CSP010_W_H

Argomento: Introduzione ai test di penetrazione della sicurezza informatica

ALLENATORI:
Paresh Rathod (Laurea)
Christos Grigoriadis (Focal Point) Ricardo Lugo (TALTECH)
Kitty Kioskli (Trustilio BV,)

PRESENTAZIONE DA PARTE DI:
Paresh Rathod
Università di Scienze Applicate di Laurea, Finlandia

CyberSecPro

Riconoscimento

- Finanziato dall'Unione Europea. I punti di vista e le opinioni espresse sono tuttavia esclusivamente quelli dell'autore o degli autori e non riflettono necessariamente quelli dell'Unione Europea o di HADEA. Né l'Unione Europea né l'autorità che concede il finanziamento possono essere ritenuti responsabili.
- Accordo di progetto n. 101083594

Introduzione ai test di penetrazione della sicurezza informatica

- Esplorate il ruolo critico dei test di penetrazione nella salvaguardia delle risorse digitali. Scoprite come gli hacker etici scoprono metodicamente le vulnerabilità per rafforzare la posizione di sicurezza informatica di un'organizzazione e prevenire costose violazioni dei dati.

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia

CyberSecPro

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia

Comprendere il panorama della sicurezza informatica

- Il panorama della sicurezza informatica è complesso e in continua evoluzione, con l'emergere di nuove minacce e vulnerabilità. Le imprese devono affrontare una sfida ardua per salvaguardare i propri asset digitali da attacchi informatici sofisticati. I test di penetrazione sono uno strumento fondamentale per le organizzazioni per valutare in modo proattivo la loro posizione di sicurezza e identificare i punti deboli prima che possano essere sfruttati.

CyberSecPro

Definizione di test di penetrazione

- Il test di penetrazione, noto anche come **hacking etico**, è la pratica di simulare attacchi informatici per valutare le difese di sicurezza di un'organizzazione.
- L'obiettivo è identificare e sfruttare sistematicamente le vulnerabilità nei sistemi, nelle reti e nelle applicazioni di un'organizzazione per valutarne sicurezza complessiva.
- I penetration tester agiscono come **avversari fidati e autorizzati** per scoprire i punti deboli che potrebbero essere sfruttati da attori malintenzionati, consentendo alle organizzazioni di rafforzare le proprie misure di sicurezza informatica.

Principi di hacking etico

Accesso autorizzato

I tester di penetrazione lavorano con il permesso e l'autorizzazione espliciti dell'organizzazione da testare, assicurandosi di rimanere entro i limiti legali ed etici.

Ridurre al minimo il danno

Gli hacker etici danno la priorità alla minimizzazione di qualsiasi potenziale interruzione o danno ai sistemi di destinazione durante il processo di test.

Divulgazione completa

I penetration tester forniscono un report completo e trasparente sulle vulnerabilità scoperte e sui passi compiuti per .

Miglioramento continuo

L'hacking etico è un processo iterativo, con l'obiettivo di migliorare continuamente la sicurezza di un'organizzazione nel tempo.

Tipi di test di penetrazione

- **Test di penetrazione della rete:** Valutazione della sicurezza dell'infrastruttura di rete interna ed esterna di un'organizzazione, compresi server, firewall e reti wireless.

- **Test di penetrazione delle applicazioni Web:** Identificazione delle vulnerabilità nelle applicazioni basate sul Web, come SQL injection, cross-site scripting (XSS) e altre minacce della Top 10 di OWASP.

- **Test di penetrazione delle applicazioni mobili:** Valutazione della sicurezza delle applicazioni mobili e delle loro interazioni con i sistemi backend, con particolare attenzione alla fuga di dati, all'autenticazione insicura e ad altre vulnerabilità specifiche dei dispositivi mobili.

Ricognizione e raccolta di informazioni

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia

1

Intelligence a sorgente aperta (OSINT)

Raccogliere le informazioni pubblicamente disponibili sull'organizzazione target da siti web, social media e altre fonti online per costruire una comprensione completa dei sistemi, dell'infrastruttura e delle potenziali vulnerabilità.

2

Scansione della rete e delle porte

Eseguire scansioni approfondite della rete e dei sistemi dell'obiettivo per identificare host attivi, porte aperte e servizi potenzialmente vulnerabili, gettando le basi per le fasi successive del test di penetrazione.

3

Identificazione delle vulnerabilità

Sfruttare strumenti specializzati e informazioni sulle minacce per identificare sistematicamente le vulnerabilità note, le configurazioni errate e i punti deboli nei sistemi e nelle applicazioni dell'obiettivo che potrebbero essere sfruttati durante il test di penetrazione.

