GRUPPO DI RICERCA AIEA
Roma 2004-2005

Il valore del Penetration Test dal punto di vista dell'auditor

Preparato da GDL
Versione 0.8 del 29/09/05

Prefazione

L'enorme evoluzione tecnologica delle telecomunicazioni, e la conseguente crescita di collegamenti in rete registrati nel recente passato, ha creato notevoli opportunità di sviluppo per i diversi attori, determinando (come accade di solito in contesti molto dinamici) anche le condizioni per un uso non sempre corretto dei nuovi strumenti a disposizione.

Ciò ha comportato, di riflesso, l'innalzamento del livello di attenzione ai problemi di sicurezza delle informazioni e delle relative applicazioni informatiche da parte delle strutture aziendali deputate alla loro gestione.

I rischi associati all'accesso non autorizzato alle reti comprendono infatti perdite economiche, furto di informazioni sensibili (personali o industriali), perdita di immagine aziendale o perdita di controllo dei sistemi informativi.

Nell'ambito della prevenzione di tali rischi e attività di ricerca e formazione su problemi di attualità svolte dall'Associazione Italiana Information Systems Auditors, è stato pertanto costituito un gruppo di ricerca con l'obiettivo di analizzare alcune tematiche relative all'audit dei presidi di sicurezza perimetrale delle reti aziendali.

L'indagine ha riguardato, in particolare, la modalità correntemente utilizzata per vagliare in modo sperimentale, la tenuta dei citati presidi, denominata "Penetration Test".

Ringrazio tutti i componenti del gruppo di ricerca per l'impegno e la disponibilità offerta nella realizzazione di questo documento:

Fabrizia Bilancini,
Piero Brunati,
Francesco Faenzi,
Enrico Recanatesi

Un ringraziamento particolare a Donatella Rosa per lo stimolo ed il coraggio profuso a tutti noi ed al nostro presidente, Silvano Ongetta, per la fiducia accordataci.

Stefano Silvestri

1. Scopo del Documento

Lo scopo del presente documento è quello di illustrare i risultati ottenuti dal Gruppo di Ricerca, stimolando nei lettori l'interesse all'argomento trattato ed agli opportuni approfondimenti.

2. Destinatari del documento

I destinatari naturali del documento sono gli Auditor che vi possono trovare, oltre ad un'esposizione razionale dei concetti ed un'omogeneizzazione delle definizioni, lo spunto per la pratica applicazione, nel proprio ambito lavorativo, delle metodologie illustrate.

L'auspicio è anche di fornire un contributo al mantenimento di un alto livello di guardia sul tema della sicurezza delle connessioni, un punto che appare particolarmente importante se si considera l'eccezionale espansione del fenomeno delle intrusioni indesiderate legate talvolta al semplice sfruttamento di tecniche di social engineering (e quindi di fenomeni non controllabili dal solo punto di vista esclusivamente tecnologico).

3. Articolazione del documento

Il documento si compone di una premessa, di una sezione **didattica**, ove sono esposte le definizioni, le vulnerabilità e le tipologie di attacco, seguita da una sezione **operativa**, nella quale sono raccolti i risultati dello studio: sono esposte dunque le principali tecniche di effettuazione dei PenTest, la loro utilità nell'ambito di un IT audit, i relativi rischi legali e le modalità di reporting dei PenTest.
Il documento contiene infine una sezione finale con le conclusioni del Gruppo di Ricerca.

Il Penetration Test – sezione didattica

4. Definizione e scopo del Pen Test

Il Penetration Test (in seguito PenTest), chiamato anche "Security Probe", è un'indagine sperimentale sulla sicurezza di un computer o di una rete, volta ad individuare vulnerabilità che potrebbero essere sfruttate in caso di tentativo di accesso non autorizzato e volta a testare i controlli che dovrebbero proteggere i computer e le reti da tali tentativi.

Il test è articolato sostanzialmente in due fasi:

1. l'esplorazione di tutti i presidi di sicurezza del sistema oggetto di verifica;
2. tentativo di violare quei presidi e di penetrare il sistema stesso (c.d. attacco).

Un'organizzazione può decidere di far eseguire il test ad un team interno, oppure ad un team di specialisti indipendenti esterni (il cosiddetto "**tiger team"**). In ambedue i casi, il team normalmente usa gli stessi metodi e strumenti utilizzati da chi porterebbe un attacco reale.
Al termine dell'investigazione, è presentato un rapporto sulle vulnerabilità individuate e sulle contromisure consigliate al Management per rendere il sistema e la rete più sicuri.

Il PenTest è pertanto un'attività volta ad ottenere informazioni, privilegi o a simulare il danneggiamento di sistemi informatici.
L'attività è svolta utilizzando tecniche generalmente più sofisticate di quelle comunemente in uso all'utente medio, con l'obiettivo di contribuire al miglioramento del livello di sicurezza dei sistemi esaminati.

Lo scopo principale è quello di fare emergere le falle del network o dei sistemi informatici oggetto del test, con particolare riguardo alla confidenzialità, all'integrità ed alla sicurezza dei dati e delle informazioni che vi risiedono.

Alcune delle possibili mancanze di sicurezza, nell'accesso ai sistemi informativi e alle reti del committente, possono riguardare:

- la rete Internet e gli altri punti di accesso elettronico, partendo da tecnologie implementate quali firewall, Virtual Private Networks, websites, ecc;
- i modelli procedurali, inclusa l'interazione umana (Social Engineering, Physical Intrusion, ecc.);
- gli accessi fisici, con particolare attenzione verso la sicurezza degli archivi e della documentazione, la simulazione di eventi naturali (power failure, incendi, allagamenti).

La differenza principale del PenTest, rispetto ad attività di hacking malevolo è che il primo è commissionato ed autorizzato da chi possiede legalmente i sistemi coinvolti.
Inoltre, mentre **l'auditor** ricerca estensivamente, attraverso un test, il maggior numero possibile di vulnerabilità, **l'hacker,** generalmente, ricerca una specifica debolezza della rete, utile a perseguire i suoi obiettivi.

5. Gli attacchi e le vulnerabilità

Per attacco si intende generalmente la vera e propria attività di testing che si sostanzia in vero e proprio tentativo di "hacking" del sistema/i oggetto di verifica, al fine di individuare le vulnerabilità; cioè le debolezze e/o le lacune nella sicurezza di tali sistemi.

Di seguito sono elencate le più frequenti tipologie di attacco.

Covert /Overt

In un PenTest "covert" (letteralmente "dissimulato"), il PenTester adotterà delle precauzioni per non far rilevare l'attacco, o quantomeno per nasconderne la provenienza reale. In questo caso, gli addetti all'amministrazione dei sistemi coinvolti non sono preventivamente informati dell'attività, potendo così verificare l'efficacia delle misure predisposte in caso di attacco o incidente (Incident Response).
Al contrario dei Tecnici, il Management sarà costantemente informato dell'andamento dell'attività.

Opposto a "covert" è il PenTest di tipo "overt", letteralmente "evidente". In questo caso, il vantaggio sta nella possibilità dei Tecnici di analizzare l'attacco in corso, senza dover procedere ad una più complessa analisi a posteriori (Forensic Analisys).

Blind

Letteralmente "cieco", un PenTest "blind" non si agevola di informazioni "elargite" dal committente, simulando così un attacco di chi non ha informazioni interne o privilegiate.
Questo porta vantaggi e svantaggi e, spesso, la scelta di operare un PenTest "blind" è conseguenza della necessità di ottenere un'attestazione da parte di enti esterni.

Si tenga presente che, di norma, ad un PenTest è dedicato un periodo di tempo limitato, solitamente misurabile in giorni o settimane, mentre un malintenzionato, spesso, non si pone limiti di tempo e di tecniche (compreso il Social Engineering) per ottenere informazioni dall'interno, sempre che non abbia agganci o provenga proprio dall'interno.

Fra gli analisti del settore è opinione comune (ed i rilevamenti statistici lo confermano) che la maggior parte degli attacchi provenga direttamente o indirettamente dall'interno. E' quindi evidente che un PenTest "blind" contribuirà in misura limitata al miglioramento del livello di sicurezza.

In base all'oggetto/finalità della verifica è possibile distinguere tra le seguenti tipologie di PenTest.

Penetration test da Internet

Il Penetration Test condotto da Internet ha come oggetto dell'attacco i servizi pubblici dell'azienda (es. Mail, Web, Ftp, Dns, Firewall).

Il Penetration Test serve a determinare se:
- i dati aziendali possono essere rubati o modificati;
- i sistemi critici possono essere compromessi;
- la rete non è disegnata correttamente;
- i sistemi non sono configurati correttamente;
- il firewall non è configurato correttamente.

