono un rapporto dettagliato che spiega i risultati, le criticità delle vulnerabilità e i consigli per la risoluzione. Tuttavia, il vulnerability assessment non coprirà le informazioni sull'impatto o sullo sfruttamento delle vulnerabilità identificate, in quanto ciò può essere rilevato solo sfruttando le vulnerabilità manualmente.

È importante ricordare che nuove vulnerabilità vengono scoperte regolarmente, quindi se si è deciso che un vulnerability assessment o un penetration test sono la scelta migliore per le esigenze della propria organizzazione, dovrebbero essere ripetute **regolarmente**.

CONCLUSIONI

La sicurezza informatica è importante perché comprende tutto ciò che riguarda la **protezione** delle nostre informazioni personali, proprietà intellettuale, dati e sistemi informativi da furti e danni tentati da criminali e avversari.

A causa del massiccio aumento di tentativi di hacking, la sicurezza informatica è diventata un argomento di discussione inevitabile negli ultimi anni. Gli eventi che si verificano in questo settore possono avere conseguenze globali e la possibilità di risultati **catastrofici**.

Se un'organizzazione non dispone di professionisti nell'ambito della sicurezza delle informazioni, può assumere appaltatori esterni: esistono oggi numerose aziende IT specializzate in audit di sicurezza, vulnerability assessment e penetration testing che offrono piani completi per la sicurezza aziendale.