HADRIAN

EBOOK

Nella mente di un hacker

Automazione della sicurezza offensiva per gli asset esterni

Indice

Introduction

La “prospettiva esterna dell'hacker” è indispensabile per una sicurezza informatica solida, perché introduce un livello di controllo e di approfondimento che spesso i team interni non sono in grado di fornire. Sebbene gli esperti di sicurezza interni siano fondamentali per mantenere e rafforzare le difese di un'organizzazione, spesso sono vincolati da conoscenze accademiche, punti di vista limitati e familiarità con il sistema, che possono inavvertitamente creare punti ciechi. Gli hacker, invece, si approcciano a un sistema senza pregiudizi o preconcetti, simulando gli attacchi che sfruttano tali debolezze.

Un aspetto determinante di questa prospettiva esterna è la capacità di identificare le vulnerabilità dal punto di vista dell'aggressore. Gli hacker non si limitano a seguire tattiche note, ma si adattano, innovano e pensano in modo creativo a come aggirare le difese. Simulando il loro approccio, le organizzazioni possono scoprire punti deboli che altrimenti verrebbero trascurati dai team interni, che potrebbero concentrarsi su vulnerabilità più di routine o teoriche. In definitiva, una prospettiva esterna consente un approccio più completo alla sicurezza informatica, che rispecchia la natura dinamica e in continuo mutamento degli attacchi del mondo reale.

Che cos'è la sicurezza offensiva?

Anche la migliore sicurezza può essere aggirata se non viene implementata correttamente o testata con continuità. La sicurezza offensiva si riferisce all'approccio proattivo che prevede la simulazione del comportamento, delle tattiche e delle tecniche di un aggressore per valutare e testare la postura di sicurezza di un'organizzazione.

A differenza della sicurezza difensiva tradizionale, che si concentra sulla protezione dei sistemi e sulla risposta agli attacchi, la sicurezza offensiva ribalta lo schema. Mette i professionisti della sicurezza nel ruolo di “hacker”, cercando intenzionalmente di violare le difese dell'organizzazione per scoprire lacune e vulnerabilità.

L'obiettivo della sicurezza offensiva è quello di emulare le strategie di avversari reali, siano essi hacker esterni, minacce interne o persino attori di singoli Stati, in modo che le organizzazioni possano identificare e correggere i punti deboli prima che vengano sfruttati in un attacco reale.