Inoltre il Penetration Test da Internet ha l'obiettivo di valutare se le protezioni e i controlli siano efficaci a prevenire un attacco condotto internamente.
Gli scenari possibili sono due:

- l'attacco è condotto da hacker esterni che tuttavia potrebbero – anche solo temporaneamente - aver avuto accesso alla rete interna;
- l'attacco è condotto da utenti legittimi dell'Azienda (es: dipendenti, consulenti) in grado di ottenere l'accesso alla rete aziendale e/o a funzioni critiche del sistema informativo.

Statisticamente questo tipo di attacco è estremamente diffuso (abuso di privilegi) e pericoloso (utenti interni disonesti conoscerebbero la locazione dei dati critici e saprebbero monetizzarne più facilmente una relativa violazione).
Tutti i test sono effettuati in modo tale da **non compromettere le funzionalità** dei servizi aziendali oggetto dell'attacco.

Wardialing penetration test
L'attività di wardialing consiste nell'effettuare un test di accesso alle linee telefoniche aziendali al fine di identificare apparecchiature (modem, fax, centralini, ecc.) non autorizzati o male configurati.
La protezione, svolta dai sistemi di difesa perimetrale (Firewall, ecc.), risulterebbe di fatto annullata se un hacker riuscisse a connettersi ad un modem allacciato ad un computer in rete.
L'attacco telefonico o wardial consiste in diverse fasi:
- scan dello spazio telefonico e riconoscimento modem/fax/voce;
- identificazione dell'apparato connesso al modem (es: access server, unix server, RAS, ecc.);
- tentativo di accesso alla risorsa attraverso "password guessing", password di default, errori di configurazione;
- accesso alla risorsa;
- reporting.

Web Application penetration test
Le applicazioni web (WWW) sono di norma strutture assai complesse e includono componenti software di vario tipo. Tipicamente queste risiedono sul web server, sull'application server, su database di vario genere e, infine, sui sistemi di backend aziendali.
Spesso le singole componenti dell'applicazione web sono sviluppate, supportate e mantenute da diversi attori e strutture di una stessa azienda.
Sebbene il termine "applicazione" tenda a connotare una singola entità funzionale, in realtà le applicazioni web si compongono di tanti parti di

codice, spesso provenienti da differenti vendor e/o sviluppatori di terze parti.
Per questo motivo rendere sicura un'applicazione web può richiedere la completa visibilità dei flussi informativi aziendali e capacità tecniche non comuni.

Il penetration test di un'applicazione web è uno strumento utile per identificare, con una metodologia chiara ed esaustiva, le possibili minacce e le relative soluzioni.

Wireless penetration test
I segnali di una scheda wireless sono in grado di coprire distanze consistenti e in molti casi la copertura del segnale va oltre i confini fisici dell'Azienda.
È facile trovare Access Points Wireless del tutto insicuri e configurati inadeguatamente.
Situazioni di questo tipo permettono ad un potenziale hacker di potersi connettere alla rete Aziendale senza lasciare alcuna traccia fisica di accesso all'edificio dell'Azienda.

Provenienza dell'attacco
Secondo la provenienza dell'attacco il PenTest può essere:

- **esterno** è eseguito su reti pubbliche (TCP/IP dedicate, reti Frame Relay, telefoniche, satellitari, ecc.) o su reti private con uscita pubblica (Internet, X.25/X.121, DECnet, modem/numeri verdi, RAS, wireless, ecc.);
- **interno** è eseguito su internal LAN (via RAS o presso il committente), LAN to LAN private, LAN to LAN pubbliche.

Penetration test esterno
Prevede l'attacco alla rete di una azienda (con bersagli specificati o meno) da una o più reti esterne e può essere utilizzato in tre diverse modalità:

1. ***Surface mode (Network Scanning/Penetration)***

L'attacco consiste nella scansione dei bersagli con diversi network e host scanner; nell'analisi delle vulnerabilità riscontrate su ogni

bersaglio, nello sfruttamento delle vulnerabilità per ottenere l'accesso non autorizzato alla rete dell'azienda.

2. ***Advance Mode (Social Engineering + Network Scanning/Penetration)***

L'attacco consiste nell'impiego delle tecniche e tecnologie adottate nel Surface Mode, nell'ottenere informazioni sensibili dalle componenti che si interfacciano con la rete bersaglio (personale interno/esterno, consulenti, fornitori, clienti, partner commerciali), nell'attacco ad eventuali network che si interfacciano con la rete bersaglio.

3. ***Total Mode (Trashing + Social Engineering + Network Scanning/Penetration)***

L'attacco consiste nell'impiego delle tecniche e tecnologie adottate nel Surface e Advanced Mode, nell'ottenere informazioni sensibili attraverso l'individuazione, il recupero e l'analisi dei rifiuti aziendali provenienti dall'azienda bersaglio.

Social engineering

Il social engineering è stato definito come "l'abile manipolazione di una popolazione tramite la disinformazione al fine di ottenere un cambiamento desiderato nelle abitudini e nelle tendenze della stessa popolazione".
Nel contesto di un security penetration testing, il social engineering é utilizzato per descrivere l'acquisizione di informazioni sensibili o di impropri accessi privilegiati ai sistemi da parte di un hacker, stabilendo ingannevole relazioni di fiducia con persone all'interno dell'organizzazione obiettivo dell'attacco.
Tali tecniche possono essere usate per ottenere fraudolentemente informazioni confidenziali, quali user-id, passwords, numeri telefonici interni, informazioni personali o qualsiasi altra informazione utile.

Penetration test interno

Prevede l'attacco alla rete bersaglio da una posizione privilegiata dell'attaccante: questo tipo di attacco presuppone una volontà del Management di voler verificare l'effettiva capacità di difesa da una minaccia dall'interno della propria azienda.

Il Management decide una collocazione aziendale di partenza ed ufficialmente assume l'attaccante, inserendolo nel contesto aziendale come un normale dipendente. L'attaccante è, a tutti gli effetti, una risorsa dell'azienda e, come tale si può avvalere delle strutture e degli strumenti aziendali, per verificare le difese interne del network bersaglio.

Il Management può decidere la durata di assunzione dell'attaccante e il settore aziendale (quindi gli strumenti aziendali assegnati) in cui impiegarlo. Il Management può inoltre decidere di specificare il raggiungimento di un determinato bersaglio interno o può richiedere la raccolta di tutte le informazioni ottenibili.

Il Penetration Test – sezione operativa

6. Tecniche e strumenti di un Pen Test

Gli strumenti utilizzabili dai PenTester sono veramente molti e soprattutto in continua evoluzione.

Farne un elenco, in questa sede, lo renderebbe obsoleto in brevissimo tempo, quindi si preferisce indicare le principali fonti per la ricerca.

La fonte principale è sicuramente Internet in quanto, proprio per la velocità di evoluzione di tali strumenti, è l'unico mezzo in grado di esserne al passo nella pubblicazione e divulgazione.

Per farsi quindi un'idea dei principali strumenti un buon punto d'inizio è la lista mantenuta da Fyodor su http://www.insecure.org/tools.html, proseguendo su PacketStorm (http://www.packetstormsecurity.org) e su SecuriTeam (http://www.securiteam.com/).

Nell'allegato "Riferimenti" è riportato un elenco delle fonti principali disponibili alla data della redazione del presente documento.

7. Obiettivi e modalità di esecuzione di un PenTest nell'ambito dell'IT Audit

OBIETTIVI

L'obiettivo di un PenTest nell'ambito di un audit dei sistemi informativi è quello di verificare che il funzionamento di componenti specifiche (singole o come insieme) del sistema di sicurezza di un network o di un sistema informativo raggiunga livelli standard predefiniti (quali possono essere, ad esempio, quelli previsti da ISACA[1]) o rispetti le politiche e procedure aziendali.

Il PenTest, in relazione ad un processo di audit, costituisce un test di verifica finalizzato alla conferma dei possibili rischi individuati

[1] Vedi standard ISACA 060.010; 060.020.

dall'attività di IT audit tradizionale o di un Vulnerability Assessment (VA).

Infatti il limite maggiore di un PenTest, dettato da motivazioni legate al rapporto costi/benefici dell'esercizio, è quello dell'impossibilità di identificare tutte le principali debolezze.

Pertanto, al fine di sfruttare al massimo i benefici di un PenTest, questo andrebbe inserito in un contesto più ampio di individuazione, tramite procedure di Risk Assessment, IT Audit e Vulnerability Assessment, di potenziali debolezze nella sicurezza, da confermare tramite un PenTest mirato.

