W19D4

Traccia:
Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto. Trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco

1. **Identificare eventuali IOC, ovvero evidenze di attacchi in corso:**
   Richieste TCP ripetute

2. **In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati:**
   è in corso una scansione sul target 192.168.200.150 dall'attaccante 192.168.200.100

3. **Consigliate un'azione per ridurre gli impatti dell'attacco:**
   Per ridurre i rischi di attacchi provenienti dall'indirizzo IP 192.168.50.100, un'azienda può adottare diverse misure di sicurezza senza entrare nel dettaglio tecnico dei comandi. Innanzitutto, si può configurare il firewall aziendale in modo da bloccare completamente il traffico da e verso quell'IP, impedendo all'attaccante di comunicare con la rete interna. Inoltre, è importante eseguire una verifica delle porte aperte, limitando l'accesso solo a quelle essenziali per l'operatività aziendale. Se possibile, l'azienda dovrebbe implementare sistemi che richiedano un'autenticazione aggiuntiva, come una VPN o l'uso di autenticazione a due fattori, soprattutto per l'accesso remoto.

Un altro passo utile è tenere costantemente aggiornati i software e i sistemi operativi aziendali, così da ridurre le vulnerabilità sfruttabili dagli attaccanti. La segmentazione della rete, separando le risorse critiche in zone isolate, può limitare i danni in caso di compromissione di una parte della rete. Per una maggiore sicurezza, si può anche implementare un sistema di monitoraggio in grado di rilevare comportamenti anomali e segnalare tempestivamente attività sospette, bloccando automaticamente eventuali attacchi in corso.

Infine, educare il personale sull'importanza della sicurezza informatica è fondamentale per evitare che errori umani facilitino un attacco. Sensibilizzare i dipendenti su pratiche sicure, come il riconoscimento di email di phishing o la gestione corretta delle password, può contribuire a proteggere l'intera azienda.