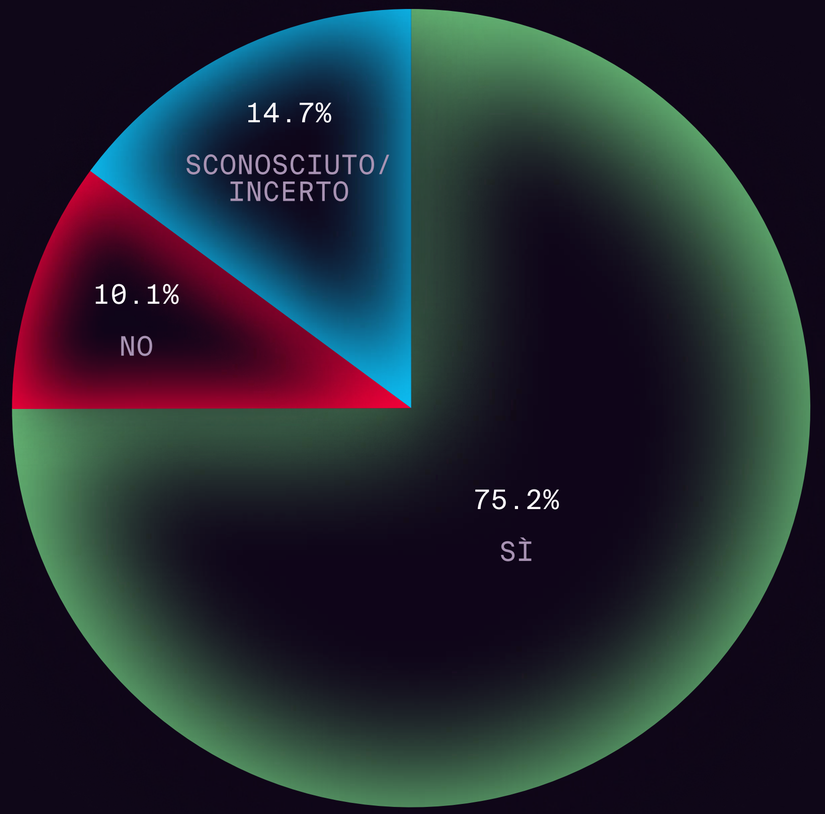
7/10

organizzazioni hanno subito un attacco che ha preso di mira un asset esterno sconosciuto, non gestito o gestito in modo inadeguato.[1]

69%

delle organizzazioni dichiara che il proprio approccio alla sicurezza è reattivo e basato sugli incidenti .[2]

Il rischio sconosciuto vi sta portando ad aumentare le pratiche di sicurezza offensive/proattive?



[1] ESG, Security Hygiene and Posture Management (2022) | [2] Ponemon, The Cybersecurity Illusion: The Emperor Has No Clothes (2019) |
[3] SANS, Building a Resilient Offensive Security Strategy (2023)

Perché concentrarsi sulla superficie di attacco esterna?

L'approccio di un hacker esterno potrebbe sfruttare una vulnerabilità o una debolezza che i team interni non avevano previsto o che consideravano troppo poco rischiosa per essere considerata prioritaria. Ciò rende la prospettiva dell'hacker uno strumento prezioso per verificare la solidità delle difese di sicurezza, assicurandosi che siano resistenti alle minacce attuali e in continua evoluzione.

Gli autori degli attacchi si evolvono più rapidamente di quanto si possano sviluppare le difese. L'unico modo per restare al passo è mettere continuamente alla prova le difese utilizzando la mentalità e i metodi di quanti cercano di sfruttarle. Senza questo approccio esterno, le organizzazioni rischiano di sottovalutare la complessità e la persistenza delle minacce moderne e di lasciare delle lacune critiche nella loro strategia di sicurezza.

Checklist per la prospettiva degli hacker:

- ✓ Abbiamo mappato tutti i punti di accesso alla nostra rete e ai nostri sistemi?
- ✓ Siamo al corrente di tutti gli asset presenti nel nostro ambiente, compresi lo shadow IT e i servizi cloud?
- ✓ Monitoriamo in modo continuo gli asset esterni (siti web, API, piattaforme cloud)?
- ✓ Teniamo conto di fornitori e appaltatori terzi che potrebbero introdurre nuovi rischi nel nostro ambiente?
- ✓ Quando è stata l'ultima volta che abbiamo condotto un Red Team o un penetration test e abbiamo controllato tutti gli elementi del nostro ambiente?

Fasi della sicurezza offensiva

La prospettiva dell'hacker viene rivelata dall'applicazione di una metodologia di sicurezza offensiva.

Ricognizione

La ricognizione, la prima fase della sicurezza offensiva, si concentra sulla raccolta di informazioni sui sistemi, le reti e la struttura organizzativa dell'obiettivo. Questa fase aiuta a identificare potenziali vettori di attacco e punti deboli, mappando le risorse e le relazioni, consentendo agli aggressori di individuare i punti di ingresso più vulnerabili.

Contestualizzazione

Questa fase esamina sistematicamente i sistemi rilevati per estrarre informazioni chiave come host attivi, porte aperte, servizi in esecuzione e stack tecnologici. Utilizzando tecniche di fingerprinting, gli aggressori identificano i sistemi e le vulnerabilità sottostanti, favorendo così la localizzazione dei punti deboli dell'ambiente.

Convalida

In questa fase, i punti deboli vengono presi di mira per accedere al sistema in modo non autorizzato o per aumentare i privilegi. L'obiettivo è verificare se tali vulnerabilità possano essere sfruttate per raggiungere gli obiettivi dell' aggressore, come accedere a dati sensibili o violare le reti interne, valutando al contempo l'efficacia dei controlli di sicurezza e della risposta agli incidenti.

