Consegna w14d1

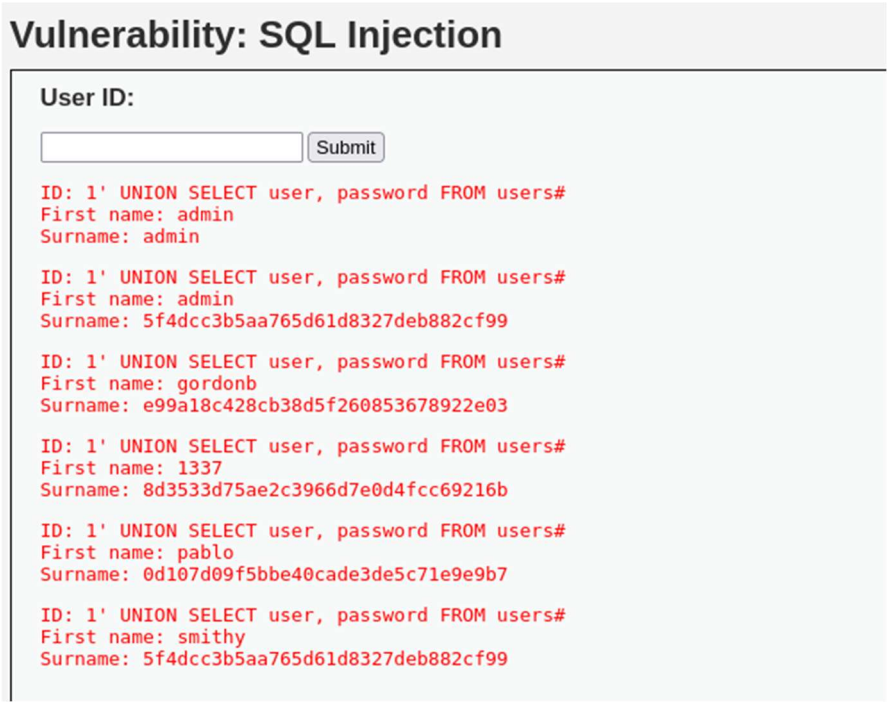
Traccia: password cracking Esercizio Traccia Abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema. Se guardiamo meglio le password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5. Recuperate le password dal DB come visto e provate ad eseguire delle sessioni di cracking sulla password con John the Ripper per recuperare la loro versione in chiaro. L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate precedentemente.

1.Estrazione degli hash tramite SQL Injection

Iniziamo con lo spiegare che cos'è una SQL Injection. La SQL Injection è una tecnica che sfrutta una vulnerabilità nei campi input di un'applicazione web per eseguire comandi SQL non autorizzati. In questo caso, abbiamo usato un payload per forzare il database a restituire username e password.

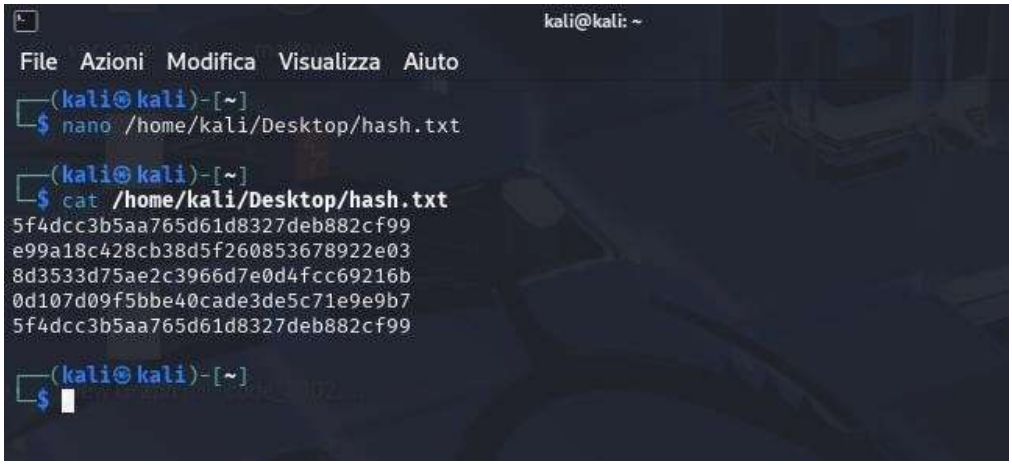
In "User ID" abbiamo inserito: "**1' UNION SELECT user, password FROM users#**" Il comando è così composto:
- 1': Chiude la stringa aperta nel campo input. Serve per "uscire" dalla query originale.
- UNION SELECT user, password FROM users: Combina i risultati della query originale con una nuova query che seleziona i campi user e password dalla tabella users.
- #: È un commento in SQL. Tutto ciò che segue viene ignorato, evitando errori nella query originale.

