PENTESTERRA

NETWORK PENETRATION TEST

La Tua Rete Resiste a un Attacco Reale?

Penetration test di rete, esterno e interno - dalla scoperta allo sfruttamento confermato, con prova, non una lista di CVE.

COS'È UN NETWORK PENTEST, IN BREVE

È una verifica attiva della sicurezza informatica (cyber) della tua infrastruttura di rete - perimetro esterno visibile da internet, e rete interna raggiungibile da chi è già dentro. Non basta sapere che una porta è aperta: bisogna sapere se un attaccante può davvero usarla per entrare, muoversi lateralmente e raggiungere i dati che contano.

Esterno + Interno

Perimetro internet-facing e rete interna, in un'unica valutazione

Verificato

Ogni exploit critico confermato in modo sicuro, non solo teorico

Non distruttivo

Nessun rischio per la continuità operativa

LA SITUAZIONE OGGI

CHI SEI

Sei il CISO, l'IT manager o il responsabile infrastruttura di un'azienda che deve sapere se la propria rete - dall'esterno e dall'interno - resisterebbe a un attaccante reale, non solo a uno scanner di vulnerabilità passivo.

COSA È SUCCESSO

L'ultimo penetration test di rete risale al ciclo di budget annuale. Da allora un nuovo server è stato messo in produzione, una regola firewall è stata aperta per un fornitore e non è mai stata richiusa, e nessuno ha verificato se questi cambiamenti hanno aperto un varco.

IL PROBLEMA

Non sai, con certezza, cosa sia davvero raggiungibile ed exploitabile nella tua rete oggi, sia dall'esterno che dall'interno. La distanza tra "testato l'anno scorso" ed "esposto adesso" è esattamente dove nascono le violazioni.

PERCHÉ FA MALE

Un servizio database esposto, una porta di amministrazione dimenticata, un movimento laterale possibile tra segmenti di rete - questi sono i dettagli che una lista di CVE non cattura, ma che un attaccante reale sfrutta per primi. Un cliente, un assicuratore cyber o un auditor possono chiedere prova di un test recente prima di firmare.

DOVE VUOI ARRIVARE

STATO DESIDERATO

Vuoi sapere, con prova concreta, cosa un attaccante potrebbe davvero raggiungere e sfruttare nella tua rete oggi - non una lista di CVE ordinata per punteggio.

LA SOLUZIONE

Un **Network Penetration Test** completo, esterno e interno, con exploit reali verificati in modo sicuro, rilevamento di servizi esposti (database, RDP, SMB) e simulazione di movimento laterale tra segmenti di rete.

PERCHÉ È DIVERSO

Non stai comprando l'ennesima scansione automatica con una lista di CVE. Stai lavorando con [NOME AZIENDA] - fornitore certificato, italiano, con quasi 20 anni di storia nel settore della sicurezza informatica. Probabilmente ci conosci già, o conosci qualcuno - un collega, un fornitore, un concorrente - che è già stato nostro cliente. Molti dei tuoi concorrenti diretti si stanno già rivolgendo a noi. E la piattaforma tiene indicizzati oltre 330.000 CVE: quando ne viene pubblicato uno critico, sai in circa 15 minuti quali host della tua infrastruttura sono esposti - inclusi i nodi interni che uno strumento cloud non può raggiungere, non solo alla prossima scansione pianificata.

PROVA CONCRETA

Il risultato è un report PDF completo, pronto da consegnare, con ogni exploit critico verificato tramite proof-of-concept. Se emergono gap più ampi, ti proponiamo le misure aggiuntive per colmarli: vulnerability assessment applicativo, penetration test web/API, formazione anti-phishing.

Database, RDP, SMB

Servizi esposti rilevati concretamente, non solo elencati

Movimento Laterale

Simulato tra segmenti di rete, non solo teorizzato

On-Prem Possibile

Distribuzione anche in ambienti air-gapped

COSA INCLUDE DAVVERO

Dalla scoperta allo sfruttamento confermato, su un unico modello dati per esterno e interno - non due strumenti scollegati.

Sempre attivo, non una tantum

Il test può girare su schedulazione o trigger, non solo come impegno annuale.

- Cadenza configurabile: pianificata, on-demand, o attivata da CI/CD
- Audit trail completo per ciclo, con report differenziale
- Copre LAN interna, cloud e topologie ibride

Exploit reali, verificati in sicurezza

La maggior parte degli scanner di rete si ferma alla lista di CVE. Qui l'exploit viene davvero lanciato.

- Catena di verifica: CISA KEV → moduli Metasploit → ExploitDB → script non distruttivi personalizzati
- Nessuna cancellazione dati, nessun payload DoS, nulla che esfiltri dati
- Approvazione umana opzionale prima dello sfruttamento attivo

Esterno e interno, un solo modello dati

Non strumenti separati cuciti insieme - una vista unica di ciò che vede un attaccante fuori e dentro.

- Rileva database esposti (MySQL, PostgreSQL, MongoDB, Redis, MSSQL)
- Servizi admin esposti (SSH, RDP, VNC, Telnet, SMB), TLS debole, OS non patchato
- I finding diventano nodi nel grafo di Attack Chain multi-dominio

Distribuzione come richiede il tuo ambiente

SaaS con nodi privati, PaaS dedicato, o on-premises completo - stesso motore, tre livelli.

- SaaS con nodi scanner privati: il piano di controllo è cloud, i dati non lasciano il tuo perimetro
- PaaS dedicato single-tenant: piano di controllo isolato, tua flotta di nodi
- On-premises completo (GOV Edition): supporto per ambienti air-gapped e classificati

PENTESTERRA

NETWORK PENETRATION TEST

COSA RICEVI

- ✓ Un report PDF completo con ogni exploit critico verificato tramite proof-of-concept
- ✓ Copertura del perimetro esterno e della rete interna, in un'unica valutazione
- ✓ Rilevamento di servizi esposti e simulazione di movimento laterale
- ✓ Raccomandazioni di remediation prioritizzate per rischio reale
- ✓ Executive summary pronto per il tuo consiglio o per un cliente enterprise

COME FUNZIONA

1

Definiamo il perimetro

Esterno, interno, o entrambi - stabiliamo insieme lo scope del test.

2

Scopriamo i servizi

Fingerprinting completo di host, porte e servizi esposti.

3

Sfruttiamo in sicurezza

Verifichiamo l'exploitability reale, in modo non distruttivo.

4

Ti consegniamo il report

Un PDF completo con i rischi prioritizzati e le azioni da intraprendere.

Scopri se la tua rete resiste a un attacco reale

Un report completo, pronto da presentare a clienti, auditor o al tuo consiglio di amministrazione.

Richiedi il tuo Network Pentest →

info@pentesterra.com · pentesterra.com/continuous-pentest