Penetration test nella sicurezza informatica



Nell’era contemporanea, dove l’infrastruttura digitale costituisce l’ossatura portante della civiltà moderna, la protezione dei confini informatici ha assunto una rilevanza paradigmatica. Il penetration testing, comunemente definito pentest, rappresenta non solo una metodologia investigativa, ma un’autentica filosofia esplorativa dei limiti della sicurezza informatica, configurandosi come una simulazione offensiva controllata che saggia l’integrità dei sistemi. In un contesto caratterizzato dalla proliferazione esponenziale delle superfici d’attacco e dall’evoluzione costante delle minacce cibernetiche, questa pratica si erge a baluardo epistemologico nell’identificazione preventiva delle vulnerabilità sistemiche.

La genealogia metodologica del penetration test

Il penetration testing affonda le proprie radici concettuali nella tradizione militare delle “red team exercises”, esercitazioni antagonistiche finalizzate a identificare vulnerabilità attraverso l’emulazione di avversari. Questa pratica ha subito una metamorfosi significativa con l’avvento dell’informatica distribuita, divenendo un protocollo formale di analisi della resilienza sistemica. La metodologia contemporanea si articola in un framework procedurale rigoroso che comprende fasi sequenziali:

1. **Ricognizione (Reconnaissance):** Acquisizione di intelligence sui target designati mediante tecniche OSINT (Open Source Intelligence) e passive fingerprinting

2. **Scansione (Scanning):** Mappatura topologica dell'ecosistema informatico attraverso l'analisi delle superfici d'attacco
3. **Enumerazione (Enumeration):** Catalogazione dettagliata dei servizi esposti e delle potenziali vulnerabilità
4. **Exploitation:** Tentativo calibrato di compromissione mediante l'applicazione di tecniche offensive
5. **Post-exploitation:** Valutazione dell'impatto potenziale mediante l'analisi dell'escalation del privilegio
6. **Documentazione (Reporting)**: Sintesi analitica delle vulnerabilità identificate e proposta di mitigazioni

Questa tassonomia metodologica, lungi dall'essere monolitica, si caratterizza per una natura adattiva che rispecchia la fluidità dell'ecosistema tecnologico contemporaneo. L'iterazione ciclica di queste fasi configura un processo dialettico di affinamento continuo, in cui ogni ciclo arricchisce il corpus conoscitivo e perfeziona l'efficacia dell'approccio.

L'ecosistema tecnologico del Penetration Testing

L'arsenale strumentale del penetration tester moderno comprende un vasto repertorio di tecnologie specialistiche. Kali Linux emerge come distribuzione paradigmatica, integrando oltre 600 strumenti dedicati all'auditing della sicurezza. Metasploit Framework rappresenta l'infrastruttura modulare per l'automazione dell'exploitation, mentre Burp Suite costituisce lo standard de facto per l'analisi delle applicazioni web.

La crescente complessità degli ecosistemi ha favorito l'emergere di approcci specialistici:

- **Web Application Penetration Testing:** Focalizzato sull'identificazione di vulnerabilità OWASP Top 10, con particolare attenzione alle problematiche emergenti

quali Server-Side Request Forgery (SSRF) e prototype pollution

- **Mobile Application Testing:** Orientato all'analisi delle superfici d'attacco specifiche degli ecosistemi iOS e Android, includendo l'ispezione del codice binario tramite tecniche di reverse engineering e l'analisi del traffico di rete crittografato
- **Network Infrastructure Testing:** Concentrato sulla valutazione dell'architettura di rete, incluse tecnologie emergenti come SDN (Software-Defined Networking) e NFV (Network Function Virtualization)
- **Social Engineering Assessment:** Mirato all'analisi del fattore umano come vettore di compromissione, integrando simulazioni di phishing mirato e tecniche di pretexting sofisticate
- **Physical Security Testing:** Integrazione dell'analisi dei controlli di accesso fisico nell'approccio olistico alla sicurezza, includendo bypass di sistemi RFID e meccanismi biometrici
- **Cloud Infrastructure Testing:** Specificamente orientato all'analisi delle configurazioni erronee e delle vulnerabilità inerenti agli ambienti multi-cloud e ibridi
- **IoT Security Assessment:** Dedicato all'esplorazione delle vulnerabilità peculiari dei dispositivi interconnessi, spesso caratterizzati da vincoli computazionali e implementazioni crittografiche sub-ottimali

Questa frammentazione specialistica riflette la crescente eterogeneità dei paradigmi tecnologici, richiedendo un approccio multidisciplinare che trascende la mera competenza tecnica per abbracciare una comprensione olistica delle architetture complesse.

