Relazione Attacco Brute Force

(Ethical Hacking)

Questa relazione dimostra un attacco brute force per accedere a un account su una macchina virtuale Windows Server 2019 utilizzando una macchina virtuale Kali Linux.

L'obiettivo è illustrare la vulnerabilità di password deboli e l'importanza di implementare robuste misure di sicurezza. Verranno descritti i prerequisiti, i passaggi per condurre l'attacco e le contromisure efficaci per difendersi da tali minacce.

by Noemi Baruffolo

Prerequisiti per l'Attacco

1 **Macchina Virtuale Kali Linux**

Necessaria con il software Hydra preinstallato e accesso alla rete.

2 **Macchina Virtuale Windows Server 2019**

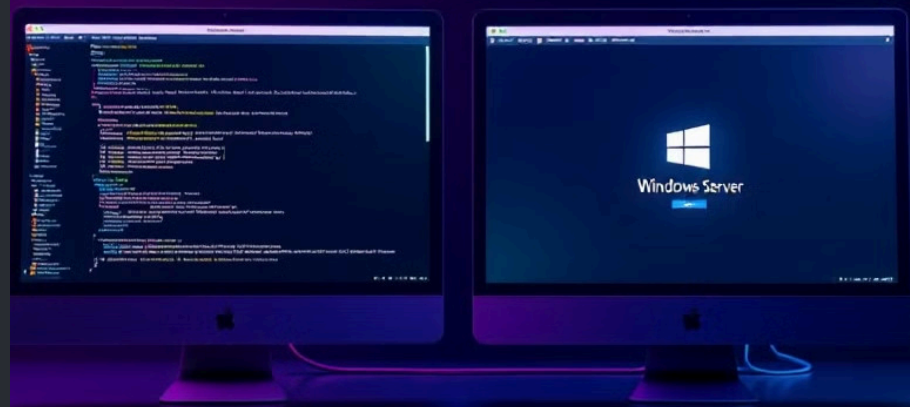
Configurata con servizio RDP abilitato e un utente con password semplice.

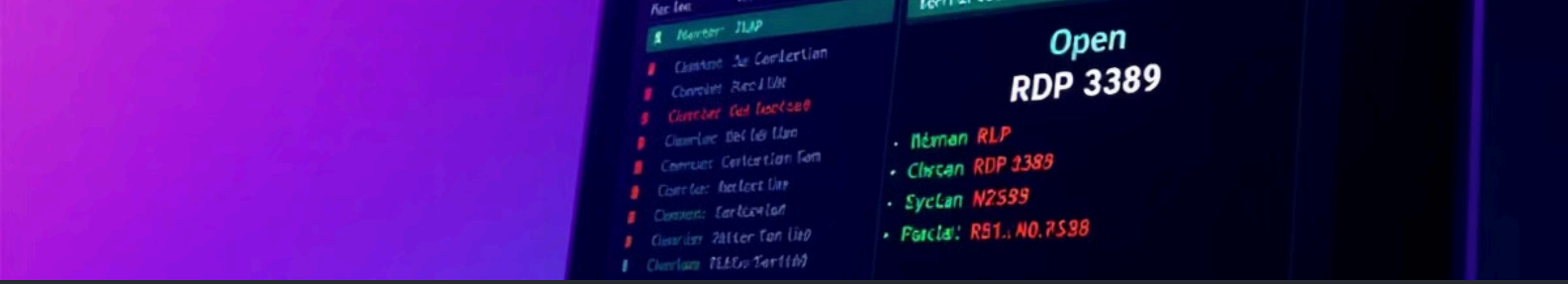
3 **Connessione di Rete Condivisa**

Entrambe le macchine devono essere sulla stessa rete o subnet.

4 **File di Dizionario**

Utilizzo di un file di password come /usr/share/wordlists/rockyou.txt incluso in Kali.





Verifica del Servizio RDP

1

Scansione con Nmap

Utilizzare Nmap per verificare che la porta RDP (3389) sia aperta sul Windows Server.