Identificazione delle vulnerabilità e Analisi

Approccio sistematico

I penetration tester seguono una metodologia strutturata per identificare sistematicamente le vulnerabilità nei sistemi, nelle reti e nelle applicazioni dell'obiettivo. Ciò include l'uso di strumenti e tecniche specializzate per scoprire i punti deboli.

Scansione delle vulnerabilità

Gli strumenti di scansione automatica delle vulnerabilità vengono utilizzati per analizzare l'ambiente di destinazione alla ricerca di vulnerabilità note, configurazioni errate e potenziali punti di accesso che potrebbero essere sfruttati dagli aggressori.

Verifica manuale

I tester di penetrazione verificano e convalidano manualmente le vulnerabilità identificate, assicurando l'accuratezza dei risultati e ottenendo una comprensione più approfondita dell'impatto potenziale e della possibilità di sfruttamento.

Valutazione del rischio

Una volta identificate le vulnerabilità, i penetration tester valutano il rischio che esse rappresentano per l'organizzazione, considerando fattori quali la probabilità di sfruttamento e il potenziale impatto di un attacco riuscito.

Tecniche di sfruttamento

Sfruttamento delle vulnerabilità

Sfruttare le vulnerabilità identificate per ottenere un accesso non autorizzato a sistemi, reti o applicazioni target.

Sviluppo di exploit

Sviluppare codice di exploit personalizzato per automatizzare lo sfruttamento delle vulnerabilità scoperte per ottenere un accesso più profondo.

Escalation dei privilegi

Elevare i privilegi degli utenti per ottenere livelli più elevati di accesso e controllo all'interno dell'ambiente di destinazione.

Mantenimento dell'accesso

Implementare backdoor e altre tecniche per mantenere l'accesso a lungo termine ai sistemi compromessi.

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia

Strategie di escalation dei privilegi

Vulnerabilità del sistema

ıttare bug e configurazioni errate del software per ottenere un livello elevato di sicurezza.

accesso.

Raccolta di credenziali

Ottenere le credenziali di amministrazione tramite phishing, keylogging o altri mezzi.

Dirottamento del servizio

Sfruttare servizi non configurati correttamente per eseguire comandi con privilegi più elevati.

L'escalation dei privilegi è una fase critica dei test di penetrazione, che consente all'hacker etico di ottenere un accesso elevato e il controllo del sistema di destinazione. Identificando e sfruttando sistematicamente le vulnerabilità, acquisendo credenziali di alto livello e dirottando i servizi privilegiati, il penetration tester può avanzare in profondità nella rete e accedere a risorse sensibili.

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia

Movimento laterale e persistenza

1

Escalation dei privilegi

Utilizzate l'accesso elevato ottenuto tramite tecniche di escalation dei privilegi per spostarvi lateralmente sulla rete di destinazione.

2

Sfruttare le relazioni di fiducia

Sfruttare connessioni affidabili tra sistemi e account per ottenere l'accesso a risorse e dati aggiuntivi.

3

Stabilire la persistenza

Implementare backdoor, attività programmate e altri meccanismi per mantenere l'accesso a lungo termine ai sistemi compromessi.

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia

Mantenere l'accesso e coprire le tracce

1

Meccanismi di persistenza

Implementare backdoor, attività programmate e altre tecniche per mantenere l'accesso a lungo termine ai sistemi compromessi, anche dopo lo sfruttamento iniziale.

2

Copertura delle tracce

Cancellare accuratamente i registri, eliminare le cronologie del browser e rimuovere altre prove delle attività di penetration test per evitare di essere scoperti dai team di sicurezza.

3

Offuscamento e furtività

Utilizzate tecniche come il process hollowing, l'iniezione di codice e il malware senza file per confondersi con la normale attività del sistema ed evitare di attivare gli avvisi di sicurezza.

4

Esfiltrazione e furto di dati

Estrarre in modo sicuro i dati sensibili dall'ambiente di destinazione, sfruttando la crittografia e altri metodi per evitare il rilevamento durante il processo di trasferimento dei dati.

Rapporti e documentazione

La fase finale del processo di penetration test prevede la stesura di un rapporto completo e di una documentazione approfondita. I penetration tester documentano meticolosamente le loro attività, i risultati e le raccomandazioni per fornire una chiara comprensione della posizione di sicurezza dell'organizzazione.

Componenti del rapporto	Descrizioni dettagliate della metodologia di test, delle vulnerabilità scoperte e del potenziale impatto sull'organizzazione.
Dettagli sulla vulnerabilità	Analisi approfondita di ogni vulnerabilità, compreso il livello di rischio, i passaggi per riprodurre il problema e i suggerimenti per porvi rimedio.
Guida alla riparazione	Raccomandazioni prioritarie per affrontare le vulnerabilità identificate e rafforzare la sicurezza complessiva dell'organizzazione.
Sintesi	Una panoramica di alto livello dell'attività di penetration testing, che evidenzia i risultati principali e le raccomandazioni per i dirigenti. livello di stakeholder.

