PENTESTERRA

VULNERABILITY ASSESSMENT

Sai Davvero Cosa È Realmente Sfruttabile?

Una valutazione delle vulnerabilità (cyber security) sul tuo perimetro esterno e interno - con verifica reale dell'exploit, non solo un punteggio CVSS su carta.

COS'È UN VULNERABILITY ASSESSMENT, IN BREVE

È l'analisi sistematica delle debolezze di sicurezza informatica (cyber) nella tua infrastruttura - server, applicazioni, reti - con l'obiettivo di capire non solo cosa è vulnerabile, ma cosa è davvero sfruttabile da un attaccante oggi. È il primo passo che quasi ogni framework di cybersicurezza, da NIS2 a ISO 27001, richiede come evidenza.

1.200+

Falsi allarmi tipici in una scansione grezza non verificata

Verificato

Ogni finding confermato con un exploit reale, non solo CVSS

In + Out

Perimetro esterno e rete interna, in un'unica valutazione

LA SITUAZIONE OGGI

CHI SEI

Sei il CISO, l'IT manager o il responsabile sicurezza di un'azienda che deve sapere, con certezza, quali vulnerabilità nella propria infrastruttura sono realmente pericolose - non solo quelle segnalate da uno scanner automatico che nessuno ha mai verificato.

COSA È SUCCESSO

L'ultima scansione ha prodotto centinaia di righe rosse, gialle e arancioni. Un CVSS alto non dice se quella falla è davvero raggiungibile, sfruttabile, o già mitigata da un altro controllo - e il tuo team ha tempo di indagare seriamente solo una manciata di quelle segnalazioni.

IL PROBLEMA

Non sai, con certezza, quali vulnerabilità di cybersicurezza rappresentano un rischio reale oggi. Le informazioni esistono in un report PDF di mesi fa, ma nessuno le ha aggiornate, e un elenco ordinato per CVSS tratta un falso positivo e una RCE attiva come lo stesso tipo di testo rosso.

PERCHÉ FA MALE

Un'unica vulnerabilità trascurata può diventare il punto d'ingresso per un ransomware. Un audit, un cliente o un assicuratore cyber possono chiedere prova che le vulnerabilità critiche siano state verificate e chiuse - e una lista grezza di CVE non basta a dimostrarlo.

DOVE VUOI ARRIVARE

STATO DESIDERATO

Vuoi una lista corta e affidabile: non centinaia di CVE teorici, ma i pochi rischi realmente sfruttabili oggi nel tuo ambiente, con la prova che lo sono.

LA SOLUZIONE

Un **Vulnerability Assessment** completo su perimetro esterno e rete interna, agentless, con verifica automatica dell'exploit su ogni finding critico prima che arrivi al tuo team - non solo un punteggio CVSS.

PERCHÉ È DIVERSO

Non stai comprando l'ennesimo scanner che genera un PDF di 40 pagine di falsi positivi. 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 ogni finding critico passa per una pipeline di verifica automatica - CISA KEV, Metasploit, ExploitDB, script personalizzati - con uno stato che non retrocede mai in silenzio, da "non confermato" a "sfruttato": il tuo team riceve una prova, non un elenco da discutere.

PROVA CONCRETA

Il risultato è un report PDF completo, pronto da consegnare, con ogni finding critico corredato di prova di sfruttabilità (PoC). Se emergono gap più ampi, ti proponiamo le misure aggiuntive per colmarli: penetration test di rete o applicativo, formazione anti-phishing, revisione DevGuard del codice.

COSA INCLUDE DAVVERO

Non una scansione grezza con un elenco di CVE - una valutazione agentless, verificata con exploit reali, e riutilizzabile nel resto del tuo programma di sicurezza.

Agentless, esterno e interno

Nessun software da installare sugli asset analizzati.

- Nessun agente da distribuire o mantenere sugli host
- Perimetro esterno, LAN interna, cloud e topologie ibride
- Nodi scanner distribuiti, incluso on-prem e air-gapped
- Modalità di scansione autenticata e non autenticata

Verifica automatica dell'exploit, in sicurezza

La funzione chiave: ogni finding critico viene verificato eseguendo davvero un exploit contro di esso.

- Catena di verifica: CISA KEV → Metasploit → ExploitDB → script personalizzati → PoC da GitHub
- Nessun crash, nessuna perdita di dati, nessuna esfiltrazione
- Approvazione umana opzionale prima dello sfruttamento attivo
- Ogni risultato ha una prova di sfruttabilità (PoC) allegata

Triage che regge nel tempo

Ogni vulnerabilità è un record con uno stato che non retrocede mai in silenzio.

- Stato per finding - non confermato, potenziale, rilevato, verificato, sfruttato
- Storico completo e differenza tra una scansione e l'altra
- Log delle esclusioni: chi, quando, perché, revocabile da qualunque revisore
- I finding verificati creano automaticamente ticket Jira con passi di riproduzione

I dati vengono riutilizzati, non archiviati

Il risultato non è un report fine a se stesso.

- Definisce lo scope e le priorità di un successivo penetration test
- Diventa un nodo nel grafo di Attack Chain multi-dominio
- Si correla con i finding DevGuard e di supply chain
- Alimenta il reporting di compliance e business-impact

PENTESTERRA

VULNERABILITY ASSESSMENT

COSA RICEVI

- ✓ Un report PDF completo con ogni finding critico verificato tramite proof-of-concept
- ✓ Copertura del perimetro esterno e della rete interna, agentless
- ✓ Uno stato di triage stabile per ogni vulnerabilità, con storico
- ✓ 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 della valutazione.

2

Scansioniamo e verifichiamo

Ogni finding critico viene confermato con un exploit reale, in modo sicuro e non distruttivo.

3

Prioritizziamo il rischio

Ordiniamo i findings per sfruttabilità reale e impatto di business, non per CVSS.

4

Ti consegniamo il report

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

Scopri cosa è davvero sfruttabile nel tuo ambiente

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

Richiedi il tuo Vulnerability Assessment →

info@pentesterra.com · pentesterra.com/vulnerability-management