UNIVERSITÀ DEGLI STUDI DI MILANO

CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER IL RECLUTAMENTO DI N. 1 UNITÀ DI PERSONALE AFFERENTE ALL'AREA DELLE ELEVATE PROFESSIONALITÀ - SETTORE TECNICO-INFORMATICO, CON RAPPORTO DI LAVORO SUBORDINATO A TEMPO INDETERMINATO PRESSO L'UNIVERSITÀ DEGLI STUDI DI MILANO - DIREZIONE ICT - CODICE 22611

La Commissione giudicatrice della selezione, nominata con Determina Direttoriale n. 21976 del 23/12/2025, composta da:

Prof. Andrea Lanzi	Presidente
Dott. Venuto Enrico	Componente
Dott.ssa Nicoletta Fornasari	Componente
Dott.ssa Federica Lionetti	Segretaria

comunica i quesiti relativi alla prova orale:

GRUPPO DI QUESITI N. 1

Threat hunting e utilizzo del framework MITRE ATT&CK

Descriva come strutturerebbe un'attività di threat hunting proattivo in un'infrastruttura universitaria che utilizza sistemi Windows, Linux e servizi cloud. Il candidato illustri come definire ipotesi di ricerca basate sul framework MITRE ATT&CK, quali fonti di dati utilizzare (log di sistema, autenticazioni, traffico di rete, endpoint telemetry) e come utilizzare un SIEM o una piattaforma XDR per correlare eventi e individuare comportamenti anomali non rilevati dai sistemi di detection automatici.

Analisi di un incidente con movimento laterale

In un'infrastruttura universitaria viene rilevata una possibile compromissione di una workstation Windows con sospetto movimento laterale verso altri sistemi della rete interna. Descriva le attività tecniche da svolgere per identificare l'origine dell'attacco, analizzare i log e verificare eventuali compromissioni di account o sistemi. Il candidato illustri inoltre le azioni di contenimento immediate e le modalità di utilizzo di strumenti per l'analisi dei log e il controllo delle autenticazioni.

Brano in inglese:

Kernel-level attacks or malicious programs such as rootkits that compromise the kernel of an operating system are one of the most important concerns in systems security at present. These attacks can modify kernel-level code or sensitive data to hide various malicious activities, change OS behavior or essentially take complete control of the system.

[Tratto da: Secure in-VM monitoring using hardware virtualization, Sharif, Monirul I. and Lee, Wenke and Cui, Weidong and Lanzi, Andrea; incluso in CCS '09: Proceedings of the 16th ACM conference on Computer and communications security, Pages 477 – 487, ISBN 9781605588940, 2009, https://doi.org/10.1145/1653662.165372]

GRUPPO DI QUESITI N. 2

Attacchi ad Active Directory e misure di mitigazione

Descriva alcune tecniche di attacco comuni contro infrastrutture Active Directory, come ad esempio Pass-the-Hash, Kerberoasting o privilege escalation tramite deleghe o servizi vulnerabili. Il candidato illustri come tali attacchi possano essere individuati tramite sistemi di monitoraggio e logging e quali misure tecniche e configurazioni di sicurezza possano essere adottate per ridurre il rischio.

IoT security

Descriva le principali problematiche di sicurezza legate a dispositivi mobili e IoT in ambito universitario. Descriva in particolare come avvengono gli attacchi a tali dispositivi e illustri le misure tecniche e organizzative per mitigare i rischi, includendo gestione centralizzata dei dispositivi e segmentazione di rete. Descriva anche quali strumenti possono essere utilizzati per poter individuare ed analizzare tali dispositivi.

Brano in inglese:
Many security approaches require the ability to monitor frequently executing events, such as host-based intrusion detection systems (IDSs) that intercept every system call throughout the system, LSM (Linux Security Module) [23] and SELinux that hook into a large number of kernel events to enforce specific security policies, or even instruction-level monitoring used by several offline analysis approaches [4]
[Tratto da: Secure in-VM monitoring using hardware virtualization, Sharif, Monirul I. and Lee, Wenke and Cui, Weidong and Lanzi, Andrea; incluso in CCS '09: Proceedings of the 16th ACM conference on Computer and communications security, Pages 477 – 487, ISBN 9781605588940, 2009, https://doi.org/10.1145/1653662.165372]

GRUPPO DI QUESITI N. 3
Processo avanzato di vulnerability management
Descriva come strutturerebbe un processo completo di vulnerability management in un ente universitario che gestisce numerosi sistemi e servizi IT. Il candidato illustri le modalità di identificazione delle vulnerabilità tramite strumenti di scansione, i criteri di prioritizzazione basati sul rischio e sull'impatto sugli asset critici, e il ruolo di attività come penetration testing e threat intelligence nel miglioramento continuo della sicurezza.

Gestione tecnica di un attacco ransomware
In un'infrastruttura universitaria vengono rilevati segnali di un possibile attacco ransomware su alcuni server e workstation. Descriva le attività tecniche da svolgere per rilevare e analizzare l'attacco, contenere la diffusione del malware e ripristinare i sistemi compromessi. Il candidato illustri inoltre il ruolo dei sistemi di monitoraggio, delle strategie di backup e delle attività di analisi post-incidente per prevenire attacchi simili in futuro.

Brano in inglese:
In this paper, we present Secure In-VM Monitoring (SIM), a general-purpose framework based on hardware virtualization features that enables security monitors residing in the same VM it is protecting to have the same level of security as residing in a separate trusted or secured VM. A security monitor in our framework retains the efficiency close to being inside the same VM by not requiring any privilege transfers when switching to the monitor for an intercepted event, and being able to access the system address space at native speed.
[Tratto da: Secure in-VM monitoring using hardware virtualization, Sharif, Monirul I. and Lee, Wenke and Cui, Weidong and Lanzi, Andrea; incluso in CCS '09: Proceedings of the 16th ACM conference on Computer and communications security, Pages 477 – 487, ISBN 9781605588940, 2009, https://doi.org/10.1145/1653662.165372]

Milano, 13 marzo 2026

La Commissione

Prof. Andrea Lanzi Presidente

Dott. Venuto Enrico Componente

Dott.ssa Nicoletta Fornasari Componente

Dott.ssa Federica Lionetti Segretaria