Prioritizzazione

Dopo aver identificato le debolezze sfruttabili, la prioritizzazione valuta la gravità e il rischio posto da tali vulnerabilità nei sistemi, nelle reti e nelle applicazioni. Questa fase aiuta a determinare quali problemi devono essere affrontati per primi in base al loro potenziale impatto.

Procedura risolutiva

La fase finale, la procedura risolutiva, prevede la compilazione dei risultati in un report per l'organizzazione. Questo report comprende il percorso dell'attacco, le vulnerabilità sfruttate e le indicazioni per le correzioni, fungendo sia da guida immediata per le azioni correttive sia da roadmap strategica per i miglioramenti della sicurezza a lungo termine.

Automazione della sicurezza offensiva

L'automazione e l'IA possono migliorare la sicurezza offensiva in ogni fase.

Ricognizione

L'IA raccoglie e analizza rapidamente grandi quantità di dati provenienti da asset, reti e sistemi esterni, automatizzando attività come il rilevamento di asset, la raccolta di dati e l'aggregazione di informazioni sulle minacce.

Risultato: aumenta la visibilità della superficie di attacco esterna ed espande i test a tutti gli asset.

Contestualizzazione

L'automazione identifica host attivi, porte aperte, servizi e tecnologie in modo più rapido e accurato, correlandoli con exploit e tecniche di attacco conosciuti e fornendo maggiori informazioni sui rischi potenziali.

Risultato: migliora l'accuratezza del rilevamento delle minacce identificando ogni potenziale vulnerabilità.

Convalida

L'automazione simula gli attacchi per convalidare le vulnerabilità sfruttabili, mentre l'IA imita le tattiche più sofisticate degli avversari, aiutando a testare l'efficacia dei controlli di sicurezza.

Risultato: assicura un test realistico delle difese di sicurezza ed elimina i falsi positivi.

Prioritizzazione

L'IA aiuta a classificare le vulnerabilità in base all'impatto potenziale, alla sfruttabilità e al rischio organizzativo, consentendo ai team di sicurezza di concentrarsi sui problemi più urgenti.

Risultato: migliora l'allocazione delle risorse identificando le vulnerabilità con l'impatto più elevato.

Procedura risolutiva

L'automazione genera report azionabili con indicazioni personalizzate e tiene traccia dei progressi delle soluzioni correttive, mentre l'IA ottimizza le strategie risolutive in base al contesto organizzativo e ai vincoli legati alle risorse.

Risultato: semplifica le attività correttive e garantisce miglioramenti della sicurezza a lungo termine.

Approcci alla sicurezza offensivi a confronto

I casi d'uso e i punti di forza di ciascun approccio sono diversi e devono essere sovrapposti tra loro per un test di sicurezza olistico.

	Scansione delle vulnerabilità	Penetration testing	Red teaming	Automazione della sicurezza offensiva
Ambito di applicazione	Asset conosciuti	Infrastrutture critiche	In base agli obiettivi	Tutti gli asset esterni
Velocità	Ore	Da giorni a settimane	Da settimane a mesi	Minuti
Sofisticatezza	Base	Alta	Alta	Media
Frequenza	Come da programmazione	Da trimestrale ad annuale	Annuale	Basata sugli eventi
Strumenti	Automatizzato	Misto	Manuale	Automatizzato
Costo	Basso	Medio	Alto	Basso
Obiettivo	Test per le vulnerabilità note e i problemi di conformità	Identifica le vulnerabilità in sistemi o applicazioni specifici.	Valuta la risposta e la resilienza complessiva della sicurezza.	Rivela la prospettiva degli hacker per una procedura risolutiva proattiva

Il valore dell’automazione della sicurezza offensiva

Pensare come un hacker rivela il modo in cui gli attacchi reali potrebbero compromettere applicazioni e infrastrutture. L'automazione della sicurezza offensiva consente alle organizzazioni di comprendere questa prospettiva e di mitigare in modo proattivo le minacce.