Valutazione della vulnerabilità vs. test di penetrazione

La valutazione delle vulnerabilità e i test di penetrazione sono entrambi componenti essenziali di una strategia completa di cybersecurity, ma hanno scopi diversi.

La valutazione delle vulnerabilità si concentra sull'identificazione e sulla catalogazione dei potenziali punti deboli nei sistemi, nelle reti e nelle applicazioni di un'organizzazione. Fornisce una panoramica completa della postura di sicurezza.

I test di penetrazione, invece, prevedono lo sfruttamento attivo delle vulnerabilità identificate per valutare l'impatto reale e il rischio che esse comportano per l'organizzazione. Simula le tattiche e le tecniche di un attaccante malintenzionato.

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia

Metodologie di test di penetrazione

1

Pianificazione

Definire l'ambito, gli obiettivi e le regole di ingaggio.

2

Raccolta di informazioni

Condurre ricognizioni e scoprire le vulnerabilità del sistema.

3

Sfruttamento

Sfruttare le vulnerabilità identificate per ottenere accesso e controllo.

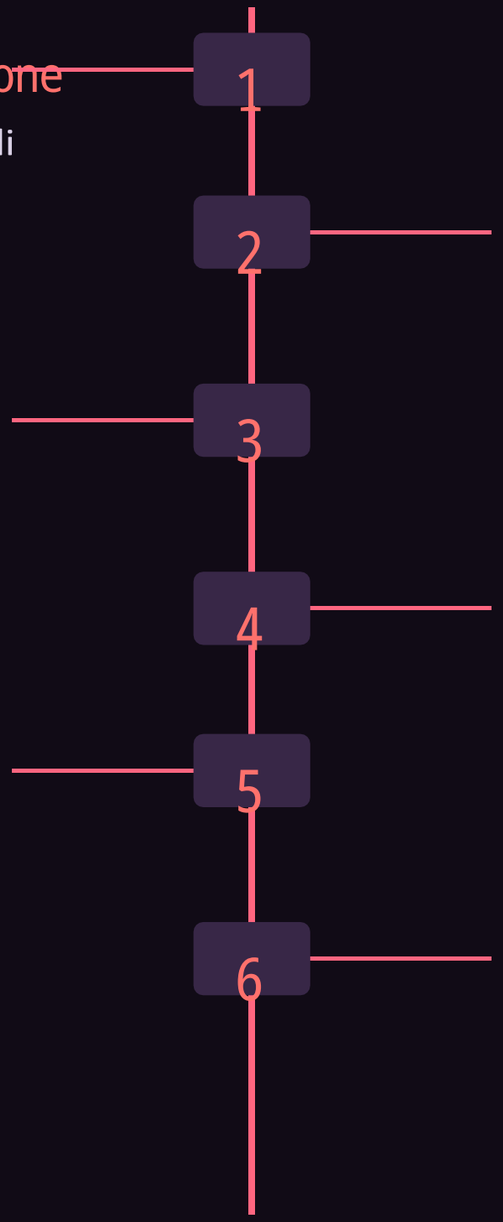
4

Post-sfruttamento

Mantenere l'accesso, aumentare i privilegi ed esfiltrare i dati.

Le metodologie di test di penetrazione seguono un approccio strutturato per valutare la posizione di sicurezza di un'organizzazione. Ciò comprende un'attenta pianificazione, la raccolta di informazioni complete, lo sfruttamento mirato delle vulnerabilità e le attività successive allo sfruttamento per valutare l'impatto reale dei potenziali attacchi.

Ciclo di vita dei test di penetrazione



1 Pianificazione

Stabilire con chiarezza obiettivi, ambito e regole di impegno per il test di penetrazione.

2 Raccolta di informazioni

Condurre una ricognizione per raccogliere informazioni sull'ambiente bersaglio e identificare potenziali vulnerabilità.

3 Valutazione della vulnerabilità

Eseguire la scansione e l'analisi sistematica dei sistemi di destinazione per individuare i punti deboli della sicurezza.

4 Sfruttamento

Sfruttare le vulnerabilità scoperte per ottenere accesso e controllo non autorizzati sui sistemi di destinazione.

5 Post-sfruttamento

Mantengono l'accesso persistente, aumentano i privilegi ed esplorano la rete compromessa alla ricerca di informazioni sensibili.

6 Segnalazione

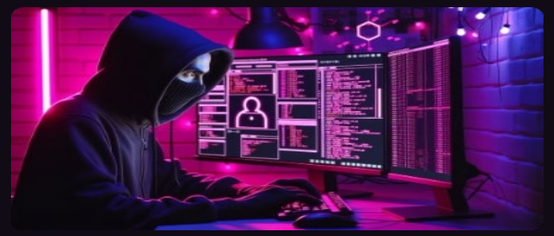
Documentare accuratamente l'intero processo di penetration test e fornire risultati e raccomandazioni dettagliate.