La dimensione normativa e compliance: evoluzione e convergenza dei framework regolatori

Il penetration testing si colloca all'intersezione tra imperativo tecnico e obbligo normativo, in un panorama regolatorio caratterizzato da crescente complessità e progressiva armonizzazione transnazionale. Il framework NIST SP 800-115, recentemente aggiornato nella revisione del 2023, fornisce linee guida metodologiche per la conduzione di test di sicurezza, introducendo considerazioni specifiche per tecnologie emergenti quali infrastrutture cloud ibride e sistemi IoT enterprise-grade. Parallelamente, lo standard ISO/IEC 27001:2022 ha rafforzato il requisito dei penetration test come componente essenziale del processo di verifica dell'efficacia dei controlli, con la clausola 9.2 che prescrive esplicitamente "valutazioni tecniche indipendenti" per verificare l'implementazione dei controlli di sicurezza.

Il panorama regolatorio europeo ha subito una significativa evoluzione con l'implementazione della direttiva NIS2 (Network and Information Systems), entrata in vigore nel gennaio 2023, che espande significativamente l'ambito di applicazione della precedente direttiva NIS, includendo esplicitamente il requisito di "security testing regolare" per le entità essenziali e importanti. Questa disposizione, in sinergia con il GDPR (General Data Protection Regulation), ha ulteriormente enfatizzato l'importanza dei penetration test come strumento di verifica dell'adeguatezza delle misure tecniche.

L'articolo 32 del GDPR prescrive esplicitamente "una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento", mentre le linee guida

dell’European Data Protection Board (EDPB) del 2024 specificano che tali test devono includere “simulazioni realistiche di tentativi di violazione”, de facto codificando il penetration testing come componente necessaria della compliance.

L’implementazione del Digital Operational Resilience Act (DORA), la cui piena applicazione è prevista per gennaio 2025, introduce ulteriori requisiti specifici per il settore finanziario europeo, prescrivendo “advanced penetration testing based on threat intelligence” su base annuale per le entità finanziarie critiche. Questo approccio intelligence-driven rappresenta un’evoluzione significativa rispetto al testing tradizionale, richiedendo l’emulazione di tattiche, tecniche e procedure (TTP) associate a threat actor specifici.

Nel contesto statunitense, l’evoluzione normativa è caratterizzata da un approccio settoriale più frammentato. Nel settore finanziario, il framework FFIEC (Federal Financial Institutions Examination Council) ha integrato nella revisione del 2023 requisiti specifici per il penetration testing delle tecnologie emergenti, con particolare attenzione alle architetture Zero Trust e alle infrastrutture cloud.

La Securities and Exchange Commission (SEC), con la Rule S7-09-22 del marzo 2024, ha introdotto l’obbligo per le entità registrate di condurre “periodic independent cybersecurity assessments”, specificando che tali valutazioni devono includere “penetration testing of critical systems”. Nel contesto sanitario statunitense, la normativa HIPAA è stata integrata dalla pubblicazione nel 2024 delle “OCR Cybersecurity Guidelines”, che esplicitano l’aspettativa che le covered entities implementino processi di verifica della sicurezza che includano penetration testing periodici.

Analogamente, nel settore energetico, la North American Electric Reliability Corporation (NERC) ha aggiornato nel 2023 i Critical Infrastructure Protection (CIP) standards per

includere requisiti specifici di “vulnerability assessment and penetration testing” per le infrastrutture critiche energetiche.

A livello globale, si osserva una convergenza progressiva verso l’adozione di framework armonizzati, con il NIST Cybersecurity Framework (CSF) 2.0, pubblicato nel febbraio 2024, che emerge come riferimento meta-normativo transnazionale. Il CSF 2.0 include esplicitamente il penetration testing come pratica di controllo (ID.RA-P5) nella categoria “Identify”, consolidando il suo ruolo come strumento fondamentale nella governance del rischio informatico a livello globale.