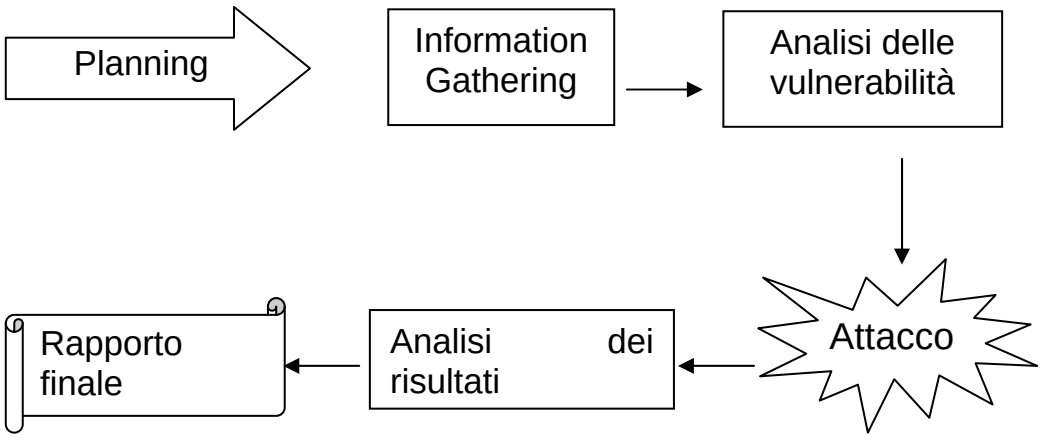
E' pur vero che, generalmente, il PenTest contribuisce ad aumentare la consapevolezza circa i problemi sulla sicurezza nel Top Management aziendale, il quale, non sempre, è in grado di valutare correttamente i rischi legati alla sicurezza informatica.

Il PenTest, in alcuni casi, può essere un utile strumento per portare all'attenzione della Direzione tali problematiche, tramite l'evidenza di reali intrusioni all'interno del sistema (p.e. dimostrando di aver ottenuto l'accesso ad informazioni riservate).

In sintesi, l'obiettivo di un PenTest, nell'ambito dell'IT Audit è quello di evidenziare e/o confermare eventuali debolezze specifiche nella sicurezza informatica, non quello di essere un esame omnicomprensivo della stessa.

Fasi del PenTest

Le fasi che compongono un PenTest possono essere sintetizzate come segue:



Pianificazione

Di solito viene effettuato un kickoff meeting per organizzare il lavoro individuando scopo ed obiettivi, parti coinvolte, modalità, tecniche ed approcci del PenTest, tempistica di esecuzione.

Information Gathering

Questa fase ha lo scopo di ottenere le informazioni relative al sistema informativo o al network: principali funzionalità, router, firewall, ecc. utilizzando classici tools TCP/IP standard (traceroute, whois, ipindex, ecc.). La quantità di informazioni raccolte dipende dal tipo di approccio prescelto.

Durante la fase di Information Gathering viene disegnata una vera e propria mappa del sistema informatico ambito del PenTest, ricostruendone la logica e la struttura con l'aggiunta di informazioni sul livello di sicurezza, particolari applicazioni software installate, marche e tipologie di sistemi operativi o "memo" su azioni da effettuarsi successivamente: l'obiettivo è ovviamente quello di farsi un'idea completa della rete oggetto delle operazioni di verifica (laddove il security probe richiesto riguarda un'intera rete dati e non singole macchine o segmenti di rete, DMZ etc...).
Gli scanning di controllo hanno come obiettivi i servizi e le porte accessibili, le trust relationship sfruttabili, i bug software - conosciuti e non - e gli errori di configurazione, mediante azioni di scansione automatiche e manuali: l'obiettivo finale è comunque sempre quello di compromettere la rete e fare venire a galla le debolezze/mancanze di sicurezza, per pianificare poi unitamente alla Direzione Sistemi Informativi un technical assessment più dettagliato sull'infrastruttura.

Per quanto riguarda tale fase di raccolta delle informazioni, sviluppata con strumenti tecnologici o meno e secondo gli "accordi" tra le parti (management e team di PenTester), si evidenzia come spesso si scelga di non dare ai PenTester informazioni preventive che agevolino il test, adducendo a giustificazione l'obiettivo di verificare la tenuta dei sistemi contro hacker occasionali.

Non vi è nulla da eccepire in questa scelta, tuttavia va considerato che:

- la maggior parte degli attacchi mirati avviene disponendo direttamente o indirettamente di informazioni provenienti dall'interno;

- ogni giorno vengono pubblicate vulnerabilità già scoperte in precedenza e disponibili nei canali underground (come ad esempio i cosiddetti Traderz). Difese perimetrali che, alla luce del miglior PenTest oggi sono sicure, potrebbero non esserlo domani (prima del prossimo PenTest): quando un hacker ha passato la barriera perimetrale, come prima cosa cerca di ottenere informazioni dall'interno e proseguire la sua "scalata" ai privilegi;
- i PenTester per motivi ovvii si pongono limiti di tempo e di risorse che gli hacker normalmente non hanno.

Il PenTest ha lo scopo ultimo di **migliorare** le difese del sistema analizzato: perché non dare all'auditor le informazioni che gli permettono di essere più efficiente nel trovare un maggior numero di vulnerabilità e quindi nell'aumentare la sicurezza di tali sistemi?

Analisi delle vulnerabilità

Durante questa fase si determinano eventuali problemi di sicurezza rilevati durante la raccolta dei dati. Tale fase produce quindi una lista di obiettivi da investigare in profondità. Vengono utilizzati tools TCP/IP standard e non (portscanner, vulnerability tools, ecc.).
E' possibile determinare ulteriori specifici obiettivi che contribuiscano al raggiungimento dello scopo finale.

Attacco

E' la fase di penetrazione nel sistema "sotto indagine" con lo scopo di ottenere, se possibile, pieni privilegi di sistema. In questa fase vengono dunque utilizzate esclusivamente le tecniche, gli strumenti e le metodologie concordate con il committente, evitando in genere test con attacchi di tipo DoS (Denial of Service), la cancellazione di dati o l'alterazione dei file di log.

L'attacco è condotto generalmente con gli stessi strumenti che userebbe un malintenzionato, salvo i casi in cui si potrebbe provocare un indesiderato disservizio.
In questi casi si procede alla segnalazione della vulnerabilità potenziale ancora "da verificare" e potrebbe quindi trattarsi di un "falso positivo" (falso allarme).

Occorre sottolineare che pianificando ed accettando la possibilità di produrre disservizi si ottenga un risultato molto più preciso, con falsi allarmi molto limitati.

Potendo invece solo supporre, senza verificare la presenza di alcune vulnerabilità, sarà necessario un maggior lavoro a posteriori per verificarne l'effettiva presenza.

Un PenTest, a differenza di un Vulnerability Assessment, non sempre ha l'obiettivo di segnalare tutte le vulnerabilità incontrate, reali o potenziali che siano.
Obiettivo di un PenTest classico, a meno che non venga esplicitamente previsto nell'incarico, è infatti quello di dimostrare o meno la penetrabilità di un sistema. Se ciò è ottenuto sfruttando uno fra molti bachi presenti, quello sfruttato sarà tipicamente **l'unico** segnalato.

Analisi dei risultati e rapporto finale
Conclusi i test, si procede all'analisi dei risultati ed alla stesura del rapporto finale da consegnare al committente, inserendo tutte le informazioni relative al lavoro svolto ed ai risultati raggiunti, incluse le attività da porre in essere per superare le vulnerabilità evidenziate.

La documentazione delle evidenze dei problemi riscontrati è essenziale, in quanto rappresenta la documentazione di audit e supporta il lavoro fatto ed i risultati dei test.

Eventuale "pulizia" delle tracce nei sistemi analizzati
Se previsto negli accordi tra le parti, il PenTester procede con la pulizia/rimozione delle tracce lasciate nei sistemi attaccati.
Questa attività, più o meno onerosa a seconda di molti fattori difficilmente prevedibili, può essere utile per dimostrare l'efficacia dei sistemi di logging (IDS, Syslog Servers, ecc.), così utili in caso di analisi postume (Forensic Analisys) o necessità di documentare denunce alle forze dell'ordine per agevolarne le ricerche.
Se la pulizia delle tracce non fosse prevista nell'incarico, il PenTester dovrebbe almeno fornire al Committente la documentazione per farlo in maniera autonoma.

Modalità di esecuzione del PenTest
Vi sono numerosi approcci per lo svolgimento di un Penetration Testing.
Tali approcci, in relazione alle circostanze, influiscono sul livello di sicurezza rilevato dal review, sui rischi legati all'esecuzione del PenTest, sui tempi di esecuzione e sui costi.