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia

Strumenti e tecniche per i test di penetrazione

Kali Linux

Una popolare distribuzione Linux progettata specificamente per i test di penetrazione, che fornisce una suite completa di strumenti per la scansione della rete, l'analisi delle vulnerabilità e lo sviluppo di exploit.



Metasploit

Un framework di penetration test flessibile e ampiamente utilizzato che semplifica il processo di identificazione, sfruttamento e reporting delle vulnerabilità di sicurezza all'interno dei sistemi target.

Suite di rutti

Una suite completa per i test di sicurezza delle applicazioni web che consente ai penetration tester di intercettare, analizzare e manipolare il traffico web per identificare e sfruttare le vulnerabilità.

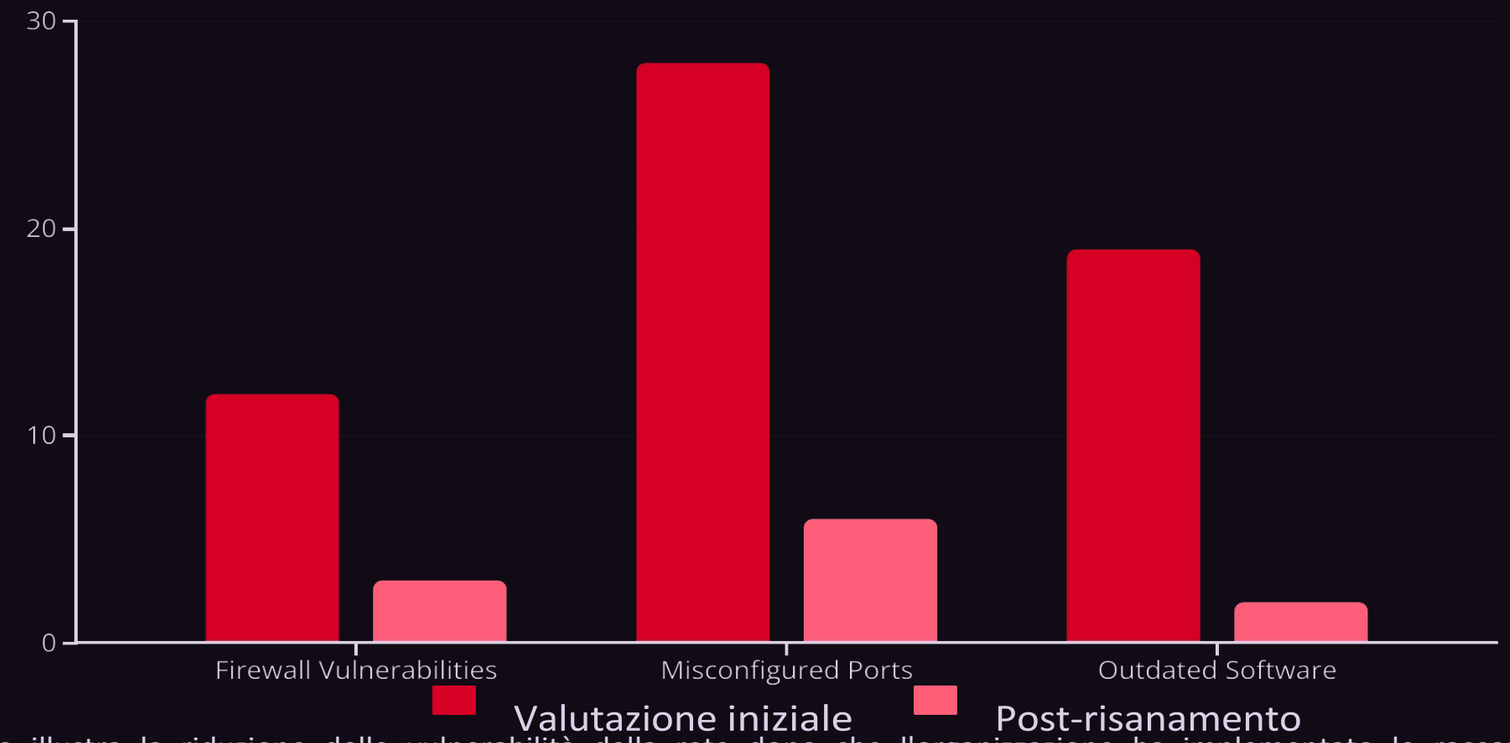
Wireshark

Un analizzatore di protocolli di rete che consente ai penetration tester di catturare, ispezionare e analizzare il traffico di rete, aiutando a identificare le vulnerabilità della sicurezza e a comprendere il comportamento della rete.

