Day 19 - Attack Diagram

CREAZIONE DI UN DIAGRAMMA CHE DEFINISCA IL PIANO D'ATTACCO VERSO UN SERVER WINDOWS.

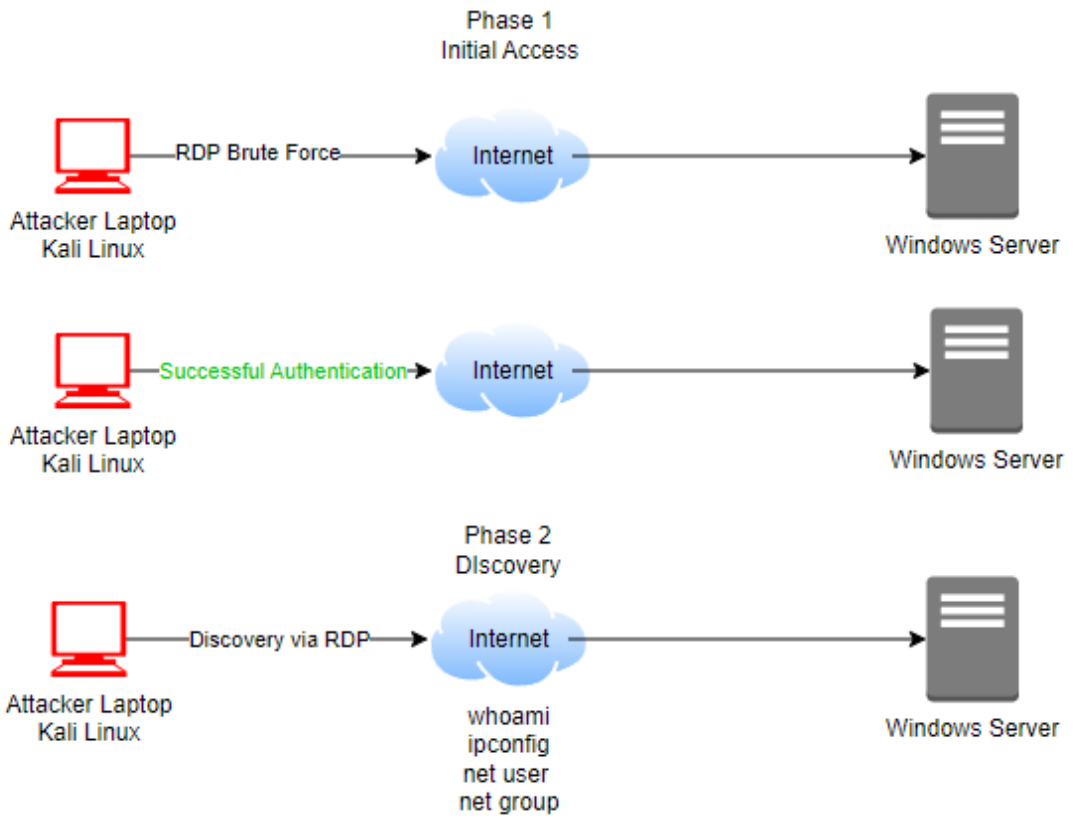
Attack Diagram

Premesse:
•C2 (Command and Control) è ospitato su un cloud provider.
•Kali Linux è installato e operativo sul nostro host locale.

Fasi del diagramma di attacco:

1.Brute Force Attack verso Windows:
Lanciare un attacco Brute Force contro un sistema Windows target per tentare di ottenere credenziali valide.

2.Discovery:
Utilizzo di comandi di scoperta per mappare la rete e ottenere informazioni sul sistema Windows target.



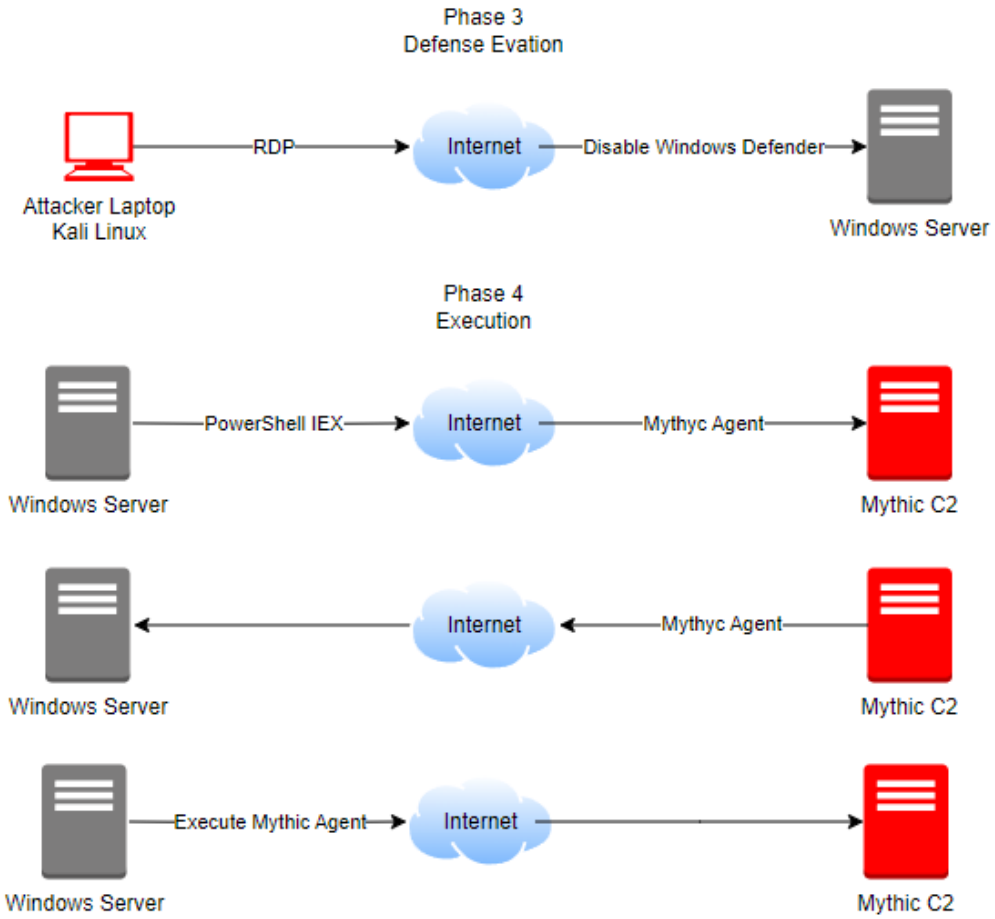
Attack Diagram

3.Defense Evasion:

Disabilitare Windows Defender per evitare che l'attacco venga rilevato.

4.Esecuzione:

Utilizzare un'espressione PowerShell per scaricare l'agente *Mythic* dal server C2 e avviarlo sul sistema compromesso.



Attack Diagram

5.Command and Control (C2):

Stabilire una sessione di controllo remoto con il server C2 per mantenere il controllo sul sistema target.

6.Exfiltration:

Sfruttare la sessione creata per scaricare un file falso contenente password dal sistema Windows compromesso verso il server C2.