Cyber Security Report

W18D1

06/11/2025

Autore :
Pace Massimiliano
email : *efmpas@gmail.com*

Indice :

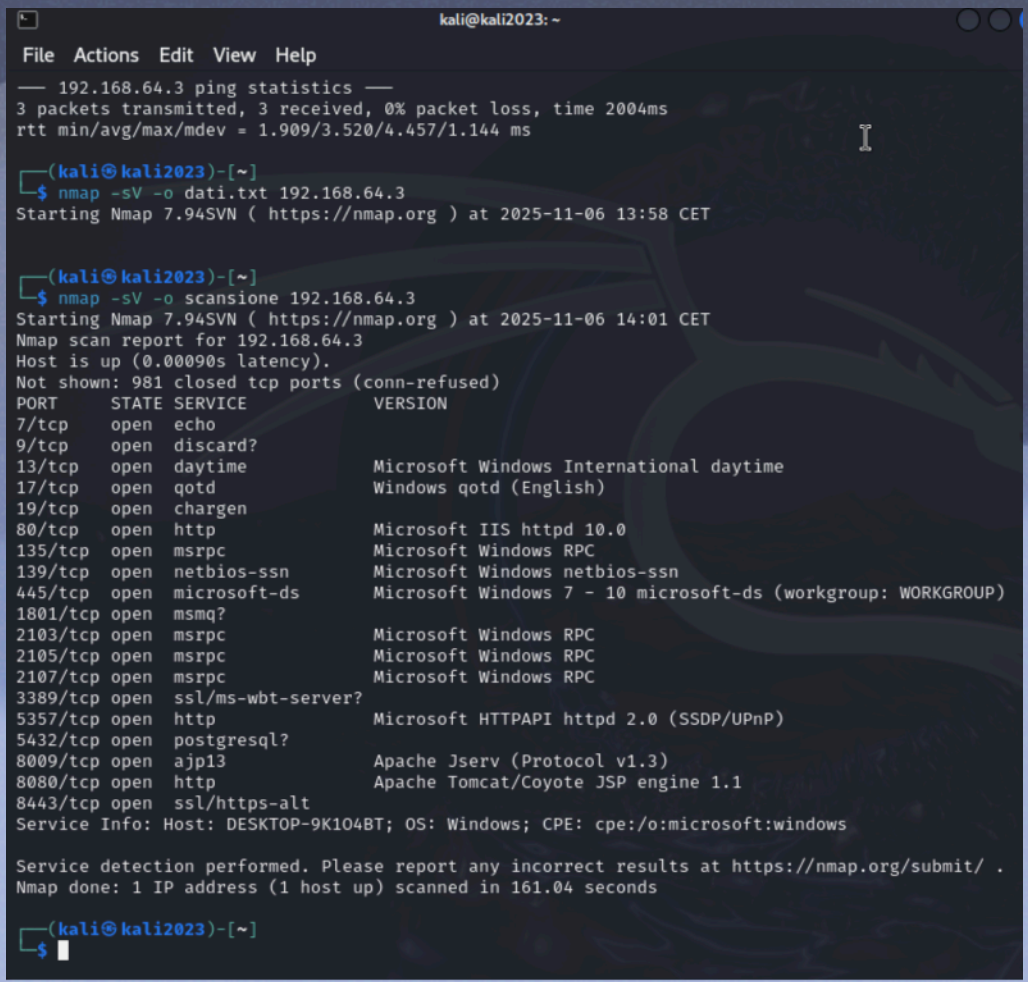
INTRODUZIONE ESERCIZIO FIREWALL

° L'esercizio odierna punta al dimostrare come cambiano i sistemi di sicurezza delle nostre macchine con l'attivazione della protezione Firewall. Andremo a dimostrare che eseguendo una scansione delle porte troveremo dati diversi con protezione disattivata e attivata