2

Esecuzione del Comando

Eseguire il comando: nmap -p 3389 <IP_target>

3

Analisi del Risultato

Confermare che la porta 3389 risulti aperta e pronta per l'attacco.

Lancio dell'Attacco Brute Force con Hydra

1

Preparazione del Comando

Strutturare il comando Hydra con le informazioni necessarie.

2

Esecuzione dell'Attacco

Lanciare il comando: hydra -l Administrator -P /usr/share/wordlists/rockyou.txt rdp://<IP_target>

3

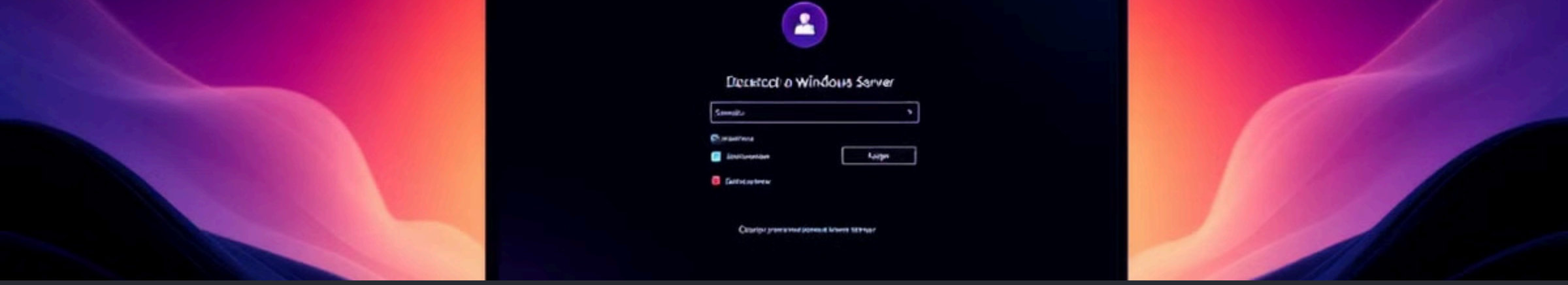
Monitoraggio del Progresso

Osservare l'output di Hydra mentre tenta diverse combinazioni di password.

4

Identificazione della Password

Attendere che Hydra trovi la password corretta, se presente nel dizionario.



Accesso al Sistema Windows Server 2019

1

Installazione di xfreerdp

Se non già presente, installare xfreerdp su Kali Linux con il comando: sudo apt install freerdp2-x11

2

Preparazione del Comando di Connessione

Strutturare il comando xfreerdp con le credenziali ottenute dall'attacco brute force.

3

Esecuzione della Connessione RDP

Lanciare il comando: xfreerdp /u:Administrator /p:password123 /v:192.168.1.100

4

Verifica dell'Accesso

Confermare l'accesso riuscito al sistema Windows Server 2019.

Contromisure: Utilizzo di Password Complesse

Lunghezza Minima

Implementare password di almeno 12 caratteri per aumentare la complessità.

Varietà di Caratteri

Includere lettere maiuscole, minuscole, numeri e simboli nella password.

Evitare Parole Comuni

Non utilizzare password presenti nei dizionari comuni per ridurre la vulnerabilità agli attacchi.

Rotazione Periodica

Cambiare regolarmente le password per mantenere un elevato livello di sicurezza.

Contromisure: Limitazione dei Tentativi di Login

1

Accesso ai Criteri di Sicurezza

Navigare su Criteri di sicurezza locali → Criteri account → Criteri di blocco account.

2

Configurazione Soglia di Blocco

Impostare la Soglia di blocco account a 3 tentativi falliti.

