Prot. n. 0205788 del 20/10/2025 - [UOR: 2-UPROR - Classif. VII/1]

UNIVERSITÀ DI SIENA 1240

1

1) Spiegare la differenza tra Firma Elettronica Semplice (FES), Avanzata (FEA) e Qualificata (FEQ) secondo eIDAS, con un esempio pratico per ciascuna.

2) "Descrivere architettura e implementazione di un sistema di monitoraggio della rete di ateneo, con lo scopo di:

A) controllare movimenti laterali malevoli, all'interno di una LAN

B) controllare l'accesso alla wireless di ateneo per escludere estranei"

3)Monitoraggio del server web di ateneo allo scopo di dimensionarlo correttamente

Within either the cyber kill chain or MITRE ATT&CK frameworks, Lateral Movement (LM) allows adversaries to progressively move deeper into a system in seek of high-value assets. Although this timely subject has been studied in the cybersecurity literature to a significant degree, so far, no work provides a comprehensive survey regarding the identification of LM from mainly an intrusion detection system (IDS) viewpoint. To cover this noticeable gap, this work provides a systematic, holistic overview of the topic, paying also special attention to Internet of Things (IoT) ecosystems. The survey part, spanning a time window of eight years and 53 articles, is split into three domains, namely, Endpoint Detection and Response (EDR) schemes, machine learning oriented solutions, and graph-based strategies. On top of that, we reveal interrelations, mapping the progress in this field over time, and offer key observations that may propel LM research forward.

UNIVERSITÀ
DI SIENA
1240

1) Con l'aggiornamento "eIDAS 2.0", è stato introdotto l'European Digital Identity Wallet (EUDI Wallet). Quali sono le principali novità e le finalità di questo strumento?

2) Descrivere architettura e implementazione di un sistema di monitoraggio della rete di ateneo, con lo scopo di:

A) controllare la sicurezza degli apparati di rete

B) svolgere un vulnerability assessment "

3) Descrivere come implementare il monitoraggio dello stato software e hardware di PC (Windows o MAC o Linux o misti) di un'aula informatica

Based on an initial point of compromise, typically through dropping malware or exploiting a vulnerability in a device or application, Lateral Movement (LM) involves moving deeper in terms of data or upwards in regard to access. Oftentimes, the attacker's goal is to remain in the system as an Advanced Persistent Threat (APT), attempting to gain as much loot 5 as possible. What is more, in the Internet of Things (IoT) era, LM is gaining increased attention; attackers can exploit a plethora of IoT devices for achieving LM. That is, IoT devices represent a particularly alluring target for a variety of threat actors aiming to move laterally and create persistence within any network, especially enterprise ones. Namely, IoT seem ideal not only for obtaining initial foothold and persistent remote access, but also for gaining new permissions and user privileges in the breached environment.

UNIVERSITÀ
DI SIENA
1240

1) Il CAD ha istituito diverse piattaforme abilitanti. Sceglierne una tra pagoPA e app IO e descriverne il suo funzionamento, i suoi obiettivi e i benefici che porta a cittadini e PA.

2) Descrivere le problematiche relative allo sviluppo di software sicuro, utilizzo di librerie di terze parti, anche opensource, individuazione delle vulnerabilità.

3) Descrivere le principali problematiche di sicurezza associate ai sistemi VoIP elencando le prindipali misure tecniche per mitigarle.

The current section briefly reviews the key pertinent literature on the subject of endpoint and log-based detection of LM events. The concentration is on the methodology of each relevant work regarding event-driven identification of the most impactful LM techniques. Particularly, we focus on the collection of system and network related logs to the specified examined attacks, the utilized rule-based policy, and the impact upon the successful incidence response. To facilitate the parsing of the relevant literature, Table 2 recaps the relevant key characteristics per work included in this section. The various studies are chronologically arranged in ascending order.

UNIVERSITÀ DI SIENA 1240

1) Descrivere il ruolo e le principali responsabilità del Responsabile per la Transizione al Digitale (RTD) all'interno di una Pubblica Amministrazione.

2) Dopo averne dato una definizione sintetica, descrivere la differenza principale tra Software as a Service (SaaS) e Platform as a Service (PaaS) in termini di responsabilità di gestione per l'utente e il provider.