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia

Test di penetrazione della rete

I test di penetrazione della rete sono una componente cruciale delle valutazioni di cybersecurity complete. Si tratta di sondare e sfruttare sistematicamente le vulnerabilità all'interno dell'infrastruttura di rete di un'organizzazione per identificare i potenziali punti di ingresso per gli attori malintenzionati.



Il grafico illustra la riduzione delle vulnerabilità della rete dopo che l'organizzazione ha implementato le raccomandazioni del test di penetrazione della rete. Affrontando le debolezze del firewall, le porte non configurate correttamente e il software obsoleto, la sicurezza della rete è stata notevolmente migliorata.

Test di penetrazione delle applicazioni web

I test di penetrazione delle applicazioni web sono essenziali per scoprire le vulnerabilità che potrebbero essere sfruttate da attori malintenzionati. I tester utilizzano tecniche avanzate per identificare e sfruttare le falle nell'architettura delle applicazioni web, nell'autenticazione, nell'autorizzazione e nella convalida degli input.

Simulando attacchi reali, i penetration tester possono valutare il rischio reale e l'impatto delle vulnerabilità delle applicazioni web, consentendo alle organizzazioni di dare priorità agli sforzi di rimedio e di rafforzare la loro postura di sicurezza complessiva.

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia

Test di penetrazione delle applicazioni mobili

Vulnerabilità delle app

Identificare le falle di sicurezza nel codice delle app mobili, nell'archiviazione dei dati e nei protocolli di comunicazione che potrebbero essere sfruttate dagli aggressori.

Bypass dell'autenticazione

Verificare la presenza di meccanismi di autenticazione deboli che consentono l'accesso non autorizzato a funzioni e dati sensibili dell'applicazione.

Perdita di dati

Scoprire informazioni sensibili, credenziali e dati personali, che potrebbero essere esposte dall'applicazione mobile.

Tracciamento della posizione

Valutare le funzionalità di geolocalizzazione dell'applicazione e identificare i potenziali rischi per la privacy o l'uso improprio dei dati di localizzazione.

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia

Test di penetrazione dell'infrastruttura cloud

I test di penetrazione dell'infrastruttura cloud sono fondamentali per identificare le vulnerabilità e convalidare la sicurezza delle risorse cloud-based di un'organizzazione. I tester utilizzano una serie di tecniche per valutare la sicurezza dei servizi cloud, delle macchine virtuali, dei container e delle relative tecnologie cloud-native.

Controllo della configurazione del cloud

I tester di penetrazione esaminano le configurazioni del cloud per identificare configurazioni errate, controlli di accesso troppo permissivi e altri punti deboli che potrebbero essere sfruttati dagli aggressori.

Test di sicurezza API

I tester esaminano la sicurezza delle API basate sul cloud, valutando l'autenticazione, l'autorizzazione e la convalida degli input per scoprire le vulnerabilità che potrebbero portare alla violazione dei dati o alla compromissione del sistema.

Valutazione della sicurezza dei container

I test di penetrazione degli ambienti containerizzati, compresi Docker e Kubernetes, aiutano a identificare le potenziali vulnerabilità nelle immagini dei container, nelle configurazioni di runtime e nei framework di orchestrazione.

Gestione dell'identità e degli accessi nel cloud

I tester valutano la sicurezza dei sistemi di gestione delle identità e degli accessi (IAM) basati sul cloud, valutando i privilegi degli utenti, i controlli di accesso basati sui ruoli e i percorsi di escalation dei privilegi.

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia

Attacchi di ingegneria sociale

- Phishing: e-mail o messaggi maligni progettati per indurre gli utenti a rivelare informazioni sensibili o a compiere azioni dannose.
- Pretestuosità: Creare uno scenario inventato per manipolare l'obiettivo e indurlo a divulgare dati riservati o a concedere un accesso non autorizzato.
- Adescamento: Lasciare supporti fisici infettati da malware (come le unità USB) in un luogo pubblico, invogliando l'obiettivo a inserirli nel proprio dispositivo.

Risposta agli incidenti e bonifica

Preparazione

Sviluppare un piano di risposta agli incidenti e formare il personale.

Rilevamento e analisi

Identificare l'incidente, valutare l'impatto e raccogliere le prove.

Contenimento e sradicamento

Limitare i danni, eliminare la minaccia e ripristinare le normali operazioni.

Recupero e lezioni apprese

Ripristinare dati, sistemi e servizi e documentare i risultati per migliorare le risposte future.

Una risposta e una bonifica efficaci degli incidenti sono fondamentali per ridurre al minimo l'impatto delle violazioni della sicurezza e garantire la resilienza dell'organizzazione. Questo approccio strutturato comprende la preparazione agli incidenti, la loro rapida individuazione e analisi, il contenimento dei danni e infine il recupero, imparando dall'esperienza.