Hadrian rivela le vulnerabilità sfruttabili valutando continuamente le minacce su tutto la superficie di attacco esterna, utilizzando le stesse tecniche e gli stessi comportamenti degli hacker.

A differenza dei penetration test statici, Hadrian offre un approccio dinamico ed evolutivo alla sicurezza che si adatta alla superficie di attacco in continua evoluzione. Grazie agli approfondimenti automatici e alla prioritizzazione dei rischi critici, Hadrian consente ai team di sicurezza di anticipare le minacce e di rafforzare le difese prima che si verifichino gli attacchi.

10x VISIBILITÀ DEI RISCHI CRITICI	Ottieni visibilità in tempo reale su ogni asset ed esposizione della tua superficie di attacco digitale. L'analisi 24 ore su 24, 7 giorni su 7 e 365 giorni su 365 di Hadrian ti tiene costantemente informato, riducendo al minimo la finestra di vulnerabilità.
10 ORE RISPARMIATE IN MEDIA A SETTIMANA	Concentrati sui rischi sfruttabili ed elimina i falsi positivi con penetration test approfonditi. Le valutazioni completamente automatizzate di Hadrian sono continue e arricchite da informazioni sulle minacce.
80% RIDUZIONE DEL TEMPO MEDIO DI RISOLUZIONE	Accelera i tempi di risposta e crea un cambiamento radicale nella postura di sicurezza. Hadrian attiva e orchestra i flussi di lavoro per semplificare la procedura risolutiva e impedire agli aggressori di attaccare.

Vantaggi per i principali stakeholder

Stakeholder	Benefici	Aree migliorate
CISO	I CISO acquisiscono una comprensione più approfondita della posizione di sicurezza dell'organizzazione, che permette di prendere decisioni più informate sulla gestione del rischio.	▪ Riduzione dell'esposizione al rischio ▪ Miglioramento del reporting a livello di consiglio di amministrazione ▪ Migliore allocazione delle risorse
Penetration tester	L'automazione semplifica le attività che richiedono tempo, come la scansione delle vulnerabilità e l'analisi dei dati, consentendo ai tester di concentrarsi sui problemi più urgenti.	▪ Test rapidi di exploit zero-day ▪ Automazione delle attività che richiedono tempo ▪ Indicazioni attuabili
Team SOC	Per il team SOC, assumere una mentalità da hacker aiuta ad anticipare i metodi di attacco avanzati e a perfezionare le capacità di rilevamento.	▪ Rilevamento dei rischi più rapido ▪ Minore quantità di falsi positivi ▪ Riduzione dei tempi di esecuzione delle procedure risolutive
Sviluppatori	Gli sviluppatori possono integrare perfettamente la sicurezza nel processo di distribuzione, con conseguente maggiore sicurezza delle applicazioni in produzione.	▪ Meno vulnerabilità durante la fase di produzione ▪ Patching più rapido dopo il rilascio ▪ Minor rischio di danni al brand
Reparto finanziario	Il reparto finanziario può quantificare meglio i potenziali impatti finanziari delle minacce informatiche e aiutare a stabilire le priorità nelle decisioni di investimento.	▪ Impatto finanziario dei rischi informatici più chiaro ▪ Miglioramento del budget per gli investimenti ▪ Migliore ROI sulla spesa per la sicurezza

Informazioni su Hadrian

Hadrian sta rivoluzionando la sicurezza offensiva attraverso l'automazione, consentendo ai team di sicurezza di operare più rapidamente e di scalare senza sforzo. Per scoprire le minacce, la nostra AI autonoma Orchestrator esegue test continui per valutare in modo completo le risorse rivolte a Internet. La tecnologia all'avanguardia è basata sul cloud, completamente priva di agenti e costantemente aggiornata e migliorata dal team di hacker etici di Hadrian.

Fiducia dei leader di mercato

NBC	amadeus	CRÉDIT AGRICOLE
AUTODESK	ABN·AMRO	London Business School
RITUALS...	SIEMENS energy	BLINQX

Orchestratore AI