SPIEGAZIONE ESERCIZIO

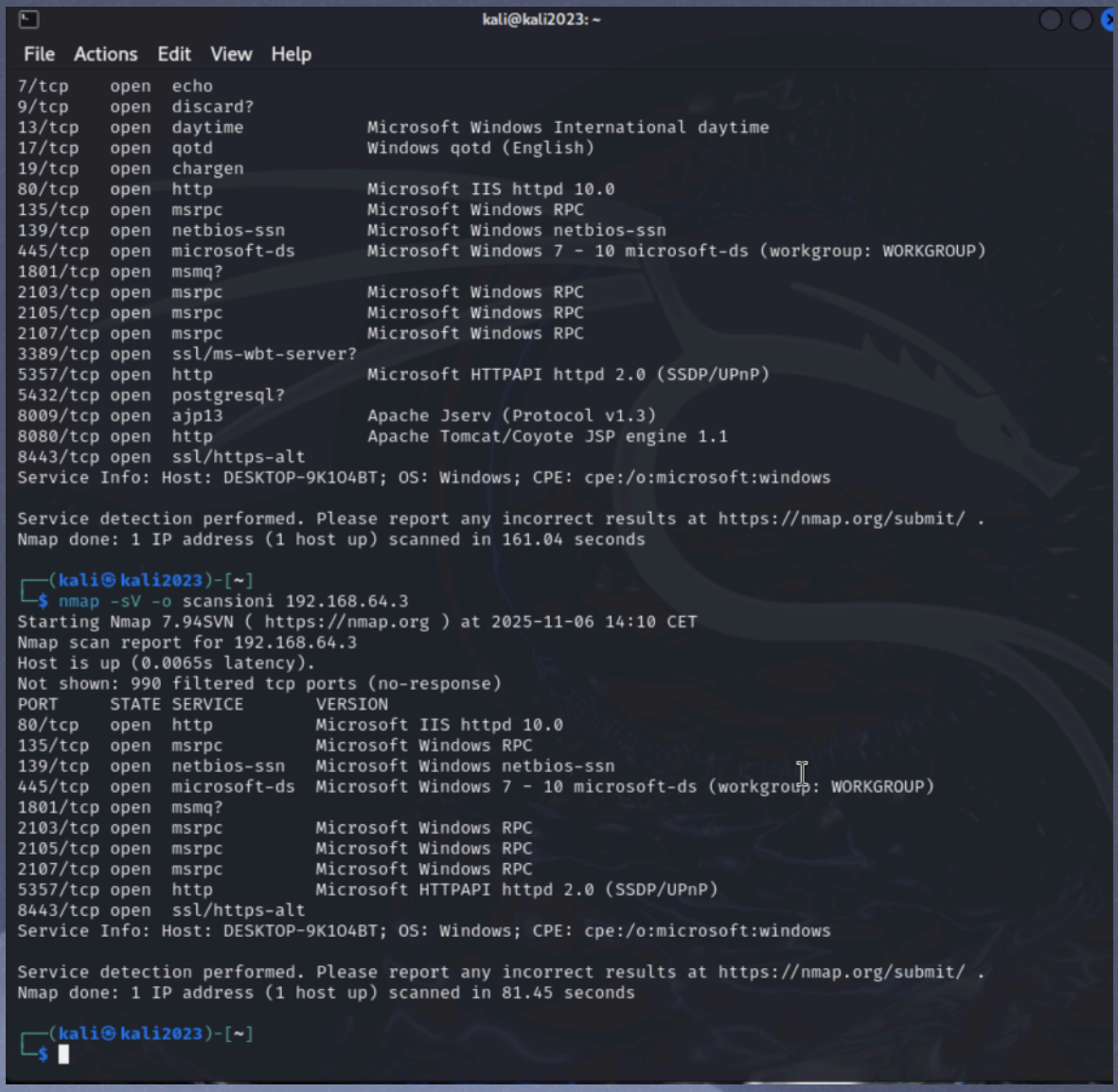
° Avviamo sia Kali che Windows eseguiamo un ping di controllo e analizziamo la macchina target con nmap -sV per la service detection e -o per creare un file da visionare in seguito con i risultati ottenuti

Firewall spento



° Ora attiviamo il Firewall e andiamo a visionare le differenze chiaramente visibili

Firewall attivo



° Ora con il firewall attivo risultano meno porte aperte e le porte risultano filtrate. Le porte risultano filtrate quando non vi e' risposta alla scansione.

CONCLUSIONI

Attivando i firewall nel nostro target , si verra’ a creare una protezione maggiore. Alcune porte risultano bloccate dall’esterno ed essendo le altre filtrate avremo una macchina piu’ sicura agli attacchi. Le impostazioni Firewall sono numerose si possono creare regole come abbiamo fatto in precedenza ed in altri esercizi e si possono chiudere anche tutte le porte rimanenti creando un target a prova di LUCA e MILENA.

Esercizio Facoltativo

Business Continuity

riguarda tutte le strategie i processi e le soluzioni che permette a un'azienda di mantenere i servizi essenziali attivi durante e dopo un'emergenza limitando al minimo le interruzione operative e proteggendo la reputazione le finanze e i clienti.

Disaster recovery

si concentrate sulle procedure tecniche e operative per ripristinare sistemi IT dati e applicazioni dopo che si e' verificato un disastro. L'obbiettivo e' tornare il più rapidamente possibile allo stato normale delle operazioni IT.

TABELLA COMPARATIVA

Titolo	Obiettivo	Attivazione	Azioni	Tempistiche
Continuità Operativa	Garantire la continuità delle opendali durante interruzioni	Eventi che minacciano l'operatività (es. (guasti tecnici)	Fino a 72	Sviuppo di un piano di continuiittà, test regolari
Attivazione	Tunte le funzioni aziendali essenziali	(es. pandemie, [illegible], [illegible]	Fino a 72 ore	Esempi
Ambito	Tunte le funzioni aziendali essenziali	Pianificazione preventiva, trasferimerento delle attività, gestione della comunicazione	trasferipazióne	Sviuppo di un piano di continuità, test regolari
Titolo				
Recupero Disastri	Ripristinare le operazioni dopo un disastro	Eventi catastrofici (es. incendi, terremoti)	Ore/giorni	Sistemi informativi e infrastrutture chiave
Azioni	Sistemi infomativi e infrastrutture chiave	Ripristino dei dati, ripristino delle applicazioni, verifica della funzionalità	Ore/giorni	Backup dei dati, replica dei server, test di ripristino

Concetto di ICT readiness for business continuity secondo IRBC (ISO/IEC 27031)

ICT Readiness for Business Continuity (IRBC): Secondo la ISO/IEC 27031, ICT readiness significa preparare in modo strutturato sistemi informatici e di comunicazione per supportare e garantire la continuità operativa rispetto a ogni tipo di evento disruptive.
Il framework include:
Analisi delle dipendenze critiche nei sistemi, inclusi server, reti, applicazioni.
Definizione di obiettivi come il Recovery Time Objective (RTO – tempo massimo accettabile di inattività) e Recovery Point Objective (RPO – perdita massima di dati tollerabile).
Implementazione di resilienza (ridondanza, backup, test periodici dell'efficacia dei piani).
Integrazione con la gestione della sicurezza delle informazioni e dei processi di business continuity.
La norma ISO/IEC 27031 offre alle organizzazioni una guida fondamentale per assicurare che le infrastrutture ICT siano in grado di sostenere l'operatività anche in condizioni di emergenza e siano in grado di riprendersi secondo i tempi prefissati.