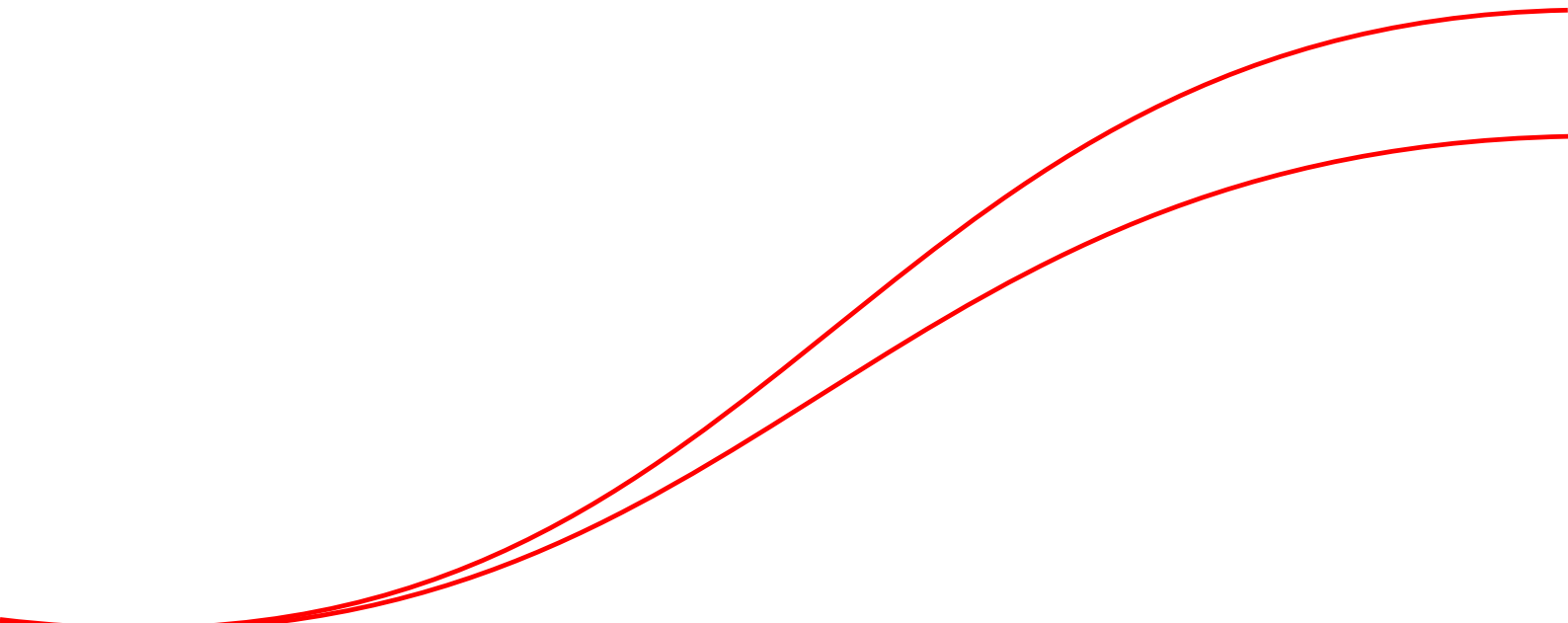


# NPT

## Network Penetration Test



# Network Penetration Test (NPT)

Trovare le vulnerabilità nei propri sistemi prima che lo faccia qualcun'altro è un processo importante per la sicurezza della propria rete. Un *Network Penetration Test* ha lo scopo di identificare le vulnerabilità, focalizzandosi sulle aree di maggior impatto per il business aziendale.

Un *Network Penetration Test* è orientato alla valutazione della sicurezza di una rete e può essere svolto dall'interno (*Internal PT*), dall'esterno (*External PT*) e con vari livelli di informazione e accesso alle infrastrutture e risorse del cliente (*Black Box*, *Gray Box* e *White Box*).