Il Management IT, committente del PenTest, dovrebbe attentamente valutare le diverse alternative, scegliendo quella che fornisce il maggior livello di assurance, collegato ed un livello di rischio operativo accettabile.

Gli approcci di PenTest sono anche definiti come:

zero-knowledge:
il team non ha alcuna informazione circa l'ambiente in cui dovrà eseguire il test. Tale tipologia è adottata per rendere il test più realistico possibile;

partial-knowledge:
il team dispone di alcune informazioni quali solitamente policy, documentazione sul network, inventario degli asset aziendali. In genere tale tipologia di attacco può essere scelta se si vuole testare specificatamente qualcosa, consentendo il risparmio, in parte, di tempo e costi;

full-knowledge:
il team dispone di un'informazione completa dell'infrastruttura aziendale e tecnologica e del business, simulando in tal modo un attacco proveniente dall'interno dell'azienda.

A questo proposito è utile notare che il PenTest è spesso eseguito per due motivi:

- innalzare il livello di consapevolezza del management sui temi di sicurezza IT, oppure
- testare le possibilità di accesso non autorizzato e le capacità di risposta.

Se l'obiettivo è quello di determinare tutte le debolezze ragionevolmente possibili, un assessment diagnostico "full knowledge" è da preferire. Il PenTest è spesso usato nelle aziende per confermare e giustificare gli stanziamenti di budget necessari per correggere le carenze di sicurezza, identificate attraverso un IT audit.

Tempi e Costi

I tempi ed i costi dei PenTest variano, sia per motivi "quantitativi" (numero ed estensione dei sistemi da verificare), sia per la tipologia del PenTest eseguito. I costi del review sono, infatti, influenzati dai tempi materiali di esecuzione del PenTest, e dal diverso livello di preparazione richiesto ai PenTesters, i quali devono avere specifiche conoscenze nella sicurezza e nell'amministrazione dei sistemi (sistemi operativi, apparati e protocolli di rete, database, ecc.).

Ulteriori elementi che influiscono su tempi e costi sono i seguenti:

Apparecchiature da verificare

Il caso più comune è il test di sistemi che forniscono servizi tramite Internet, come ad esempio WEB Server, Mail Server, Server di autenticazione, Commercio Elettronico, Applicazioni WEB, Apparati di rete (Router, Firewall, IDS, ecc.) o altri sistemi analoghi.

Oltre a questi tipi di sistemi, può essere utile verificare altri tipi di apparecchiature come ad esempio, sistemi interni di backup, stampanti, centralini telefonici, apparati wireless o bluetooth, ponti radio, telefoni cellulari e persino contatori dell'energia elettrica.
In sostanza, tutto quello che è attaccabile può essere oggetto di un PenTest, variando conseguentemente risorse, modalità, tempi e costi.

Provenienza del PenTest

Ad esempio, nel caso di una DMZ (Zona Demilitarizzata, ovvero sottorete circoscritta in cui sono racchiusi alcuni computer critici), gli attacchi possono provenire da Internet, dalla rete interna, o anche da sistemi eventualmente compromessi all'interno della DMZ stessa.
In questi casi il PenTest deve essere eseguito fisicamente dall'interno della DMZ ed ha modalità di esecuzione sensibilmente diverse in quanto l'auditor dovrebbe preferibilmente operate dall'interno dell'azienda, in prossimità dei sistemi oggetto del test.

Esaustività

Nel caso di un numero elevato di sistemi da verificare, specie se simili, tempi e costi possono essere ridotti eseguendo controlli "a campione", cercando di trovare un compromesso ragionevole che fornisca un

risultato significativo. Il campione deve essere il più possibile rappresentativo, perciò generalmente si scelgono delle "porzioni" logiche significative quali, ad esempio:

- un sub-network (la DMZ citata sopra, un singolo ufficio, fabbricato o data center, un dominio od un gruppo omogeneo di servers);
- un'applicazione con tutte le sue componenti (il sistema applicativo, il suo database, il sistema operativo sui quali risiedono e le varie componenti software ed hardware a supporto);
- un singolo componente od una famiglia di componenti di rete (il firewall, il sistema operativo "xyz" di una specifica versione, il web od il mail server, il sistema vPN od il file repository).

Tali elementi si influenzano fra di loro e difficilmente assistiamo a due PenTest uguali, a meno che non siano attività eseguite in serie su siti ed apparecchiature analogamente predisposte.

Come anticipato, il PenTest può essere svolto da personale dell'azienda, oppure commissionato a terze parti, in genere gruppi di esperti conosciuti come Tiger Team.

Fare eseguire il test da un **team interno** è una soluzione che può comportare i seguenti vantaggi e svantaggi per l'azienda:

Vantaggi

- Minori costi (o comunque più difficilmente quantificabili)
- Maggiore conoscenza della rete e dei sistemi informativi
- Maggiore flessibilità e rapidità nell'implementare le azioni correttive

Svantaggi

- Minore specializzazione e necessità di aggiornamento continuo in relazione agli sviluppi tecnologici
- Possibili danneggiamenti del sistema informatico
- Possibile conflitto d'interesse, in quanto il team, nella maggior parte dei casi, dipenderebbe dalla stessa funzione aziendale (i Sistemi Informativi)

Fare eseguire il PenTest da **terze parti** può comportare i seguenti vantaggi e svantaggi:

Vantaggi

- Maggiore imparzialità

- Uso di tecniche "Hacker", meno convenzionali
- Mancanza di possibili conflitti d'interesse ed una sorta di "attestazione" da parte di un terzo che fornisce maggiori garanzie agli stakeholders
- Mancanza di condizionamenti e preconcetti
- Maggiore specializzazione e aggiornamento

Svantaggi

- Accesso da parte di terze parti ad informazioni sensibili dell'organizzazione
- Maggiori costi (anche se certi e normalmente predeterminati)
- Minore conoscenza della rete e dei sistemi informativi
- Risultati normalmente disponibili solo alla fine delle verifiche

La scelta del tipo di PenTest da effettuare deve comprendere l'analisi della documentazione del PenTest offerto: nella documentazione del PenTest, per poterne valutare l'attendibilità, dovrebbero essere indicati gli strumenti utilizzati ed i limiti a cui è sottoposto, compresi quelli derivanti dal budget.

Il PenTest non è sempre il migliore strumento possibile per individuare tutte le carenze di sicurezza. Un assessment delle reti, che includa un attenta review diagnostica dell'architettura IT e di rete è facilmente in grado di identificare più carenze di un tool commerciale di PenTest.

Il mercato ufficiale offre, infatti, pacchetti commerciali di PenTest (c.d. vulnerability scanner) ad un costo predeterminato e limitato. In effetti, questa pacchettizzazione può, in molti casi, soddisfare le verifiche di vulnerabilità rispetto ad attacchi generalizzati del momento (es. Worm, ecc.), ma non è molto efficace contro attacchi specifici e potrebbe non soddisfare gli obiettivi del committente.

L'esperienza di alcuni PenTest porta a non utilizzare, per proprio standard interno, pacchetti di tipo "commerciale", preferendo concetti quali "I learn on my own", "Ethical Hacking" ed "Hands on", producendo internamente la maggior parte dei tool ed effettuando un aggiornamento continuo grazie al lavoro di ricerca e sviluppo (Security R&D) e ad un confronto diretto con i pacchetti proposti dal mercato, ufficiale e non.

E' infine necessaria una considerazione sulla validità temporale del Penetration Test: il PenTest è una "**foto istantanea**" del livello di

sicurezza dei sistemi informativi e delle reti. Per questo, il test si limita ad evidenziare carenze riferite alla esistente, al momento configurazione di rete.

Che il PenTest sia stato negativo oggi, non consente di escludere che nuove carenze emergano successivamente, infatti il fatto che il team di PenTester non abbia scoperto vulnerabilità della rete non significa che altri (hacker) non lo abbiano fatto o lo faranno.

Questo perché i sistemi informativi sono in continua evoluzione:
- gli antivirus sono cambiati anche più volte nel corso di una giornata
- i sistemi operativi, le applicazioni, i database e tutte le varie componenti software sono continuamente oggetto di patches, upgrades od aggiornamenti di release
- nuovi componenti hardware e software vengono installati o sostituiti (una workstation, un router od un hub)
- i sistemi stessi vengono mantenuti e modificati

Tutto ciò contribuisce a modificare l'equilibrio dal quale dipende il grado di sicurezza di uno o più sistemi, per cui delle vulnerabilità possono essere introdotte.