Significativa è anche l’evoluzione dell’approccio regolatorio verso i requisiti di attestazione e certificazione. Il framework di certificazione EUCC (Common Criteria based European candidate cybersecurity certification scheme) dell’ENISA prescrive, per i livelli di assurance sostanziale ed elevato, la conduzione di penetration test da parte di laboratori accreditati, mentre lo schema di certificazione EU Cloud Services (EUCS) include requisiti analoghi per i servizi cloud. Parallelamente, nel contesto ISO, lo standard ISO/IEC 29147:2024 sulla “Vulnerability Disclosure” completa il quadro normativo fornendo linee guida per la gestione responsabile delle vulnerabilità identificate durante i penetration test.

In Asia, il Cybersecurity Act di Singapore ha subito un emendamento significativo nel 2023, introducendo il concetto di “Critical Information Infrastructure Protection Program” che include requisiti specifici di penetration testing per le infrastrutture critiche. In Giappone, il Financial Services Agency ha pubblicato nel 2024 le “Guidelines for Financial Institutions’ Cybersecurity”, che allineano i requisiti di penetration testing giapponesi con gli standard internazionali, mentre in Cina la Personal Information Protection Law (PIPL) e la Data Security Law (DSL) configurano un framework composito che implicitamente richiede testing di

sicurezza regolari.

Questa stratificazione normativa globale riflette il riconoscimento istituzionale del penetration testing come strumento cardine nella governance del rischio informatico, sebbene permangano significative eterogeneità interpretative nei diversi contesti giurisdizionali. La sfida emergente per le organizzazioni multinazionali risiede nell'armonizzazione di questi requisiti eterogenei in un programma di testing coerente che soddisfi simultaneamente le disposizioni normative di molteplici giurisdizioni, configurando un approccio "compliance by design" che integri i requisiti più stringenti di ciascun framework applicabile.

Un'ulteriore dimensione emergente è rappresentata dalla responsabilità legale inerente alla conduzione di penetration test. La giurisprudenza recente, in particolare la sentenza della Corte di Giustizia dell'Unione Europea nel caso C-748/23 del marzo 2024, ha stabilito importanti principi relativi alla responsabilità dei penetration tester in caso di danni collaterali non intenzionali, configurando un framework di "diligenza professionale qualificata" che stabilisce standard di cautela specifici per il settore. Parallelamente, l'evoluzione delle normative sulla notifica obbligatoria delle violazioni interagisce con la pratica del penetration testing, sollevando questioni complesse relative all'obbligo di notifica per vulnerabilità identificate ma non ancora sfruttate attivamente.

La convergenza tra requisiti di sicurezza e considerazioni di privacy aggiunge un'ulteriore dimensione di complessità, con le Autorità Garanti europee che hanno iniziato a pubblicare linee guida specifiche sulla conduzione di penetration test in conformità con i principi di minimizzazione e limitazione delle finalità del GDPR. Questo approccio "privacy by design" al penetration testing richiede l'implementazione di salvaguardie specifiche, quali la pseudonimizzazione dei dati personali utilizzati durante i test e la definizione di

politiche rigorose per la gestione post-test dei dati acquisiti.

La dialettica etica del Penetration Test

La natura intrinsecamente ambivalente del penetration testing solleva questioni etiche significative. La distinzione fondamentale tra hacking etico e attività malevole risiede nel consenso esplicito (Rules of Engagement) e nella finalità costruttiva.

Il framework etico del penetration testing si articola su principi fondamentali:

- **Principio di non-maleficenza:** Impegno a non causare danni permanenti durante i test, implementando salvaguardie per prevenire interruzioni di servizio o perdita di dati
- **Principio di confidenzialità:** Gestione rigorosa delle informazioni sensibili acquisite durante l'assessment, inclusa la crittografia dei report e la sanitizzazione dei dati personali
- **Principio di trasparenza:** Comunicazione chiara dei limiti e degli obiettivi del test, con esplicitazione delle metodologie e delle tecniche impiegate
- **Principio di proporzionalità:** Calibrazione dell'intensità dei test in base alla criticità dei sistemi, adottando un approccio graduale che minimizzi il rischio di impatti negativi

Queste considerazioni deontologiche acquisiscono particolare rilevanza in contesti critici, quali infrastrutture sanitarie o sistemi di controllo industriale, dove le conseguenze di un'interruzione potrebbero avere implicazioni significative sulla salute pubblica o sulla sicurezza.

Il dibattito contemporaneo si estende ulteriormente alla questione della disclosure responsabile delle vulnerabilità identificate. Il paradigma della “responsible disclosure”, che prevede la notifica preventiva al vendor prima della pubblicazione, si contrappone all’approccio “full disclosure”, che privilegia la trasparenza immediata. Questa tensione dialettica riflette diverse concezioni del rapporto tra sicurezza e trasparenza, con implicazioni significative per l’ecosistema della sicurezza informatica.