Conformità normativa e test di penetrazione

I test di penetrazione svolgono un ruolo cruciale nel garantire la conformità alle normative. Le organizzazioni devono aderire a standard e normative specifiche del settore, come PCI-DSS, HIPAA e GDPR, che impongono valutazioni regolari della sicurezza per identificare e ridurre le vulnerabilità.

I test di penetrazione aiutano le organizzazioni a dimostrare la conformità, fornendo prove delle loro misure di sicurezza e dell'efficacia delle loro strategie di gestione del rischio. I rapporti dettagliati generati da questi test servono come documentazione per gli enti normativi e i revisori.

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia

Le migliori pratiche per i test di penetrazione

Definire chiaramente l'ambito di applicazione

Stabilire i confini, le attività e gli obiettivi per garantire che il test di penetrazione sia in linea con le esigenze dell'organizzazione.

Sfruttare l'hacking etico

Utilizzate le stesse tecniche e gli stessi strumenti utilizzati dagli aggressori del mondo reale per scoprire le vulnerabilità.

Privilegiare le vulnerabilità

Concentrarsi sulle questioni più critiche che rappresentano il rischio più elevato per l'organizzazione.

Mantenere la professionalità

Condurre la valutazione in modo etico, legale e senza causare danni o disagi involontari.

Certificazioni e qualifiche per i test di penetrazione

$50K

Stipendio medio

I tester di penetrazione con le giuste certificazioni possono ottenere stipendi elevati nel mercato del lavoro della cybersecurity.

100+

Opzioni di certificazione

Per i professionisti dei test di penetrazione è disponibile un'ampia gamma di certificazioni neutre e specifiche per i fornitori.

80%

Priorità di assunzione

I datori di lavoro spesso danno la priorità ai candidati con certificazioni e qualifiche riconosciute nel campo dei test di penetrazione.

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia

Test di penetrazione come servizio (PTaaS)

Il PTaaS è un modello emergente in cui le organizzazioni esternalizzano le proprie esigenze di penetration testing a fornitori specializzati in cybersecurity. Questo approccio offre numerosi vantaggi, tra cui l'accesso a tester esperti, risorse scalabili e monitoraggio continuo della sicurezza.

PTaaS semplifica il processo di penetration test, fornendo alle organizzazioni valutazioni di sicurezza complete e raccomandazioni personalizzate per i loro requisiti specifici, riducendo al minimo l'onere per i team IT interni.

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia

Test di penetrazione per piccole e Medie imprese

Le piccole e medie imprese (PMI) si trovano spesso ad affrontare sfide uniche in materia di cybersecurity a causa di risorse e competenze limitate. I test di penetrazione possono fornire a queste organizzazioni un modo economico per identificare e risolvere le vulnerabilità, proteggendo i dati sensibili e i sistemi critici.

