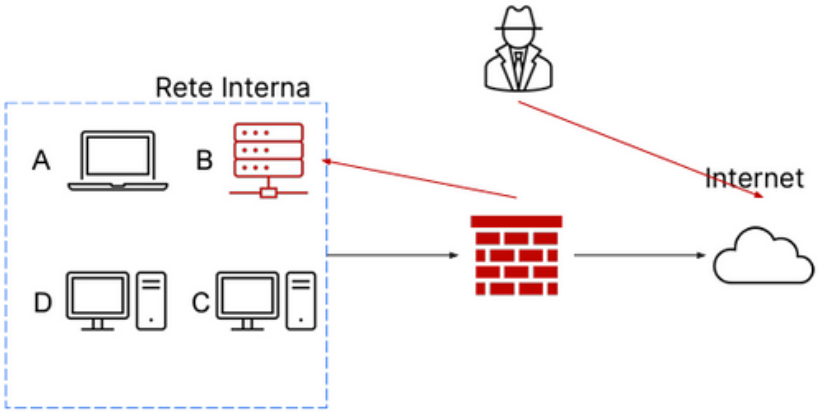
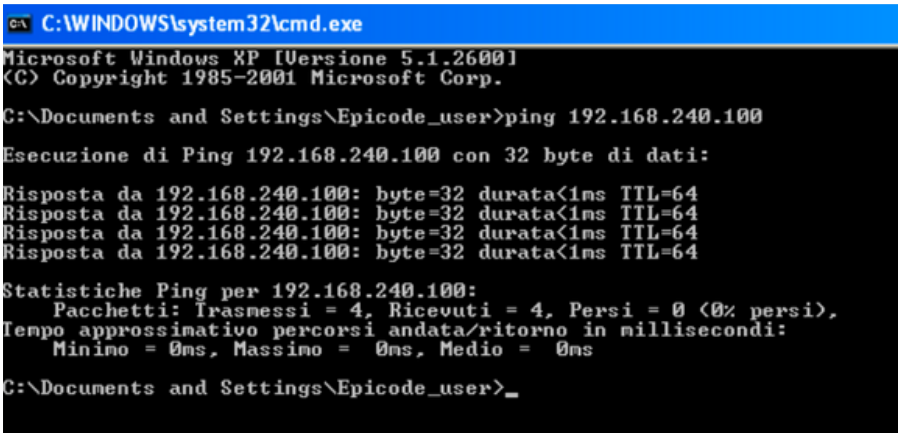
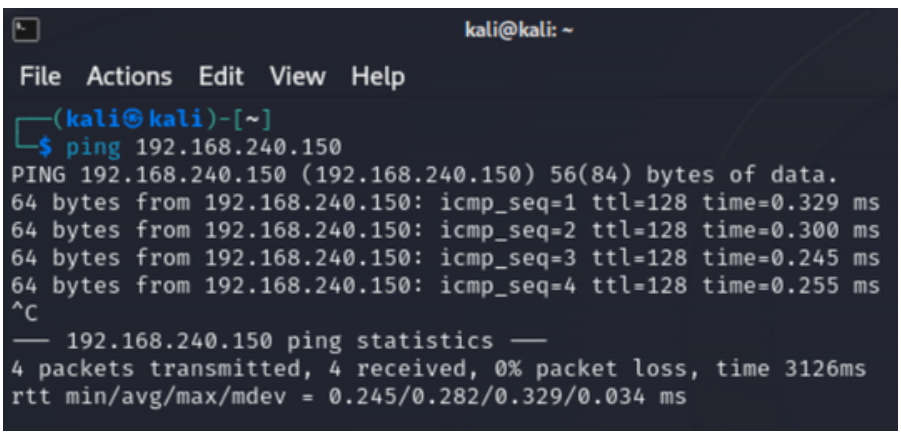
Security Operation: azioni preventive