La crescente professionalizzazione del settore ha portato all’emergere di framework etici formalizzati, quali l’EC-Council Code of Ethics e il SANS Penetration Testing Code of Conduct, che codificano principi deontologici condivisi e stabiliscono standard di comportamento professionale. Parallelamente, programmi di bug bounty istituzionalizzati, come HackerOne e Bugcrowd, hanno creato ecosistemi strutturati per la disclosure etica, bilanciando incentivi economici e rigore metodologico.

DevSecOps e Security Testing continuo

L’evoluzione contemporanea dei paradigmi di sviluppo software ha catalizzato una trasformazione significativa nell’implementazione del penetration testing. L’emergere dell’approccio DevSecOps, che integra considerazioni di sicurezza nel ciclo di sviluppo continuo, ha determinato il superamento del modello tradizionale di testing periodico in favore di un paradigma di continuous security testing.

Questa transizione paradigmatica si manifesta nell’implementazione di pipeline di sicurezza automatizzate che incorporano scansioni di vulnerabilità, static application security testing (SAST) e dynamic application security testing (DAST) come componenti integrali del processo di integrazione continua. Strumenti come OWASP ZAP e Gauntlt consentono

l’automazione dei test di sicurezza, mentre framework come Terraform’s Sentinel e AWS CloudFormation Guard implementano policy-as-code per la validazione preventiva delle configurazioni infrastrutturali.

Il penetration testing tradizionale si trasforma così in un processo ibrido che combina automazione continua e interventi manuali specialistici, configurando un approccio stratificato in cui l’automazione garantisce copertura estensiva mentre l’analisi manuale approfondisce scenari complessi che richiedono intuizione euristica. Questa evoluzione rispecchia la transizione più ampia da un modello di sicurezza perimetrale a un paradigma di sicurezza intrinseca, in cui i controlli di sicurezza sono incorporati nell’architettura stessa piuttosto che sovrapposti a posteriori.

Purple Teaming: superamento della dicotomia offensiva-difensiva

Un’evoluzione metodologica significativa è rappresentata dall’emergere del paradigma del “purple teaming”, approccio che supera la tradizionale dicotomia tra red team (offensivo) e blue team (difensivo) per implementare un modello collaborativo integrato. In questo framework, i penetration tester lavorano in simbiosi con il team di difesa, condividendo tecniche e osservazioni in tempo reale per accelerare il ciclo di apprendimento e ottimizzare l’efficacia delle contromisure.

Questa metodologia simbiotica favorisce un trasferimento di conoscenze bidirezionale: i difensori acquisiscono una comprensione approfondita delle tecniche offensive, mentre i penetration tester sviluppano consapevolezza delle sfide operative inerenti all’implementazione delle mitigazioni. Piattaforme come MITRE ATT&CK forniscono una tassonomia condivisa che facilita questa comunicazione cross-funzionale, mappando tecniche offensive e contromisure difensive in un

framework unificato.

L’implementazione operativa del purple teaming si concretizza in sessioni strutturate di “adversary emulation”, in cui tecniche offensive specifiche vengono eseguite in ambiente controllato con piena visibilità per il team difensivo. Questo approccio consente la validazione empirica dell’efficacia dei controlli di sicurezza e l’ottimizzazione dei sistemi di rilevamento, con particolare attenzione alla riduzione dei falsi positivi e all’incremento della signal-to-noise ratio nei sistemi di monitoraggio.

AI-Driven Penetration Test

L’evoluzione contemporanea del penetration testing è caratterizzata dall’integrazione di tecnologie di intelligenza artificiale e machine learning. Questi approcci innovativi consentono l’identificazione automatizzata di pattern di vulnerabilità complessi e l’ottimizzazione delle strategie di exploitation.

Tecnologie come DeepExploit implementano algoritmi di reinforcement learning per personalizzare automaticamente gli exploit in base alle specifiche configurazioni delle target, mentre sistemi come AI.JSAC adottano approcci neuromorfici per la previsione delle superfici d’attacco emergenti. L’applicazione di tecniche di Natural Language Processing consente l’analisi semantica del codice sorgente per l’identificazione di vulnerabilità logiche complesse, trascendendo i limiti dell’analisi sintattica tradizionale.