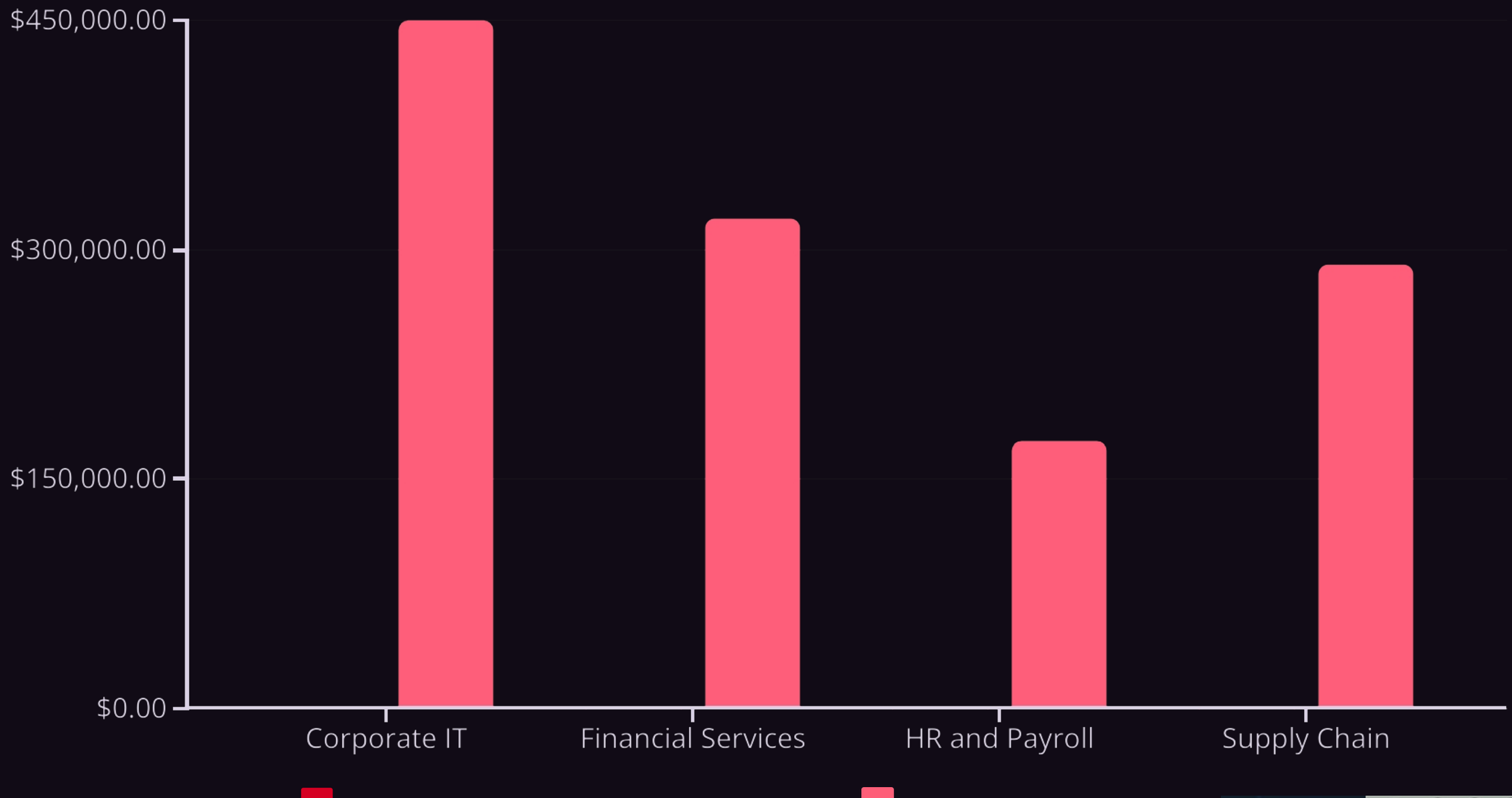
- **Valutazioni su misura:** I test di penetrazione per le PMI possono essere personalizzati per concentrarsi sui rischi specifici e sui vettori di attacco rilevanti per il settore, le dimensioni e l'infrastruttura.
- **Raccomandazioni pratiche:** I risultati dei test di penetrazione forniscono PMI indicazioni utili per migliorare la loro posizione di sicurezza, dando priorità alle fasi di rimedio di maggiore impatto.
- **Conformità e normative:** I test di penetrazione possono aiutare le PMI a dimostrare la conformità agli standard e alle normative del settore, come HIPAA, PCI-DSS e GDPR.

Test di penetrazione per le aziende Organizzazioni

I test di penetrazione sono fondamentali per le grandi aziende con infrastrutture IT complesse e dinamiche. Queste organizzazioni devono affrontare rischi di cybersecurity più elevati e garantire la sicurezza delle loro vaste reti, delle applicazioni critiche e dei dati sensibili. I test di penetrazione completi aiutano i clienti di livello aziendale a identificare le vulnerabilità, a convalidare i controlli di sicurezza e a rafforzare la loro posizione di sicurezza complessiva.

Il grafico a barre evidenzia il numero di vulnerabilità riscontrate e i relativi costi di ripristino nelle diverse unità aziendali di una grande impresa. Questi dati granulari consentono all'organizzazione stabilire le priorità e di allocare efficacemente le risorse per affrontare i problemi di sicurezza più critici.

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia



Tendenze emergenti nei test di penetrazione

1

Automazione e valutazioni guidate dall'intelligenza artificiale

L'ascesa di strumenti dotati di intelligenza artificiale in grado di scansionare autonomamente le vulnerabilità e lanciare attacchi per identificare i punti deboli su scala, riducendo l'impegno manuale necessario per i test di penetrazione.

2

Attacchi ransomware simulati

Penetration tester che conducono simulazioni realistiche di ransomware per valutare la capacità di un'organizzazione di rilevare, rispondere e recuperare da queste devastanti minacce informatiche.

3

Test dell'infrastruttura cloud

Maggiore attenzione alla sicurezza degli ambienti cloud attraverso test di penetrazione completi delle applicazioni, dell'infrastruttura e dei servizi basati su cloud per scoprire le configurazioni errate e le vulnerabilità.

Il futuro dei test di penetrazione della sicurezza informatica

I test di penetrazione diventeranno sempre più automatizzati e guidati dall'intelligenza artificiale, sfruttando l'apprendimento automatico e l'analisi avanzata per identificare e sfruttare le vulnerabilità a velocità e scala senza precedenti. Tecnologie emergenti come l'informatica quantistica e i droni autonomi rivoluzioneranno il modo in cui le organizzazioni valutano e si difendono dalle minacce informatiche in evoluzione.