6. Rischi legali, contrattuali e normativi

I rischi legali sono legati alla natura dei dati e delle informazioni di cui gli strumenti di difesa oggetto di test sono a protezione. Tali dati potrebbero essere quindi letti, copiati o, nella peggiore delle ipotesi, distrutti nel corso del test.
Tali rischi dovrebbero essere evidenziati nel lettera d'incarico ed il management deve darne manleva all'esecutore del test.

Nel presente capitolo si espongono i contenuti del cosiddetto Disclaimer, cioè il documento che descrive i termini delle attività specialistiche finalizzate alla ricerca ed analisi di vulnerabilità nei sistemi Internet, di seguito indicate come attività VA/PenTest (Vulnerability Assessment & Penetration Testing).

In particolare il Disclaimer intende acquisire dal soggetto committente il suo consenso circa i *possibili rischi* associati allo svolgimento di attività di VA/PenTest.

L'elenco dei principali punti che il Disclaimer dovrebbe considerare, e sui cui l'auditor e l'auditee dovrebbero convenire, è descritto di seguito.

Regole di ingaggio

Le "regole di ingaggio" documentano le procedure e le modalità che dovrebbero essere adottate per l'analisi e la verifica delle vulnerabilità dei sistemi Internet dell'auditee.

L'attività di VA/PenTest dovrebbe innanzitutto essere limitata ad un preciso periodo.

Il soggetto auditee e l'auditor dovrebbero collaborare al raggiungimento del risultato accettando integralmente le regole di ingaggio, che costituiscono una sorta di "autorizzazione a procedere", soprattutto se l'auditee è formalmente incaricato della responsabilità degli asset sottoposti al VA/PenTest.

Obiettivi

L'auditor effettuerà la ricerca e l'analisi delle vulnerabilità del sistema informatico dell'auditee con lo scopo di verificare la possibilità di accedere ed utilizzare in modo non autorizzato risorse ed informazioni critiche dell'auditee.

In questo scenario, le regole di ingaggio descritte nel Disclaimer sono necessarie per assicurare la conduzione della verifica in modo da minimizzare l'impatto sull'operatività dell'auditee e massimizzare il valore della verifica stessa.

Resta chiaro all'auditee che alcuni inconvenienti si potrebbero verificare anche durante la sua operatività, e ciò nonostante il massimo impegno dell'auditor a limitare tali inconvenienti.

L'auditor deve inoltre impegnarsi, nel caso di eventuali danni o cambiamenti che dovessero emergere a seguito dell'attività di testing, a fornire tutte le indicazioni, dai dettagli sulle procedure effettuate ai risultati ottenuti, al fine di ripristinare la situazione preesistente.

Scopi del test

Segue un esempio di elenco di condizioni tipo che definiscono gli scopi del test.

1	Le procedure adottate dall'auditor per il test esterno sono configurate per verificare la possibilità di penetrare dall'esterno (via internet e/o dial-up) la rete ed i sistemi dell'auditee attraverso l'utilizzo congiunto di strumenti di scansione automatici ed operazioni manuali.
2	Le procedure adottate dall'auditor per tutti i test concordati con l'auditee utilizzano tecniche non distruttive limitate alla visualizzazione delle informazioni. Nessun file o dato sarà intenzionalmente modificato, distrutto o cancellato nel corso delle sessioni di test. L'evidenza delle vulnerabilità sarà limitata al salvataggio delle schermate video ed alle informazioni dei log. Il successo dell'intrusione è definito dal verificarsi di una delle seguenti condizioni: ▪ ottenere la possibilità di copiare, modificare o cancellare, localmente o da remoto, i file di configurazione dei sistemi (in nessun caso i file saranno modificati o cancellati); ▪ ottenere la possibilità di visualizzare o modificare le password dei sistemi; ▪ ottenere la possibilità di deviare il traffico di rete (in nessun caso il traffico di rete sarà deviato).
3	L'auditor utilizzerà strumenti di war-dialing per tentare di ottenere l'accesso non autorizzato all'infrastruttura di rete dell'auditee.

Pianificazione

L'auditor dovrebbe condurre i test secondo la pianificazione precedentemente concordata con l'auditee. Riportiamo di seguito un esempio:

Dal	Al	Tipo di test (interno/esterno/sistema)
		Indagine preliminare
		Prima scansione automatica del perimetro
		Seconda scansione automatica del perimetro
		Verifica manuale delle vulnerabilità
		Scansione automatica e verifica interna
		Analisi dei log (firewall e, IDS)

Modalità di esecuzione dei test

L'esecuzione dei test dovrebbe avvenire nel rispetto di alcune indicazioni prevedendo, se applicabile, una procedura abbreviata di eventuale revisione delle stesse, nel caso queste comportino un limite eccessivo alla finalità delle verifiche durante l'esecuzione.

Dovrebbero essere inoltre concordata preventivamente l'eventuale assistenza (modalità e tempistiche) da parte del personale tecnico del committente, se richiesto dalla tipologia delle verifiche.

Descriviamo di seguito un esempio di tali indicazioni.

1	Tutte le procedure automatiche di intrusione e le scansioni sulla rete saranno condotte esclusivamente nei periodi stabiliti nel paragrafo "Pianificazione".
2	La prima scansione automatica sarà condotta fuori le normali ore di lavoro (dalle 23:00 alle 05:00) ed includerà la verifica dei Denial of Service.
3	La seconda scansione automatica sarà condotta durante le normali ore di lavoro (dalle 09:30 alle 17:00) e non includerà la verifica dei Denial of Service.
4	L'auditor non effettuerà attacchi di negazione di servizio (DoS) al di fuori di quanto concordato precedentemente. Non rientrano in questa categoria eventuali problemi dovuti ad overflow dei log di sistema.

5	I test di intrusione manuali, esterni ed interni, saranno condotti durante le normali ore di lavoro (dalle 09:30 alle 17:00).
6	Nessun indirizzo IP (o numero di telefono) sarà escluso dalle operazioni di test.
7	L'auditor effettuerà i test utilizzando equipaggiamenti e risorse proprie, attivate e gestite solo ed esclusivamente dallo staff dell'auditor incaricato del test.
8	Sarà mantenuto un giornale delle attività di intrusione durante tutto il periodo di test.
9	L'intenzione dell'auditor e dell'auditee è di condurre l'analisi in modo controllato, minimizzando i disservizi all'utenza durante tutto il periodo di test. L'auditee è comunque consapevole che questi test possono involontariamente causare il *crash* o il *reboot* dei sistemi ed accetta la propria piena responsabilità relativamente ai rischi potenziali ed alle attività necessarie per il ripristino delle funzionalità degradate.

Durante i test di intrusione, l'auditor dovrebbe attenersi a precise regole volte a minimizzare l'impatto sull'infrastruttura dell'auditee. Se ne riporta un esempio:

1	Non saranno utilizzati strumenti o tecniche non precedentemente testati.
2	Nessuna modifica sarà apportata ai file contenuti nei sistemi dell'auditee; questi potranno essere visualizzati al solo scopo di dimostrare l'esistenza di vulnerabilità.
3	L'auditor si adopererà in modo da ridurre al minimo il rischio di blocco delle *user-id*, sia delle utenze dell'auditee, sia relative all'amministrazione o gestione dei sistemi, impegnandosi ad informare tempestivamente l'auditee in caso di blocco accidentale delle password per il ripristino dell'accesso.

4	Ogni sistema su cui l'auditor otterrà l'accesso potrà essere utilizzato, nel corso del test, per ottenere l'accesso ad altri sistemi dell'auditee, sfruttando le relazioni di fiducia col sistema compromesso.
5	File ed informazioni contenute sui sistemi informatici dell'auditee saranno trattati dall'auditor secondo le vigenti norme in materia di riservatezza e confidenzialità od, alternativamente, secondo le specifiche esigenze del committente, se più stringenti. In particolare, l'auditor si impegna a non divulgare a terzi informazioni o file dell'auditee di cui sia venuto a conoscenza e/o in possesso durante l'attività di intrusione. I risultati del test saranno consegnati, in formato elettronico e cartaceo, esclusivamente nelle mani del destinatario dell'Audit Report.
6	Le attività di scansione automatica e manuale saranno svolte esclusivamente da sistemi i cui indirizzi IP saranno preventivamente comunicati.