Parallelamente, l’applicazione dell’intelligenza artificiale ha trasformato anche il panorama delle minacce, con l’emergere di malware polimorfici e tecniche di evasione avanzate. Algoritmi generativi basati su architetture transformer consentono la creazione dinamica di payload evasivi che aggirano le signature tradizionali, mentre tecniche di adversarial machine learning manipolano i sistemi di

rilevamento basati su AI.

Questa co-evoluzione delle capacità offensive e difensive configura una nuova dimensione della sicurezza informatica, in cui il penetration testing deve necessariamente incorporare competenze in data science e algorithmic adversarial thinking per rimanere efficace. L'emergere di framework come DARPA's Cyber Grand Challenge evidenzia il potenziale trasformativo dell'automazione intelligente nel dominio della sicurezza offensiva e difensiva.

Quantum-Safe Penetration Test: anticipando il paradigma Post-Quantum

L'incombente avvento del computing quantistico configura una disruption potenziale nei fondamenti crittografici che sottendono l'intero ecosistema della sicurezza digitale. In questo scenario, il penetration testing evolve per incorporare la valutazione della resistenza quantistica delle implementazioni crittografiche, configurandosi come strumento proattivo di transizione verso il paradigma post-quantum.

Metodologie emergenti includono l'assessment della "crypto-agilità" dei sistemi, ossia la loro capacità di transizione fluida verso algoritmi quantum-resistant, e l'analisi delle implementazioni di primitive crittografiche basate su reticoli, codici correttori d'errore e funzioni hash multivariabili, candidate a resistere all'attacco di computer quantistici.

Parallelamente, il quantum penetration testing esplora le implicazioni delle tecnologie quantum-based per l'offensive security, incluse le potenzialità dell'algoritmo di Shor per la fattorizzazione di chiavi RSA e la risoluzione del problema del logaritmo discreto, e dell'algoritmo di Grover per

l’accelerazione degli attacchi brute-force contro primitive simmetriche.

Questa frontiera emergente richiede l’integrazione di competenze quantistiche nel repertorio cognitivo del penetration tester contemporaneo, prefigurando un’ulteriore specializzazione disciplinare che trascende i confini tradizionali dell’informatica classica.

Il Penetration Test nell’era dell’iperconnessione: 5G e beyond

L’avvento delle reti 5G e la prospettiva delle tecnologie 6G introducono paradigmi di connettività caratterizzati da densità esponenzialmente superiori e latenze ulteriormente ridotte, abilitando scenari applicativi inediti ma introducendo simultaneamente superfici d’attacco senza precedenti. In questo contesto, il penetration testing evolve per incorporare la valutazione di architetture di rete virtualizzate, implementazioni di slicing di rete e paradigmi edge computing.

Metodologie specifiche emergono per l’assessment di tecnologie quali:

- **Network Function Virtualization (NFV):** Analisi delle vulnerabilità inerenti all’orchestrazione di funzioni di rete virtualizzate e all’isolamento tra tenant
- **Software-Defined Networking (SDN)**: Valutazione della sicurezza dei controllori SDN e delle interfacce northbound/southbound
- **Multi-access Edge Computing (MEC):** Penetration testing delle implementazioni edge, con particolare attenzione alle problematiche di trust boundary e segregazione
- **Network Slicing**: Assessment dell’isolamento effettivo tra slice e potenziale di lateral movement inter-slice

Queste tecnologie abilitanti introducono complessità architetturali che trascendono i paradigmi tradizionali, richiedendo metodologie di testing che integrino competenze in virtualizzazione, orchestrazione e programmabilità di rete.

La convergenza IT/OT e il Security Testing delle infrastrutture critiche

La progressiva digitalizzazione dei sistemi industriali ha determinato una convergenza tra Information Technology (IT) e Operational Technology (OT), configurando scenari ibridi caratterizzati da requisiti di sicurezza eterogenei e spesso contrastanti. In questo contesto, il penetration testing di infrastrutture critiche acquisisce connotazioni specifiche che riflettono la natura safety-critical di questi ambienti.

