Report Security Operation: azioni preventive W18D1

In questo esercizio dovremo avviare una scansione di Nmap da Kali verso Windows 7 prima con il firewall spento e poi acceso ed annotare le differenze riscontrate.

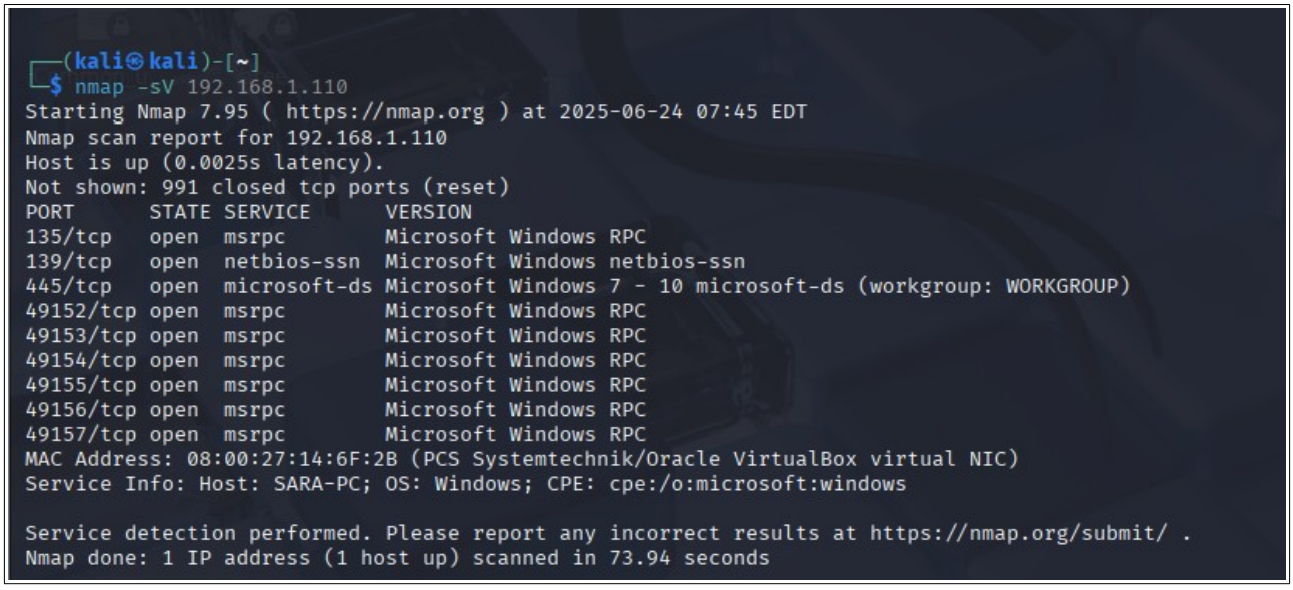
Firewall disattivato

Le porte aperte trovate con i relativi servizi sono:

- Microsoft Windows RPC: 135, 49152, 49153, 49154, 49155, 49156, 49157;
- Microsoft Windows netbios-ssn: 139;
- Microsoft Windows 7-10 microsoft-ds: 445

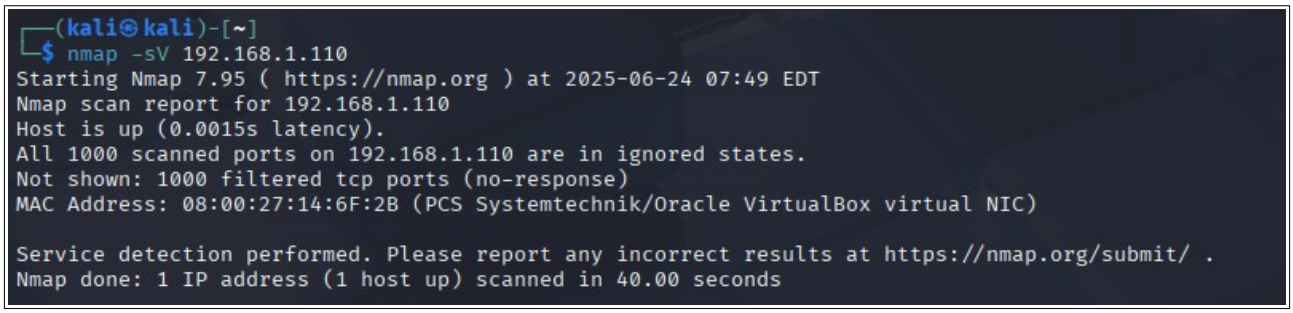
Service info:

- Hostname: SARA-PC;
- OS: Windows;
- CPE: cpe:/o:microsoft:windows



Firewall attivato

Con il Firewall attivato, l’unica informazione che potremo ricavare dalla scansione è che l’host legato all’IP risulta raggiungibile.