Durante i test di intrusione l'auditee si dovrebbe impegnare ad osservare opportune regole, volte a consentire la buona riuscita dei test. In particolare:

- l'auditee si impegna a non utilizzare, durante il periodo di test, strumenti o procedure estranee all'architettura di sicurezza correntemente in produzione che possano pregiudicare il risultato dell'analisi, arrecare danno o sottrarre informazioni ai sistemi utilizzati per condurre le operazioni di verifica;
- l'auditee condivide con l'auditor la responsabilità della buona riuscita del test assicurando:
  - la disponibilità di tutte le informazioni necessarie per la corretta configurazione degli strumenti di scansione. Tali informazioni dovrebbero essere concordate preventivamente e la loro natura ed ampiezza conformi alla tipologia di test (ad esempio "open" o "blind";
  - l'operatività e la disponibilità delle reti e dei sistemi nei periodi concordati per le operazioni di test;
  - la corretta comunicazione agli amministratori ed operatori responsabili delle reti e dei sistemi oggetto dell'analisi e la loro consapevolezza circa gli impatti che l'analisi potrebbe avere su reti e sistemi da loro gestiti;

- la presenza e la disponibilità di risorse adeguate al ripristino delle funzionalità degradate durante le operazioni di test;
- l'individuazione, per ogni sito oggetto dell'analisi, di un riferimento tecnico in grado di fornire o recuperare tutte le informazioni necessarie alla buona riuscita delle operazioni di test.

Procedure di notifica

L'auditor potrebbe essere incaricato di coordinare un gruppo di lavoro per le attività di VA/ PenTest. In tal caso egli è il punto di riferimento per l'auditee.
L'auditee potrebbe avere la facoltà di *bloccare* ogni attività ritenuta non conforme allo scopo del test o che ritiene non sia correlata con il test in corso. In quest'ultimo caso l'auditee è tenuto ad informare l'auditor per concordare le azioni da intraprendere.
L'auditor si dovrebbe impegnare ad informare tempestivamente l'auditee (via eMail, SMS, ecc.) qualora siano rilevate situazioni od eventi che possano risultare bloccanti per le funzionalità dei sistemi. Altresì l'auditor dovrebbe notificare i casi in cui le attività di "intrusione" portino ad ottenere accesso fortuito a sistemi esterni al perimetro di intervento. Ciò al fine sia di concordare un eventuale allargamento dello scope, sia di permettere al committente di provvedere ad eventuali azioni correttive.

Proprietà dei risultati

Al termine dell'attività sarà prodotto un Audit Report.

In virtù della funzione aziendale che l'auditor ricopre, è chiaro che l'auditee lo autorizza ad archiviare, in maniera adeguatamente protetta, i risultati del test all'interno del proprio sistema informatico. In caso l'auditor sia esterno devono essere esplicitamente concordate nella lettera d'incarico le modalità di conservazione dei dati e dei risultati ottenuti durante le verifiche, la possibilità o meno che questi possano essere conservati e per quanto dall'auditor, nonché se debbano essere o meno consegnati al committente ed in quale forma.

Contatti

Dovrebbe essere concordata la lista delle persone coinvolte nel progetto di analisi delle vulnerabilità e test di intrusione.

Organizzazione	Ruolo	Cognome e Nome	Telefono	Email
Auditor				
Auditor				
Auditee				
Auditee				

Target dell'analisi

Dovrebbe essere stilato l'elenco delle reti e dei sistemi oggetto dell'analisi delle vulnerabilità e dei test di intrusione.

Tipo (rete/sistema)	Indirizzo IP/maschera	Incluso/Escluso

I suddetti sistemi/reti costituiranno il ToE (*Target of Evaluation*) dell'analisi VA/ PenTest oggetto del Disclaimer.

Rischi associati alle attività VA/ PenTest

Ogni attività di ricerca ed analisi delle vulnerabilità espone inevitabilmente i sistemi dell'auditee a rischi di diversa natura e gravità che, a causa della complessità degli ambienti applicativi e dei sistemi operativi, non possono essere previsti a priori.

Per ridurre al minimo i rischi associati alle attività VA/PenTest, l'auditor dovrebbe eseguire le attività secondo le regole di ingaggio descritte nel Disclaimer, ma necessita comunque della piena e completa disponibilità dell'auditee per porre in atto opportune *misure precauzionali*.

L'auditee, infatti, dovrebbe necessariamente:

- proteggere i propri dati mediante opportune attività di backup;
- informare il personale tecnico preposto alla gestione dei sistemi dell'eventualità che, contestualmente alle attività di VA/PenTest, possano verificarsi interruzioni/alterazioni dei servizi e delle applicazioni di tali sistemi;
- predisporre il personale tecnico affinché, a fronte di eventuali interruzioni/alterazioni dei servizi contestuali alle attività

VA/PenTest, possa intervenire in modo tempestivo per il ripristino del corretto funzionamento dei sistemi/servizi.

Limitazioni di responsabilità

L'auditor si dovrebbe impegnare a fornire servizi eseguiti a regola d'arte ed in linea con le regole legali, deontologiche e professionali applicabili, regolando e limitando le responsabilità in apposita sezione della lettera d'incarico (Disclaimer).

Conseguentemente, l'auditor non sarà gravato da eccessiva responsabilità per danni diretti o indiretti che dovessero verificarsi all'auditee e/o a terzi per l'esecuzione del servizio di VA/ PenTest, salvo che questi abbia operato nei limiti del mandato conferito. Un eventuale rimedio sarà l'impegno a fornire tempestivamente ogni materiale/informazione raccolta ed utile al ripristino del danno.

In particolare, l'auditee, sottoscrivendo il Disclaimer, darà specifico assenso al grado di responsabilità dell'auditor per le attività svolte e dei relativi risultati di tali attività.

Appare indispensabile operare una mediazione sulle responsabilità dell'auditor che, dove possibile, dovrebbero limitarsi al caso questi non applichi la dovuta diligenza professionale. Infatti "penalità" maggiori potrebbero scoraggiare l'assunzione dell'incarico.

Nel caso in cui l'auditor sia un'organizzazione terza rispetto all'auditee (auditor o consulente esterno), il Disclaimer dovrebbe prevedere un limite esplicito agli oneri a carico dello stesso, in particolare precisando l'ammontare massimo del risarcimento che, nella prassi, viene rapportato all'ammontare degli onorari (normalmente viene stabilito un importo tra la metà ed il doppio degli stessi).

Accettazione

Con la sottoscrizione del Disclaimer le parti interessate concordano nell'accettare le regole esposte in tale documento per l'attività di analisi delle vulnerabilità e test di intrusione che l'auditor condurrà nei confronti delle reti e sistemi dell'auditee.

In particolare, il capitolo del Disclaimer riguardante l'accettazione dei termini di servizio, comporta per l'auditee l'accettazione incondizionata di quanto stabilito al capitolo "Limitazioni della responsabilità" e libera

l'auditor (soprattutto se si tratta di una società esterna) da ogni responsabilità per danni diretti o indiretti di qualsiasi natura ed entità che dovessero verificarsi all'auditee e/o a terzi per l'esecuzione del servizio di VA/ PenTest.

Un'accettazione formale dovrebbe concludersi con una firma, ad esempio nelle modalità riportate di seguito.

Soggetto	Nome	Data	Firma
Auditor			
Auditee			

7. Forma e contenuto del report

Al termine dell'attività, si procede alla stesura di un report da consegnare al committente.

Il report finale, solitamente, è composto da due parti:

- sintetica: in cui sono riportate le informazioni relative allo scopo del lavoro ed agli obiettivi, l'approccio utilizzato, la definizione delle informazioni di partenza, il sommario delle criticità risultanti dal PenTest, la definizione del livello di rischio e le relative conclusioni;

- analitica: in cui sono documentate in dettaglio le attività svolte, le debolezze riscontrate, i relativi rischi e le indicazioni per effettuare le misure correttive. Se necessario si possono allegare anche report generati dai tool di scansione e di analisi, contenenti le informazioni riguardanti le macchine analizzate e le vulnerabilità individuate.

Mentre la parte sintetica, in alcuni casi, può essere omessa anche in funzione del destinatario del report (p.e. nel caso in cui il PenTest è inserito in un progetto più ampio di IT Audit o VA), la parte analitica dovrebbe essere sempre prodotta, sia per documentare adeguatamente il lavoro svolto, sia al fine di fornire tutte le informazioni utili per la risoluzione delle problematiche rilevate.

Nel report dovrebbero essere comunque riportate, od almeno riepilogate, le regole d'ingaggio stabilite per poter così contestualizzare correttamente i risultati del lavoro. Nel caso in cui tali regole abbiano posto significative limitazioni all'esecuzione e/o all'ottenimento dei risultati, questo dovrebbe essere espressamente indicato, unitamente alla spiegazione degli effetti di tali limitazioni.