3

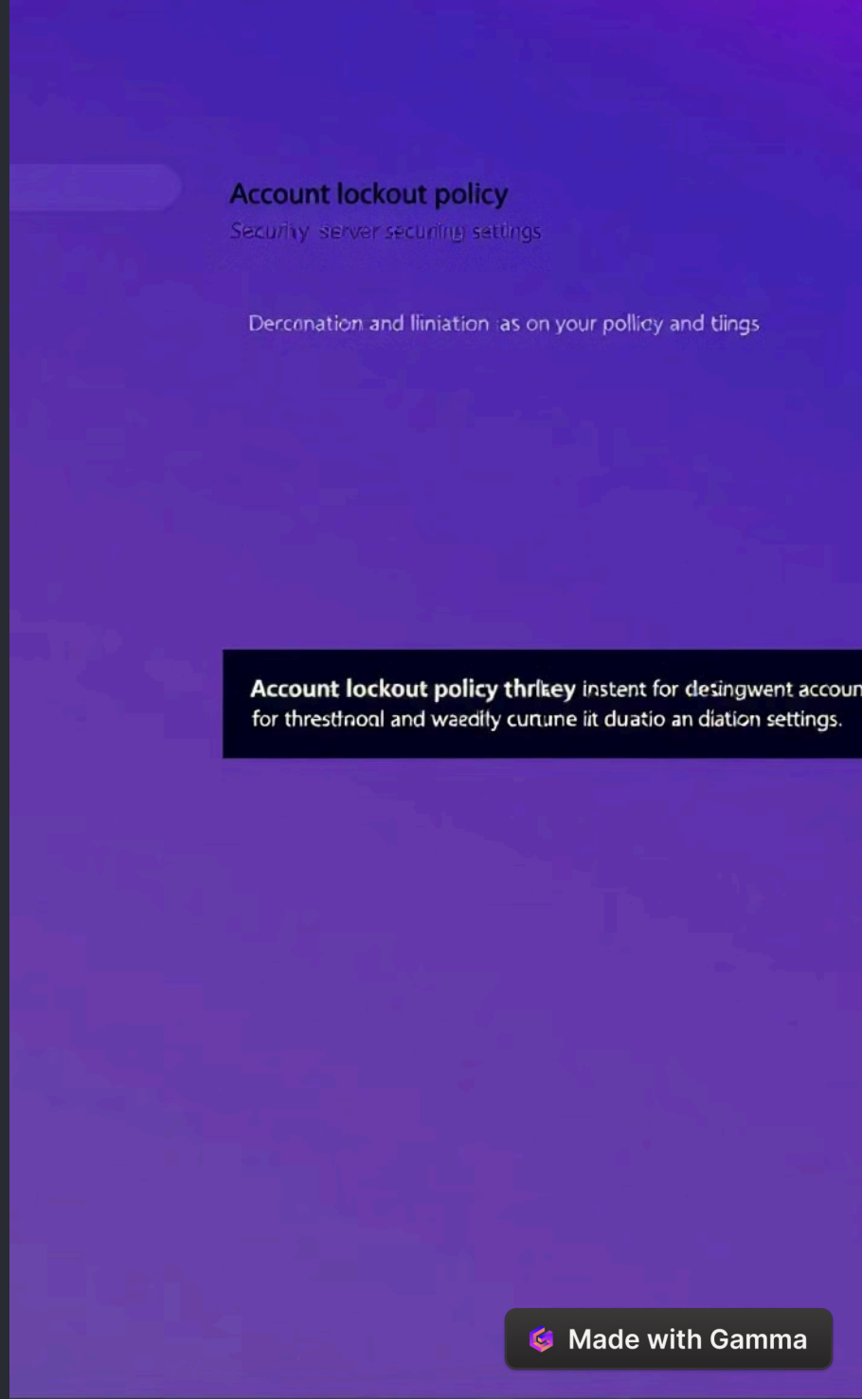
Impostazione Durata Blocco

Configurare la Durata blocco account a 15 minuti.

4

Applicazione delle Modifiche

Salvare le impostazioni e applicare i nuovi criteri di sicurezza.



