

Cyber Security Report



W20D1

19/11/2025

Autore :

Pace Massimiliano

email : *efmpas@gmail.com*

Indice :

° Introduzione e descrizione pag. 2 - 3

° conclusioni pag. 4

Report Incident Response – W20D1

1. Contesto e Scenario

Il sistema B, che gestisce un database con diversi dischi per lo storage, è stato compromesso da un attaccante che è riuscito a bucare la rete e accedere al servizio tramite Internet. L'attacco è ancora in corso e il team CSIRT deve intervenire rapidamente.

2. Tecniche di Isolamento e Rimozione del sistema B infetto

Isolamento

- Scollegare il sistema B dalla rete interna e da Internet.
- Bloccare tutte le connessioni attive, sia locali che remote.
- Disabilitare le interfacce di rete del sistema coinvolto.
- Attivare i controlli di accesso fisici per impedire ulteriore manipolazione o sabotaggio.

Rimozione

- Spegner e disconnettere fisicamente il server compromesso.
- Spostare i dischi interessati in un ambiente isolato per successive analisi forensi.
- Seguire le policy interne sull'evidenza digitale prima di manipolare hardware/software compromessi.

3. Differenza tra Purge, Destroy e Clear

Metodo	Descrizione	Sicurezza
Purge	Sovrascrittura sicura dei dati, rendendoli irrecuperabili tramite software wipe.	Alta
Destroy	Distruzione fisica del supporto: degaussing, incenerimento, triturazione, ecc.	Massima
Clear	Cancellazione semplice (delete/format): i dati possono essere recuperati.	Bassa

- Si raccomanda sempre di utilizzare Purge per i dati sensibili e Destroy per informazioni particolarmente riservate, seguendo conformità ISO/GDPR.
- Clear è sconsigliato per supporti con dati confidenziali

Diagramma: Attacco alla Rete Interna

- La figura mostra la struttura della rete aziendale, evidenziando che il sistema B (database/storage) è situato nella rete interna insieme ad altri host.
- L'attaccante ha sfruttato una vulnerabilità, bypassando il firewall e accedendo direttamente a B tramite Internet.
- L'obiettivo immediato del team CSIRT è contenere l'attacco, isolare B e avviare la risposta all'incidente secondo quanto sopra

Conclusioni

Nelle fasi finali dell'ultimo esercizio, il team CSIRT ha adottato un approccio sistematico per gestire la compromissione del sistema B, limitando al massimo l'impatto dell'attacco. L'isolamento e la rimozione del database infetto sono stati cruciali per prevenire l'ulteriore propagazione della minaccia nella rete aziendale.

La distinzione fra "purge", "destroy" e "clear" ha permesso di scegliere il metodo di cancellazione più adatto in base al livello di riservatezza dei dati e alle normative di sicurezza. Infine, la documentazione di tutte le procedure e la corretta gestione dei supporti compromessi garantiscono la conformità e la protezione degli interessi aziendali anche durante la post-incident analysis.

Conclusione

Il tipo di attacco che risulta più evidente dagli screenshot è un TCP SYN Scan, tipicamente usato per mappare porte e servizi attivi su uno o più host della LAN. Questo comportamento è compatibile con una fase di reconnaissance precedente ad un exploitation.

Se il traffico fosse ancora più massiccio e da molteplici sorgenti, potrebbe leggersi come tentativo di DoS/DDoS, ma da questi screenshots il pattern è quello del port scanning.

Se hai usato tool come Nmap, Masscan o simili su questa rete, questo tipo di cattura è il risultato normale del loro utilizzo. Se invece non hai avviato alcun tool di scanning, potresti essere di fronte a una ricognizione non autorizzata sulla tua LAN.