In linea generale, una bozza del report, od almeno una sintesi dei risultati, andrebbe preventivamente discussa con i referenti individuati, da una parte per validare tali risultati e per vagliare le possibili soluzioni da implementare, dall'altra per poter meglio identificare ed esporre i rischi derivanti dalle debolezze riscontrate.

Se ritenuto opportuno e se previsto dai termini dell'incarico, una copia (anche elettronica) di tutta la documentazione raccolta e delle "carte di lavoro" può essere allegata al report finale.

8. Conclusioni

Come già evidneziato, nella sua forma più semplice, il security penetration test è una tecnica di audit nata da un semplice principio: trovare le vulnerabilità relative alla sicurezza prima che lo facciano gli hackers.
Questa tipologia di test usa tecniche analoghe a quelle usate dagli hackers per individuare tali vulnerabilità ed al fine di correggerle.

Spesso ci si limita a questa definizione comune del penetration testing che tende a limitare l'intervento sulla configurazione ed i "bachi" del sistema operativo o delle difese perimetrali di una rete. Se inteso semplicisticamente a questo livello tecnico e se eseguito come una serie di test "meccanici", il penetration test non è migliore di una limitata analisi diagnostica della sicurezza di un sistema.

Ciò è vero perché, per determinare la sicurezza di un sistema, è sempre più efficace uno studio accurato ed in dettaglio della configurazione. Il penetration test "puro", per sua natura, deve partire senza il vantaggio di conoscenze interne sulla configurazione del sistema (rif. par. "Modalità di esecuzione del pen-test – zero knowldge" pag. 17-18). Infatti, se non è possibile esaminare un sistema

dall'interno, come è possibile determinare che sia "sicuro" basandosi esclusivamente su test eseguiti dall'esterno (e con un certo grado di casualità)? Quindi, ad un primo esame, questa tecnica può apparire fondamentalmente limitata e fallace.
Tuttavia, se si da per assunto che la sicurezza informatica è, in realtà, un sistema di policies, procedure, standard operativi e di configurazione delle componenti tecnologiche e di rete, attività di monitoraggio e di audit, il tutto intrecciato in un complesso sistema di controlli preventivi e di rilevazione, allora il penetration test può avere dei benefici unici.

Un tale approccio può dare una visione alternativa della sicurezza che può non essere facilmente ottenibile utilizzando tradizionali tecniche "diagnostiche".

Ad esempio sistemi dimostratisi sicuri da attacchi diretti al sistema operativo od al network, potrebbero soccombere ad attacchi che sfruttano una serie di debolezze procedurali od associate a sistemi "adiacenti". Inoltre con l'incremento dell'e-commerce si è incrementata l'attività c.d. di "Cybercrime" ed i metodi utilizzati dagli hackers si sono fatti sempre più complessi.

La diversità e la complessità di tali attacchi richiede vigilanza continua e l'utilizzo efficace di tecniche di risk assessment per l'identificazione delle vulnerabilità negli accessi e per sviluppare contromisure dagli eventuali attacchi.

Il penetration test dovrebbe essere anche il mezzo con cui rimediare al fatto che gli amministratori della sicurezza potrebbero non essere a conoscenza, o comunque non ad un livello adeguato, di tali tecniche, ponendoli in una posizione di svantaggio rispetto agli hackers.

Un penetration test, se condotto correttamente, fornisce un unico punto di vista sulla sicurezza di un'organizzazione. Questo documento è stato redatto in quest'ottica e con l'obiettivo di aggiungere una tessera al puzzle delle misure messe in atto dalle organizzazioni nell'ambito della sicurezza e dell'audit. Riteniamo che delinei in maniera esaustiva gli obiettivi di un penetration test, utili per massimizzarne il valore nell'effettiva applicazione.

Riferimenti

Principali fonti e strumenti per l'esecuzione di un PenTest.

ISACA - IS AUDITING PROCEDURE: SECURITY ASSESSMENT– PENETRATION TESTING AND VULNERABILITY ANALYSIS DOCUMENT P8

http://www.isaca.org/Template.cfm?Section=Standards&Template=/ContentManagement/ContentDisplay.cfm&ContentID=18815

Procedura di audit emessa dall'ISACA che, oltre a fornire una breve spiegazione delle principali tecniche di pen-test, include un programma di lavoro in forma di checklist, molto utile come linea guida nel corso dell'audit.

LiveCD

Un PenTester in genere mantiene una propria "collezione" degli strumenti che gli servono aggiornati giornalmente. Tuttavia per un uso occasionale, o per provare qualche strumento nuovo, i Live CD sono un'ottima soluzione.

Sono dei CD contenenti un Sistema Operativo, completo dei principali ferri del mestiere. Si avviano accendendo il PC dopo aver inserito il Live CD nel lettore CD-ROM/DVD (avendo abilitato il boot da CD nel BIOS), e dopo pochi istanti il PC è un'ottima "macchina da guerra" senza rischio di apportare alcuna modifica involontaria all'Hard Disk del PC, ma potendovi eventualmente salvare quanto serve. Come unità di memorizzazione si possono usare anche le memorie USB.
I Live CD stanno incontrando sempre più il gradimento di tecnici, appassionati e professionisti e ne nascono continuamente di nuovi e per gli usi più disparati.
Ad esempio, dyne:bolic (http://www.dynebolic.org/) trasforma il PC in uno studio multimediale per foto, filmati, musica e può essere usato persino come server di diffusione audio/video in rete o Internet.

I Live CD hanno molteplici usi. Possono ad esempio essere usati per eseguire attività senza lasciare tracce sul proprio PC, verificare il

funzionamento di periferiche senza installare software, ripristinare sistemi danneggiati, analizzare in modo sicuro ed affidabile la presenza di malfare sui supporti magnetici senza modificarli, analizzare il contenuto di un disco senza inquinarne il contenuto, e molto altro.

Rimanendo sul terreno del PenTest, ecco una breve descrizione dei Live CD più in voga al momento della stesura di questo documento.

Auditor

http://www.remote-exploit.org

Basato su Linux Debian, è incentrato sulla facilità d'uso, e quindi è indicato anche ad utilizzi occasionali.
Dispone di un menu ben organizzato ed include un'ottima documentazione per ciascuno degli strumenti accessibili da menu.
All'avvio non configura automaticamente la rete, che va configurata con l'apposita scelta di menu (o via shell in modo tradizionale).

WHoppix

http://www.whitehat.co.il

Basato su Linux Knoppix (Debian) la versione stabile si è affacciata recentemente in rete.
Gestito dal gruppo White Hats, è in fase di notevole evoluzione. Include una raccolta pressoché completa degli exploits di PacketStorm.
Il gruppo mette a disposizione una serie di filmati utili a capire alcuni utilizzi dello strumento, che per la manualità richiesta richiede un minimo di competenze in ambiente Linux.

Operator

http://www.ussysadmin.com

Basato su Linux Debian, è aggiornato regolarmente ed include gran parte degli strumenti di PenTest oltre ad una raccolta dei principali exploits.

Un'indicazione delle principali novità nei software del settore la si può dedurre anche dal changelog di questa distribuzione (http://www.ussysadmin.com/operator/Changelog.txt).

Knoppix-STD

http://www.knoppix-std.org/

Basato su Linux Knoppix (Debian) attualmente non è fra quelli aggiornati più di frequente, nondimeno merita una menzione quanto meno per essere stato fra i più completi capostipiti del settore.
È anch'esso incentrato sull'usabilità, ma non eguaglia la semplicità di Auditor.

NST

http://www.networksecuritytoolkit.org

Basato su Linux RedHat, non dispone di molti strumenti come gli altri contendenti, tuttavia ha una caratteristica che lo rende interessante: può essere avviato su un PC ed usato da remoto via Browser web o SSH .
È facile da aggiornare e può essere condiviso contemporaneamente fra più collaboratori.

LAS

http://localareasecurity.com/

Basato su DamnSmall Linux ha la caratteristica di avere dimensioni ridotte (185 Mbytes circa), per cui può essere masterizzato su un Mini-CD.

PHLAK

http://www.phlak.org

Professional Hacker Linux Assault Kit.
Interessante strumento tutto-fare.

FIRE

http://fire.dmzs.com

E' basato su FreeBSD (uno Unix, non Linux).
Ha un'interessante collezione di strumenti, documentata sul sito.

IrItaly

http://www.iritaly.org

E' una distribuzione destinata alla Forensic Analisys, ma egualmente interessante per i PenTester.
Il progetto, gestito dal Dipartimento di Tecnologie dell'Informazione dell'Università Statale di Milano, nel Polo Didattico e di Ricerca di Crema, avvalendosi del contributo di Dario Forte, è documentato in italiano in modo eccellente, ed è un punto di riferimento per l'analisi con valenza probatoria di sistemi compromessi o attività illecite.

m0n0wall

http://m0n0.ch

Basato su FreeBSD (Unix), è un firewall su Live CD, con caratteristiche molto interessanti e per molti aspetti utili al PenTest.