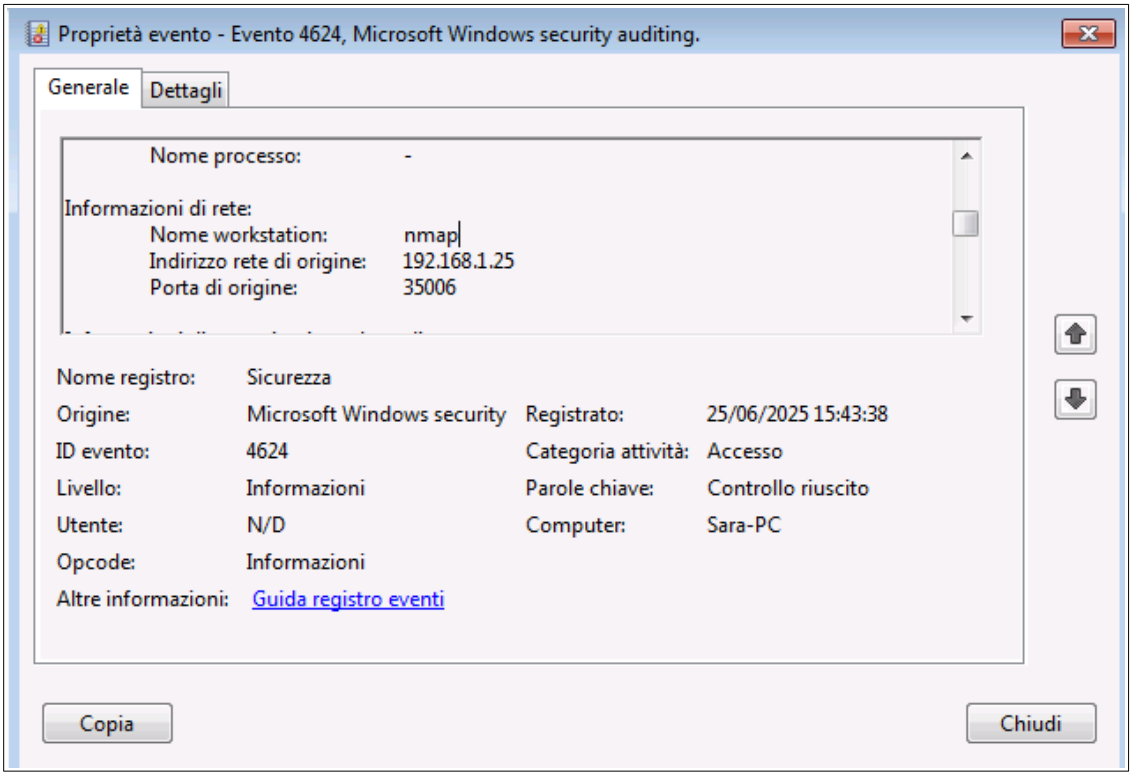


Facoltativo

Controllare i log di sistema durante le operazioni effettuate in precendenza.

Firewall disattivato

Controllando i log a firewall spento potremo trovare un log con codice 4624 che riporta un login riuscito da parte dell'IP 192.168.1.25 (Kali), il nome della workstation (nmap) e la porta di origine (35006).



Firewall attivo

Come visto in precedenza, visto che il firewall blocca la scansione, nei log non apparirà nulla a riguardo.

Pratica extra

Business continuity

Definizione: La business continuity (BC) rappresenta l'abilità di un'azienda di proseguire le proprie attività anche quando si verificano problemi o imprevisti.
L'azienda pianificherà in anticipo le misure da adottare in questi casi, così da ridurre le conseguenze dell'interruzione e garantire una rapida ripartenza.

Disaster Recovery

Definizione: Il Disaster Recovery è una branca della Business Continuity che si occupa in particolare del ripristino di dati, applicazioni e infrastrutture tecnologiche dopo un guasto o una perdita significativa.
Si concentra su aspetti come le copie di sicurezza, le procedure di recupero e la velocità con cui i sistemi informatici possono tornare disponibili.

Tabella comparativa:

Categorie	Business Continuity	Disaster Recovery
Scopo	Garantire la continuità operativa di tutti i processi essenziali dell'organizzazione	Ripristinare infrastrutture IT e dati dopo un disastro
Ambito	Strategico e organizzativo (persone, processi, tecnologie)	Tecnico e operativo (sistemi informatici e dati)
Tempistica	Prevede risposte immediate e piani a lungo termine	Azioni mirate al ripristino rapido post-evento
Focus principale	Minimizzare impatto complessivo su clienti e operazioni	Minimizzare tempi di inattività IT e perdita di dati
Norme di riferimento	ISO 22301	Buone pratiche ITIL, ISO/IEC 27031
Esempi di misure	Sedi alternative, piani di emergenza, backup manuali	Backup dati, sistemi ridondanti, recovery site

ICT readiness for business continuity

Definizione: La norma ISO/IEC 27031 offre linee guida per preparare le tecnologie ICT a sostenere la continuità operativa, aiutando le organizzazioni a prevenire, affrontare e superare interruzioni informatiche che mettono a rischio le attività essenziali.