Metodologie specialistiche si sviluppano per l'assessment di tecnologie quali:

- **Industrial Control Systems (ICS):** Penetration testing di architetture SCADA, PLC e DCS, con particolare attenzione ai protocolli industriali quali Modbus, DNP3 e IEC 61850
- **Building Management Systems (BMS):** Valutazione della sicurezza dei sistemi di automazione degli edifici, inclusi controlli HVAC e sicurezza fisica
- **Smart Grid Technologies**: Assessment delle infrastrutture di rete intelligente, inclusi Advanced Metering Infrastructure (AMI) e sistemi di automazione della distribuzione

Il principio cardine in questi contesti è il "do no harm", con l'implementazione di metodologie passive e simulazioni che mitigano il rischio di interruzioni operative. Framework specialistici come ICS-CERT Assessments e CISA Industrial Control Systems Cybersecurity Assessment Tool forniscono linee

guida specifiche per il testing in ambienti critici, bilanciando l’imperativo della sicurezza con il requisito primario della continuità operativa.

La sicurezza come processo iterativo

Il penetration testing rappresenta non un evento isolato ma un processo ciclico di miglioramento continuo della postura di sicurezza. La dialettica tra difensori e attaccanti genera un’evoluzione costante delle metodologie, in un equilibrio dinamico che richiede adattamento perpetuo.

In questa prospettiva, il penetration testing trascende la dimensione puramente tecnica per configurarsi come elemento essenziale di una cultura organizzativa orientata alla sicurezza, dove la consapevolezza delle vulnerabilità costituisce il primo passo verso la resilienza digitale. La sua efficacia ultima non si misura nella mera identificazione di vulnerabilità, ma nella catalizzazione di un processo trasformativo che eleva la maturità complessiva del sistema socio-tecnico.

In un’era caratterizzata dall’espansione esponenziale della superficie d’attacco e dall’emergere di vettori offensivi sempre più sofisticati, il penetration testing si erge come prassi epistemica fondamentale, strumento euristico che illumina le zone d’ombra nella comprensione organizzativa del proprio profilo di rischio. La sua evoluzione futura sarà inevitabilmente plasmata dalla convergenza di tecnologie emergenti e dalla crescente complessità degli ecosistemi digitali, configurando una disciplina in perpetua metamorfosi al servizio della resilienza sistemica.

Bibliografia

- Alvarez, M. et al. (2022). “Advanced Penetration Testing Methodologies: A Comparative Analysis”. *Journal of Cybersecurity Research*, 34(2), 78-96.
- Bou-Harb, E., Debbabi, M., & Assi, C. (2023). “Quantum-Safe Security Assessment: Methodologies and Challenges”. *IEEE Transactions on Quantum Engineering*, 4(1), 17-32.
- Chen, L., & Moody, D. (2024). “Post-Quantum Cryptography: Current State and Future Directions”. National Institute of Standards and Technology. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
- CISA (2024). “Industrial Control Systems Cybersecurity Assessment Tool”. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/industrial-control-systems
- ENISA (2023). “Penetration Testing Procurement Guide”. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/penetration-testing-procurement-guide
- European Central Bank. (2023). “TIBER-EU Framework: How to Implement the European Framework for Threat Intelligence-based Ethical Red Teaming”. https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html
- Gonzalez, D., & Kossakowski, K. P. (2024). “Purple Teaming: Bridging Offensive and Defensive Security Through Collaborative Simulation”. *International Journal of Information Security*, 23(1), 45-62.
- Khan, S., & Parkinson, S. (2023). “AI-Driven Penetration Testing: A Comprehensive Survey”. *ACM Computing Surveys*, 55(3), 1-34.
- Mitre Corporation. (2024). “Common Vulnerabilities and Exposures (CVE)”. https://cve.mitre.org/
- Mitre Corporation. (2024). “MITRE ATT&CK Framework”.

https://attack.mitre.org/
- NIST (2023). “Technical Guide to Information Security Testing and Assessment” (SP 800-115 Rev. 1). National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-115/rev-1/draft
- OWASP Foundation. (2024). “OWASP Top Ten”. Open Web Application Security Project. https://owasp.org/www-project-top-ten/
- PCI Security Standards Council. (2024). “Payment Card Industry Data Security Standard (PCI DSS) v4.0”. https://www.pcisecuritystandards.org/document_library/
- Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). “Technical Guide to Information Security Testing and Assessment” (NIST Special Publication 800-115). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
- Taddeo, M., & Floridi, L. (2023). “The Ethics of Penetration Testing in Critical Infrastructure: A Philosophical Analysis”. *Ethics and Information Technology*, 25(2), 113-129.
- Yampolskiy, R. V. (2024). “Offensive AI: The Dark Side of Artificial Intelligence in Cybersecurity”. *IEEE Security & Privacy*, 22(1), 18-27.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/penetration-test-2/