Bibliografia

James S. Tiller, The Ethical Hack: A Framework for Business Value Penetration Testing, CRC Press LLC, 2005, ISBN 0-8493-1609-X

Susan Young – Dave Aitel, The Hacker's Handbook: The Strategy Behind Breaking into and Defending Networks, CRC Press LLC, 2004, ISBN 0-8493-0888-7

Mike Shema - Bradley C. Johnson, Anti-Hacker Tool Kit, Second Edition, McGraw-Hill, 2004, IBSN 0-07-223020-7

John Chirillo, Hack Attacks Testing: How to Conduct Your Own Security Audit, Wiley Publishing, Inc., 2003, ISBN 0-471-22946-6

Carl Endorf - Gene Schultz - Jim Mellander, Intrusion Detection and Prevention, McGraw-Hill, 2004, IBSN 0-07-222954-3

Kevin D. Mitnick, L'arte dell'inganno - I consigli dell'hacker più famoso del mondo, Feltrinelli, 2003, ISBN: 8807170868 (V.O.: The Art of Deception, Wiley Publishing, Inc., 2002, ISBN 0-471-23712-4)

Glossario

Access Point Wireless
Dispositivo hardware di livello 2 della suite ISO/OSI, equivalente ad uno switch nella comunicazione wired, che consente la creazione di reti wireless con infrastruttura, permettendo l'integrazione dei dispositivi dotati di connettività wireless all'interno di una LAN.

AIEA
Associazione Italiana Information Systems Auditors - (http://www.aiea.it).

Audit
Attività di verifica e controllo, svolta da un soggetto indipendente, che attesta la conformità a standards, policy o procedure.

BIOS
Basic Input Output System – Insieme di procedure di basso livello residenti in memoria ROM, che interpretano le istruzioni di base per l'interfacciamento con i dispositivi hardware.

Bluetooth
Suite di protocolli di comunicazione wireless basati su onde radio, orientati allo utilizzo in reti di host di piccola estensione (Personal Area Network) e in ambito mobile.

Bug Software
Porzione di codice software contenente errori che lo rendono inutilizzabile o maggiormente esposto ad attacchi esterni. I bug possono essere sfruttati da hackers come passaggio preferenziale per l'accesso non autorizzato ad un host.

Computer Network
Sistema costituito da elaboratori(host) interconnessi tra loro in grado di comunicare e condividere risorse hardware/software.

DECnet
Nome commerciale della DNA (Digital Network Architecture), identifica la suite di protocolli per il networking proprietaria della Digital Equipment Corporation. Anch'essa, come la suite ISO/OSI, è composta da sette livelli.

DMZ
Demilitarized Zone, sottorete che ospita i Server pubblici maggiormente esposti ad attacchi esterni e che non permette l'accesso diretto all'Intranet aziendale. Le connessioni dall'esterno avvengono esclusivamemente verso un Bastion Host ospitato nella DMZ a cui si collegano due Router che fungono da interfaccia esterna e interna verso la rete locale.

DNS
Domain Name System, sistema che effettua la risoluzione dei nomi simbolici in indirizzi IP all'interno di una rete.

DOS
Denial of Service, tecnica di attacco ad un sistema informatico che consiste nel sovraccaricare i Server (Web, ftp, mail,…) di un numero eccessivo di richieste da parte degli utenti, spesso ignari, ottenendo di fatto l'indisponibilità dei servizi di rete.

Firewall
Dispositivo fisico o applicazione software che implementa una politica di restrizione degli accessi remoti ad un host o ad una rete, impedendone gli accessi non autorizzati e aumentendone la sicurezza.

Frame Relay
Protocollo di comunicazione di livello 1,2 della suite ISO/OSI per reti WAN a commutazione di pacchetto. E' considerato il successore di X.25.

FTP
File Trasnfert Protocol, protocollo di comunicazione orientato alla trasmissione di files.

Hacker
Soggetto che accede in maniera non autorizzata a sistemi informatici, eludendo i sistemi di sicurezza degli stessi, allo scopo di recuperare dati, commettere operazioni per cui non si dispone dei privilegi e/o danneggiare il sistema stesso.

Hub
Dispositivo hardware di livello 1 della suite ISO/OSI tipico delle topologie di rete a stella. Tutti gli host ad esso collegati possono comunicare tra loro tramite il broadcast effettuato da questo dispositivo.

IDS
Intrusion Detection System, sistema complementare a firewall e router, permette di rilevare ed allertare l'utente di un sistema o l'amministratore dell'avvenuta rilevazione di un attacco.

IP
Internet Protocol, protocollo di comunicazione di livello 3 della suite ISO/OSI orientato ad Internet, fornisce un indirizzo univoco per la localizzazione di un host sull'Internet. L'attuale versione IPv4 utilizza una configurazione di quattro byte per la codifica degli indirizzi, l'inadeguatezza numerica della IPv4 per la identificazione univoca ha richiesto la nascita della nuova versione IPv6 a 8 byte.

ISACA
The Information Systems Audit and Control Association – (http://www.isaca.org)

ISO/OSI
International Organization for Standardization/Open System Interconnection, standard "de iure" per la stratificazione dei protocolli di comunicazione tra elaboratori. La suite è composta da sette livelli e ricalca il modello proprietario SNA dell'IBM.

LAN
Local Area Network (Project IEEE 802), rete di calcolatori caratterizzata da una estensione limitata, in genere non valica i confini di un edificio.

Mail Server
Server di posta elettronica che processa richieste di protocolli SMTP, POP3, IMAP.

Modem
MOdulatore-DEModulatore, dispositivo hardware in grado di codificare/decodificare segnali digitali allo scopo di effettuare una trasmissione tramite un canale di comunicazione.

Network Scanning
Procedura per la ricerca degli host attivi di una rete spesso eseguita a scopo di hacking. E' possibile in tal modo individuare gli indirizzi IP degli host e i servizi attivi utili all'attacco alla rete.

Patch
Porzione di codice contenuta in un'applicazione, spesso rilasciata dall'implementatore del software, che pone rimedio ai bugs identificati dopo il rilascio del prodotto.

Port Scanner
Strumento software in grado di interrogare le porte logiche presenti su un determinato host o all'interno di un range di indirizzi IP, allo scopo di recuperarne informazioni utili per un attacco.

RAS
Remote Access Server, Server per la gestione dei collegamenti remoti tramite modem.

Reboot
Operazione di re-inizializzazione di un sistema informatico conseguente ad un incidente grave o ad operazioni di manutenzione straordinaria.

Rete
Vedi Computer Network

Router
Dispositivo hardware di livello 3 della suite ISO/OSI che effettua l'instradamento dei pacchetti di dati tra reti omogenee.

Syslog Server
Server di rete, inizialmente presente su sistemi Unix, che memorizza e rende disponibili ai fini dell' auditing le richieste di connessioni al sistema informatico.

TCP/IP
Internet Protocol Suite, standard "de facto" per Internet prevede la stratificazione dei protocolli di comunicazione su quattro livelli, deriva concettualmente dal modello utilizzato da Unix.

Traderz
Web Sites, in genere a carattere monotematico, che mettono a disposizione dei loro frequentatori dei canali di scambio di informazioni e oggetti

Virtual Private Network
Tecnologia di comunicazione che, utilizzando protocolli di tunneling, permette di estendere una rete privata facendo uso di infrastrutture pubbliche, garantendo sicurezza e privacy dei dati.

WAN
Wide Area Network – Conosciuta come Rete Geografica è una rete di calcolatori che ha estensione diffusa sul territorio.

Web Site
Applicazione software resa disponibile da un Web Server e basata sul paradigma Client-Server. In genere è accessibile tramite un Internet Browser.

Web Server
Server in grado di soddisfare richieste degli utenti effettuate tramite protocollo HTTP.

Wireless
Con il termine Wireless si identificano tutte le tecnologie di comunicazione che non fanno utilizzo di cavi per la trasmissione. Esempio di tecnologie Wireless sono: Wi-fi, Bluetooth, Infrarosso, GPRS.

Worm
Codice software malevolo in grado di propagarsi, via network, ad altri computer.

X.25
Suite di protocolli di comunicazione su WAN pubbliche basate su linee telefoniche a commutazione di pacchetto.

X.121
Standard per la descrizione del formato degli indirizzi utilizzati da X.25.