3) Illustrare il concetto di Quality of Service (QoS) per il traffico VoIP e descrivi almeno due tecniche per implementarlo in una rete aziendale.

Marquez et al. [32] presented a modern detection scheme for pivoting attacks, namely APIVADS. The latter analyzes APT pivoting tactics based on the flow of traffic in Small Office Home Office (SOHO) and corporate facilities, where IoT interconnected devices find great applicability. The presented identification scheme aims to overcome the literature gaps that were permitting adversaries to infiltrate the targeted traffic, breach and gain access through parallel obfuscation 335 of their pivoting traces. To succeed that, the authors focused on the flow-based statistical analysis of the generated traffic during pivoting incidents, in an effort to identify anomaly indicators produced by malicious events.

UNIVERSITÀ DI SIENA 1240

1) Qual è la differenza sostanziale tra "dato anonimo" e "dato pseudonimizzato" secondo il GDPR e perché questa distinzione è cruciale?

2) Quali fattori economici (es. Capex vs Opex) entrano in gioco nella decisione di adottare una soluzione SaaS o PaaS rispetto a un'infrastruttura on-premise?

3) Indicare i criteri per la scelta dei log e i criteri di retention nell'ipotesi di implementazione di un sistema di log centralizzato.

The current section provides a condensed summary of the key pertinent literature on the subject of LM-specific ML 390 IDS concepts. The concentration is on the methodology of each relevant work regarding the implementation of ML models, either via supervised (SML) or unsupervised (UML) data manipulation techniques. Particularly, we focus on the identification of the core ML algorithm's function in terms of shallow and DNN applicability, the implementation of feature selection processes, and the leverage of publicly available benchmark datasets, if any, towards the evaluation of the effectiveness of each proposed IDS. To facilitate the parsing of the relevant literature, Table 4 recaps the relevant 395 key characteristics of every work included in this section.

UNIVERSITÀ DI SIENA 1240

1) Spiegare il principio di accountability (responsabilizzazione) introdotto dal GDPR. Quali sono almeno tre adempimenti pratici che un Titolare del trattamento deve mettere in atto per dimostrarla?

2) Descrivere le minacce AI, phishing/social engineering, awareness e approcci per affrontarle

3) Quali sono i criteri principali per stabilire se una violazione dei dati personali (data breach) debba essere notificata all'Autorità Garante? E quando non è necessario farlo?

The work of Kaiafas et al. [40] is considered cutting-edge compared to their related counterparts dedicated to the 400 field of log-based identification and anomaly detection. Precisely, the authors focused on the creation of an adaptable and efficient anomaly IDS methodology that leverages the combination of 10 generic log-based features and other eight custom-made, respectively. Both these set of features were extracted from the popular, publicly available Los Alamos National Laboratory (LANL) log-based corpus that was gathered between 1996 and 2005 [41]. The collected subsets were manipulated via various sampling techniques towards the facilitation of pre-processing and computational power 405 issues with such voluminous data volumes.

UNIVERSITÀ DI SIENA 1240

7

1) Il Piano per l'Informatica nella pubblica amministrazione 2024-2026 pone un forte accento sulla "sovranità tecnologica". Cosa si intende con questo concetto e quali azioni concrete il Piano promuove per raggiungerla?

2 Descrivere i tipi di attacchi DoS e DDoS e le tecniche per la loro prevenzione e mitigazione.

3) Descrivere il concetto di Failover e Resilienza in un'infrastruttura di virtualizzazione desktop, citando e descrivendo qualche strategia per garantirli.

In the era of Internet of Everything (IoV), LM has evolved as a game-changing tactic in the quiver of cybercriminals, especially when it comes to APT. In this volatile ecosystem, the present article offers the first to our knowledge fullfledged, systematic review of literature works about schemes designed to timely identify and possibly counteract LM in the network perimeter or deeper in the network, mainly in the form of an IDS. We differentiate among three kinds 820 of such defensive solutions, namely, those that hinge on either graph algorithmic schemes, ML classification models, or EDR log-based policy strategies. Interestingly, for each category of solutions, an additional distinction is made between schemes proposed for general network domains, especially enterprise intranets, and IoT or IIoT ones. Just as important, an extensive and thorough array of essential observations and discussions is given, highlighting the utilized methodologies and datasets, as well as certain deficiencies and challenges