È possibile quindi simulare scenari di attacco differenti. Un *External PT* di tipo *Black Box* ad esempio mira ad identificare quale danno può essere causato da un attaccante casuale esterno all'organizzazione mentre un *Internal PT* di tipo *Gray Box* simula un dipendente malintenzionato.

ISGroup è il fornitore ideale per le Vostre necessità di Network Penetration Test e opera con serietà secondo standard internazionalmente riconosciuti ai più alti livelli di qualità grazie al costante impegno nell'ambito della ricerca. Contattateci per informazioni e richiedete un preventivo personalizzato.

## Descrizione del servizio

Oggi che il commercio elettronico, le operazioni *on-line B2B (Business-to-Business)* e la connettività globale sono diventati componenti fondamentali della strategia di un business di successo, le imprese hanno adottato processi e pratiche di sicurezza.

La maggior parte delle imprese opera con diligenza per mantenere un efficiente ed efficace politica di sicurezza che implementi i più recenti prodotti e servizi per prevenire le frodi, gli atti di vandalismo, sabotaggio e attacchi *DoS (Denial of Service)*.

Nonostante questo molte imprese non danno il giusto risalto ad un ingrediente chiave del successo di una politica di sicurezza: la verifica che la rete e i sistemi di sicurezza funzionino come previsto.

L'attività di *Network Penetration Test*, utilizzando strumenti e processi per scansionare l'infrastruttura di rete alla ricerca di vulnerabilità, aiuta a rifinire una politica di sicurezza aziendale, identificando le vulnerabilità, e di garantire che l'implementazione di sicurezza effettivamente fornisca la protezione che l'azienda richiede e necessita.

Eseguire regolarmente *Penetration Test* aiuta le imprese a scoprire i punti deboli della sicurezza della rete, che possono portare a dati o apparecchiature compromesse o distrutte da *Exploit*, *Virus*, *Trojan*, attacchi *Denial of Service* e altre intrusioni. La verifica può esporre anche altre vulnerabilità che possono essere introdotte da *patch* e aggiornamenti o da errori sui *Server*, *Router* e *Firewall*.

*Network Penetration Test* in breve:

- Vengono ricercate dall'esterno o dall'interno vulnerabilità nei sistemi maggiormente esposti.
- Le vulnerabilità identificate vengono sfruttate al fine di violare il perimetro della rete.
- I sistemi interni vengono ispezionati alla ricerca di altre vulnerabilità che permettano di ottenere ulteriore accesso ai dati e alle infrastrutture.
- Il processo viene ripetuto fintanto possibile.

# Specifiche del servizio di Network Penetration Test

Il servizio di *Network Penetration Test* viene effettuato da qualificati professionisti secondo metodologie riconosciute internazionalmente, quali l'OSSTMM (*Open Source Security Testing Methodology Manual*), un manuale *Open Source* per l'esecuzione dei *test* di sicurezza verso infrastrutture ed asset informatici), adattate rispetto le specifiche esigenze del cliente e dello scenario di attacco.

Tutte le parti più delicate e tecniche vengono svolte da ricercatori *senior* per garantire la massima professionalità e far sì che non vi siano danneggiamenti né all'infrastruttura né ai dati.

Dall'esterno (*External PT*) o dall'interno (*Internal PT*) e col livello di informazioni scelto dal cliente (*Black Box*, *Gray Box* e *White Box*) per simulare diversi scenari di attacco.

Ogni nostro servizio è personalizzabile secondo le esigenze del cliente e integrabile con gli altri servizi e prodotti offerti. Un *NPT* può tenere conto dell'aspetto prettamente informatico o anche delle persone e dei processi (*Social Engineering*) e della sicurezza fisica. È il cliente a decidere quali sono gli aspetti più importanti dell'attività e dove gli sforzi del *team* di attacco debbano essere concentrati.

I risultati dell'attività di *testing* vengono riassunti ed esposti nel *Report*, un documento semplice e dettagliato composto da tre sezioni principali.

