ENETWORKS
WITH DATA WE WORK

PENETRATION TEST

Rileva le vulnerabilità che possono essere sfruttate per penetrare la tua infrastruttura IT.

Cos'è il Penetration Test?

Un team di ethical hacking rileva le vulnerabilità e le sfrutta per penetrare l'infrastruttura IT.
Non effettuiamo attività spot restituendo un semplice report, ma offriamo Penetration Test continuativi e all'interno di un'azione più globale di Cyber Risk Assessment.

Se hai qualche regolamentazione da soddisfare, come la PCI o le ISO, o prevedi di stipulare un'assicurazione Cyber o devi fornire evidenze del tuo livello di sicurezza ai tuoi clienti, l'attività di Penetration Test è necessaria. In ogni caso è sempre utile testare la sicurezza della rete esterna e interna, e delle relative componenti.

Il nostro servizio

Si tratta di un servizio in due step effettuato inizialmente da un team di Ethical Hacking, che fa fisicamente il test, e completato dal team CSIRT che include la componente di analisi rischio e prepara il report finale da consegnare.

Il Penetration Test più semplice è quello che può essere condotto in modalità esterna o blackbox, simulando attacchi da chi non conosce i sistemi. Esiste anche una variante interna che – con una serie di informazioni su come sono fatti i sistemi e la rete – prova ad attaccare il sistema.

+20
anni di attività

+4
sedi in Italia

+6
nazioni servite

+100
collaboratori



Scopri di più alla sezione
Cyber Security del nostro sito!

ENETWORKS SRL
P. IVA 03087860965
Cap. Soc. 50.000 Euro
Iscr. R.E.A. MI-1637887
www.enetworks.it

MILANO HEADQUARTER
via Gaspare Gozzi, 1
20129 - Milano (MI)
milano@enetworks.it

ROMA
p.zza G. Marconi, 15
00144, Roma (RM)
roma@enetworks.it

TORINO
via Nizza, 262
10126, Torino (TO)
torino@enetworks.it

BARI
via Pasubio, 35
70125, Bari (BA)
bari@enetworks.it

ENETWORKS
WITH DATA WE WORK

I vantaggi

TEST INTERNI ED ESTERNI

Attraverso il nostro servizio, decidi tu il perimetro di azione durante il test. La modalità esterna – blackbox – è quella meno invasiva. Quella interna, che prevede di rivelare maggiori informazioni sulla tua architettura e sulle sue componenti, ti può anche far capire a che livello di compromissione può arrivare chi volesse attaccare i tuoi sistemi, ad esempio nel caso di un client o un server compromessi o di un utente che ha aperto un file o cliccato su un link malevolo.

NON SOLO UN TEST, MA UN ASSESSMENT DI SICUREZZA

Possiamo ovviamente effettuare attività sporadiche di test.
Tuttavia, il Penetration Test è qualcosa di propedeutico a un Cyber Risk Assessment, per fare la valutazione completa di tutta l'infrastruttura. Nella reportistica che ti forniamo, inseriamo già alcune informazioni aggiuntive di analisi del rischio, che fanno parte di una più estesa attività di risk assessment.
A tua scelta, puoi sempre decidere di non limitarti al Penetration Test, ma di condurre insieme a noi un'esplorazione a 360 gradi dei tuoi rischi cyber.

UN APPROCCIO IN PARTNERSHIP

Ogni attività del test è preconcertata con te, nelle tempistiche e nei modi.
Se evidenziamo situazioni critiche, ti avvertiamo subito, ovviamente senza sfruttare la vulnerabilità riscontrata.

ELEVATA GARANZIA DI STANDARD E DI QUALITÀ

Il nostro team segue specifici processi e standard. Operiamo all'interno delle linee guida degli standard OSSTMM (Open Source Security Testing Methodology Manual) e OWASP (Open Web Application Security Project), sempre nelle relative versioni più aggiornate.

Digital Twin: la tecnologia del modello digitale

Il servizio di Cyber Attack Simulation offre una completa valutazione delle minacce cyber attraverso la Digital Twin, una soluzione predittiva in grado di creare una copia virtuale dell'infrastruttura di rete IT/OT dei tuoi clienti e simulare migliaia di potenziali attacchi su di essa, per identificare i percorsi di attacco e fornire le patch mirate per ridurre la soglia di rischio calcolato.

Simulazioni WHAT-IF

Difendi il tuo sistema con delle analisi WHAT-IF e tramite simulazioni di vulnerabilità 0-day. Un Digital Twin supporta inoltre asset potenziali, sia fisici che logici. Questo permette di eseguire analisi WHAT-IF anche quando gli asset ancora non esistono, analizzando le ripercussioni di una modifica ad un sistema esistente e permettendo di scegliere l'evoluzione migliore tra quelle possibili.

Certificazioni aziendali

Microsoft Partner
Microsoft
Gold Collaboration and Content
Gold Communications
Gold Messaging
Gold Datacenter
Silver Application Integration

ISO 9001
BUREAU VERITAS Certification
N° IT259433

ENETWORKS SRL
P. IVA 03087860965
Cap. Soc. 50.000 Euro
Iscr. R.E.A. MI-1637887
www.enetworks.it

MILANO HEADQUARTER
via Gaspare Gozzi, 1
20129 - Milano (MI)
milano@enetworks.it

ROMA
p.zza G. Marconi, 15
00144, Roma (RM)
roma@enetworks.it

TORINO
via Nizza, 262
10126, Torino (TO)
torino@enetworks.it

BARI
via Pasubio, 35
70125, Bari (BA)
bari@enetworks.it