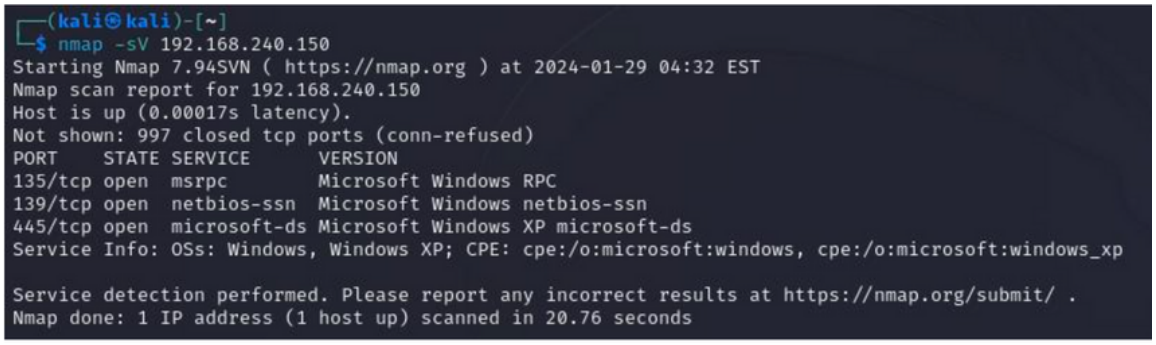
Traccia:
Con riferimento alla seguente figura, il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet. L'attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai seguenti quesiti. Mostrate le tecniche di: I) Isolamento II) Rimozione del sistema B infetto Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi



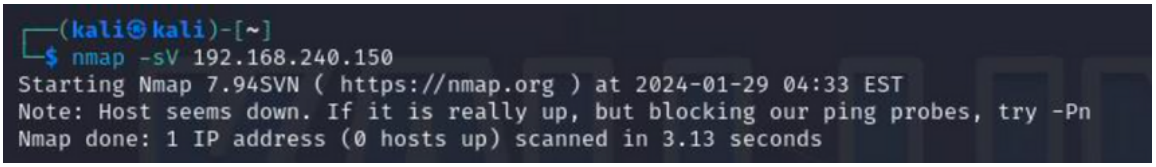




Con il comando ***nmap -sV 192.168.240.150*** scansiono le porte aperte sulla macchina target e tento di identificare la versione dei servizi in esecuzione (firewall disattivato)



Riprovo dopo aver attivato il firewall



Le analisi dettagliate effettuate tramite l'utilizzo di Nmap, un noto software di scansione di rete, forniscono una chiara dimostrazione dell'impatto significativo che i firewall hanno sulla sicurezza dei sistemi operativi, in questo caso specifico, Windows XP. Quando i firewall sono attivati, si osserva che ogni tentativo di ping verso il sistema viene efficacemente bloccato. Questo fenomeno evidenzia l'efficacia dei firewall come strumento cruciale per la difesa del sistema, agendo da barriera contro gli attacchi esterni e impedendo l'individuazione remota delle attività del sistema.
Al contrario, disattivando i firewall, la situazione cambia drasticamente. Senza questa barriera protettiva, Nmap riesce a eseguire una scansione approfondita delle porte, permettendo così di rilevare quelle aperte e di identificare potenziali vulnerabilità all'interno del sistema. Queste vulnerabilità possono essere sfruttate da attaccanti per infiltrarsi nel sistema, causando potenziali danni o compromettendo dati sensibili.
Queste osservazioni sottolineano l'importanza vitale di mantenere sempre attivi i firewall e di adottare un approccio olistico alla sicurezza informatica, che includa l'implementazione di varie misure di sicurezza come software antivirus, aggiornamenti regolari del sistema e pratiche di navigazione sicura. Inoltre, è essenziale per gli amministratori di sistema e per gli utenti finali essere consapevoli delle configurazioni di sicurezza dei loro dispositivi e di comprendere il ruolo fondamentale che le misure preventive giocano nel proteggere i sistemi informatici da attacchi esterni e intrusioni indesiderate. In sintesi, la protezione offerta dai firewall, unita ad altre pratiche di sicurezza, costituisce una difesa essenziale contro le minacce informatiche, salvaguardando l'integrità e la privacy dei dati nei sistemi operativi moderni.