Una parte iniziale di alto livello, chiamata *Executive Summary*, dedicata al *Management*. Una parte tecnica che descrive nel dettaglio le vulnerabilità rilevate e il loro impatto, dedicata al *Security Manager*. Una parte tecnica con istruzioni precise su come risolvere le problematiche identificate, dedicata al *System Administrator*, chiamata *Remediation Plan*.

## Scenari di Network Penetration Test

ISGroup esegue i propri *test* con varie modalità operative:

### Internal PT

I *test* vengono effettuati posizionandosi all'interno della rete aziendale.

### External PT

I *test* vengono effettuati posizionandosi all'esterno della rete aziendale.

Inoltre è possibile differenziare tra *testing Black Box*, *Gray Box* e *White Box*, a seconda delle informazioni fornite sui sistemi da attaccare. Ecco alcuni esempi e scenari:

### External PT Black Box

Simula un attaccante casuale o esterno (ad esempio un concorrente) ma comunque senza accesso ad informazioni e credenziali di accesso dell'azienda.

### Internal PT Black Box

Simula un attaccante che abbia accesso fisico (ad esempio un consulente esterno o un visitatore in una sala riunioni) o remoto (ad esempio un *computer* di una segretaria

compromesso) alla rete aziendale.

### External PT White Box

Simula la compromissione di una componente esposta all'esterno per capire che livello di accesso un attaccante possa ottenere alle altre parti dell'infrastruttura aziendale.

### Internal PT White Box

Simula un attaccante interno all'organizzazione con informazioni ed accesso ad alcune parti dell'infrastruttura per capire che livello di accesso alle componenti critiche sia possibile ottenere.

### Wireless Penetration Test

Cerca di compromettere l'infrastruttura *wireless*, simula un attaccante che sia fisicamente prossimo ad uno degli edifici dell'azienda in cui sia installata una rete *wireless*.

### Social Engineering

Invece di attaccare la componente informatica viene attaccata quella "umana", con tecniche di manipolazione si cerca di indurre le persone a compiere azioni o a rivelare informazioni.

# Output

Il *Report* è un documento semplice e dettagliato che riassume i risultati dell'attività ed è suddiviso in tre differenti aree come precedentemente descritto:

## Executive Summary

All'inizio del *Report* e di lunghezza non superiore ad una pagina, è il riassunto di alto livello destinato al *Management*.

## Vulnerability Details

La parte tecnica che descrive nel dettaglio le vulnerabilità riscontrate e il loro impatto, dedicata al *Security Manager*.

## Remediation Plan

Sezione tecnica con istruzioni precise su come risolvere le problematiche identificate, dedicata al *System Administrator*.

Nel caso in cui l'attività sia per una terza parte lavoriamo con disinvoltura su modelli di *Report* preventivamente forniti con la grafica e secondo le modalità che ci vengono indicate.

Precisione e dettaglio, semplicità e chiarezza sono i fondamentali di un buon *Report*. Vista la complessità delle problematiche di sicurezza cerchiamo sempre di facilitare il lavoro di chi si appoggia a noi tramite documenti redatti con la massima cura e che siano veramente utili e "pragmatici".

Poniamo grande attenzione al *Remediation Plan*. Questa componente, spesso considerata di secondo piano, è fondamentale per far sì che le problematiche identificate vengano realmente risolte nella maniera corretta.

I nostri *Report* sono uniformi e facilmente compatibili tra di loro.

Per richiedere un esempio di *Report* anonimizzato, oltre che discutere delle vostre specifiche esigenze, contattateci senza impegno.

## Richiedi servizi di Network Penetration Test

Lavorare con noi è molto semplice, chiamando il numero +39-045-4853232 o spedendo una mail a [sales@isgroup.it](mailto:sales@isgroup.it) potremo conoscervi e discutere delle vostre necessità di fornitura di servizi di *IT Security*.