Contromisure: Modifica della Porta RDP Predefinita

Accesso al Registro di Sistema

Aprire l'Editor del Registro di Sistema di Windows e navigare fino alla chiave HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp.

Modifica del Valore PortNumber

Individuare il valore PortNumber e modificarlo con un nuovo numero di porta (es. 3390). Assicurarsi che la nuova porta non sia già in uso da altri servizi.

Riavvio del Servizio RDP

Dopo aver modificato il numero di porta, riavviare il servizio RDP per applicare le modifiche. Questo renderà il servizio RDP meno individuabile per potenziali attaccanti.

Contromisure: Monitoraggio dei Log di Accesso

1

Apertura del Visualizzatore Eventi

Accedere al Visualizzatore eventi di Windows Server.

2

Navigazione ai Log di Sicurezza

Selezionare Registri di Windows → Sicurezza.

3

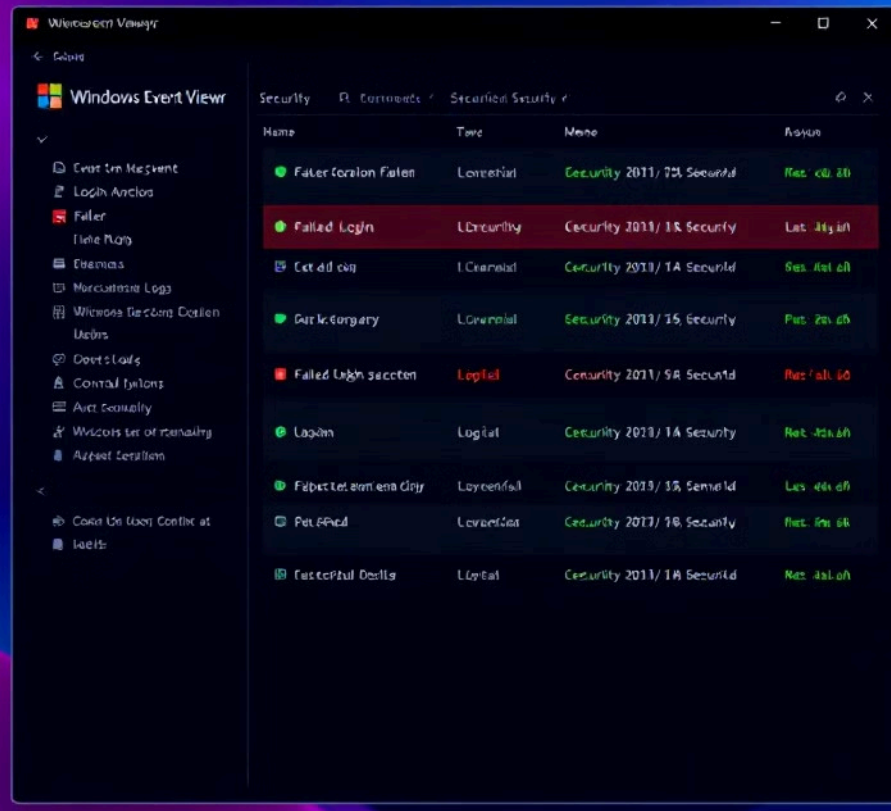
Ricerca Eventi Specifici

Cercare eventi con ID 4625 (tentativo di accesso fallito) e 4624 (accesso riuscito).

4

Analisi dei Tentativi di Accesso

Esaminare i log per identificare pattern sospetti o tentativi di attacco brute force.



Conclusione e Raccomandazioni Finali

Implementazione di Misure di Sicurezza

Applicare tutte le contromisure discusse per proteggere efficacemente il sistema da attacchi brute force.

Formazione sulla Sicurezza

Educare gli utenti sull'importanza di password robuste e pratiche di sicurezza.

Aggiornamenti Regolari

Mantenere il sistema e il software sempre aggiornati per prevenire vulnerabilità note.

Monitoraggio Continuo

Implementare un sistema di monitoraggio costante per rilevare e rispondere rapidamente a potenziali minacce.