Il monitoraggio continuo e in tempo reale e la caccia proattiva alle minacce saranno la norma, con test di penetrazione perfettamente integrati nel ciclo di vita della sicurezza di un'organizzazione. Gli hacker etici lavoreranno a fianco dei sistemi intelligenti per scoprire i rischi nascosti e convalidare l'efficacia dei controlli di sicurezza in ambienti IT complessi e dinamici.

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia

Conclusioni e risultati principali

1

La sicurezza informatica rimane una priorità assoluta

I test di penetrazione sono una componente fondamentale di una strategia di cybersecurity completa, che aiuta le organizzazioni a stare al passo con l'evoluzione delle minacce e a garantire la protezione dei loro beni preziosi.

3

Conformità e governance I regolari test di penetrazione aiutano le organizzazioni a dimostrare la conformità alle normative.

conformità, ridurre i rischi e mantenere la fiducia dei clienti e degli stakeholder.

2

L'hacking etico è essenziale

Impiegando le stesse tattiche e tecniche degli aggressori del mondo reale,

I test di penetrazione consentono alle organizzazioni di scoprire le vulnerabilità e rafforzare le difese di sicurezza.

4

Miglioramento continuo

Le attività di penetration test e di remediation sono fondamentali per tenere il passo con l'evoluzione del panorama della cybersecurity e per garantire la resilienza a lungo termine di un'organizzazione.

Riferimenti

1. IEEE. (2016). Codice etico IEEE. https://www.ieee.org/about/corporate/governance/p7-8.html
2. Codice etico e di condotta professionale ACM (2018). Association for Computing Machinery. https://www.acm.org/code-of- etica
3. Barquin, R. C. (1992, 7 maggio). Alla ricerca dei "dieci comandamenti" per l'etica informatica. Istituto di etica informatica. https://en.wikipedia.org/wiki/Ten_Commandments_of_Computer_Ethics
4. I Dieci comandamenti dell'etica informatica, creati nel 1992 dal Computer Ethics Institute, offrono una serie di principi fondamentali per un uso etico del computer (Barquin, 1992).
5. Agenzia dell'Unione europea per la sicurezza informatica. (2022). ECSF, quadro europeo delle competenze in materia di cibersicurezza. Ufficio delle pubblicazioni. https://doi.org/10.2824/859537
6. R. Schoon e S. Kleinaltepohl, Cybersecurity in the Electricity Sector: Managing Critical Infrastructure (SpringerLink, 2018).
7. J. R. Vacca, Industrial Cybersecurity for Engineers (Elsevier, 2015).
8. ECSO, "Energy Networks and Smart Grids", Cyber Security for the Energy Sector, WG3, Sectoral Demand, novembre 2018 URL: https://ecs-org.eu/ecso-uploads/2022/10/5fdb2673903c6.pdf
9. ENISA, "Smart Grid Threat Landscape and Good Practice Guide", dicembre 2013, URL: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide.
10. Altri riferimenti elencati in ogni argomento del modulo CSP

Trasparenza: Fonti

1. Contenuto del video teaser: Il contenuto di questo video teaser si basa sui Deliverable del Work Package 3 del progetto CyberSecPro con il prezioso contributo dei partner CyberSecPro.
2. Competenza linguistica: Il prodotto D3.1 è stato sottoposto a una rigorosa revisione linguistica. Ciò ha comportato l'utilizzo di Grammarly AI e la revisione meticolosa da parte di un madrelingua inglese.
3. Contenuti multimediali: Le immagini, i video e l'audio utilizzati sono stati reperiti da Pictory, Getty Images e altri database multimediali aperti.
4. Collaborazione con i partner: Riconosciamo il contributo dei nostri partner CyberSecPro, comprese le foto dei formatori presenti nel programma.
5. Materiale didattico: I materiali didattici per questo modulo di CyberSecPro sono stati forniti da un formatore elencato e il merito va agli autori.
6. Credito creativo: video teaser creato utilizzando queste risorse dal professionista europeo della sicurezza informatica Paresh Rathod.
7. I materiali della formazione sono stati creati utilizzando la letteratura accademica e di ricerca e i materiali didattici aperti (OEM) con i dovuti crediti agli autori.
8. Alcuni materiali hanno utilizzato strumenti basati sull'intelligenza artificiale, tra cui simulatori vocali (con i dovuti crediti agli autori) per fornire ai partecipanti le migliori esperienze di apprendimento.

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia

Connettersi con CyberSecPro: come registrarsi e altre informazioni pratiche

1. Sito web: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Grazie

Si prega di inviare tutte le domande ai formatori (e/o):
paresh.rathod@laurea.fi

CSP010_W_H:
Formatore: Paresh Rathod, Laurea UAS, Finlandia