Bonus: Analisi degli attacchi rilevati nel file shadow.zip

Dettagli delle rilevazioni

Dal file `shadow.zip` sono stati identificati i seguenti attacchi, tutti provenienti dall'IP 10.0.0.1 e diretti verso vari host nella rete interna.

Host colpiti:

- Da `192.168.1.10` a `192.168.1.22`, tutti gli host tra i due IP compresi

Sono stati tentati diversi tipi di attacchi:

1. **Cross-Site Scripting (XSS):**
   Rilevati tentativi di iniezione di script dannosi tramite input utente, URL sospetti e l'uso di funzioni JavaScript pericolose.
2. **Denial of Service (DoS):**
   Identificati attacchi che hanno causato un sovraccarico del sistema tramite richieste multiple, traffico eccessivo e pacchetti SYN, con l'obiettivo di interrompere o rallentare il servizio.
3. **Password Attack:**
   Segnalati attacchi di forza bruta tramite ripetute tentativi di login e tentativi di accesso da località sospette.
4. **Phishing:**
   Identificate email contenenti link malevoli e tentativi di spoofing, con l'intento di ingannare gli utenti e compromettere le credenziali.
5. **Ping of Death:**
   Un pacchetto ICMP anomalo è stato rilevato, con il potenziale di causare disservizi sul sistema target.

Conclusioni

Questi attacchi evidenziano una serie di tentativi di compromettere la sicurezza della rete, variando dalle vulnerabilità applicative (XSS) e i problemi di accesso (attacchi di password) a minacce più aggressive come il **Ping of Death** e i **DoS**.

Il traffico **Phishing** indica una possibile campagna mirata a rubare credenziali e informazioni sensibili.

Si consiglia di adottare le seguenti misure:

- Rafforzare i filtri di sicurezza per prevenire l'esecuzione di script dannosi e bloccare pacchetti ICMP non autorizzati.
- Implementare tecniche di rilevamento avanzato per identificare attività di forza bruta e phishing.
- Monitorare costantemente il traffico di rete per rilevare attività sospette e mitigare i rischi derivanti da attacchi di **Denial of Service**.