Visto che il campo "User ID" è vulnerabile, non filtra correttamente l'input. Questo permette di inserire codice SQL e ottenere dati privati.



2.Creazione del file hash.txt

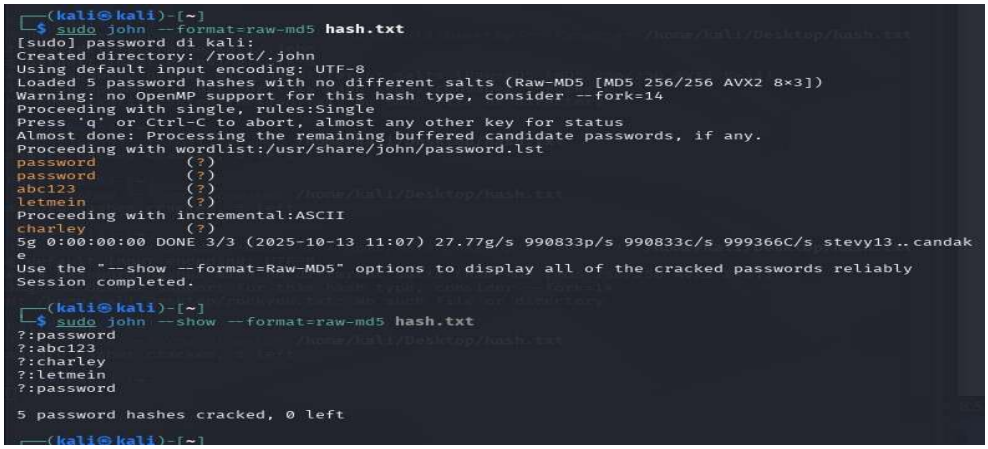
Iniziamo con il creare il file, entriamo nel terminale e con il comando "**nano /home/kali/Desktop/hash.txt**". Il passo seguente è quello di inserire con il comando "**cat**" tutti gli hash MD5 raccolti in precedenza.



3. Cracking con John the Ripper e visualizzazione delle password craccate

Iniziamo con lo spiegare John the Ripper (JtR) è uno strumento open-source usato per craccare password. Confronta gli hash con un dizionario di parole comuni per trovare la corrispondenza.

Nel terminale: "**sudo john --format=raw-md5 hash.txt"** Questo comando avvia John the Ripper per craccare gli hash MD5 contenuti nel file, usando un dizionario predefinito (se non specificato) e privilegi di amministratore con sudo.



Dopo il cracking: "**sudo john --show --format=raw-md5 hash.txt**". Questo comando serve per visualizzare le password craccate da John the Ripper, dopo che il processo di cracking è stato completato. Non esegue il cracking, ma mostra i risultati già ottenuti.

Tabella riepilogativa

Username	Hash MD5	Password trovata
admin	5f4dcc3b5aa765d61d8327deb882cf99	password
gordonb	e99a18c428cb38d5f260853678922e03	abc123
1337	8d3533d75ae2c3966d7e0d4fcc69216b	charley
pablo	0d107d09f5bbe40cade3de5c71e9e9b7	letmein
smithy	5f4dcc3b5aa765d61d8327deb882cf99	password

Facoltativo

Traccia: Hai scoperto che un computer Windows in azienda è stato infettato dal ransomware **WannaCry**. Questo malware cifra i file e chiede un riscatto in Bitcoin per sbloccarli. L'obiettivo è:

- Intervenire subito sul sistema infetto
- Proporre soluzioni di messa in sicurezza
- Valutare pro e contro di ogni soluzione

1. Azioni urgenti da eseguire

Isolare il dispositivo: Disconnetti il computer dalla rete per evitare la diffusione

Spegnere il sistema: Se il ransomware è attivo, spegnere può evitare ulteriori danni

Informare il team IT: Coinvolgere subito chi gestisce la sicurezza

Non pagare il riscatto: Pagare non garantisce il recupero dei file e incoraggia gli attacchi

2. Possibili soluzioni di messa in sicurezza

1.Ripristino da backup

Descrizione: Ripristinare il sistema da un backup precedente all'infezione.

Pro	Contro
Recupero veloce dei dati	Richiede backup aggiornati e funzionanti
Evita il pagamento del riscatto	Se il backup è vecchio, si perdono dati recenti

2. Formattazione e reinstallazione

Descrizione: Cancellare tutto e reinstallare Windows.

Pro	Contro
Rimozione totale del malware	Perdita completa dei dati se non salvati
Sistema pulito e sicuro	Tempo necessario per reinstallare e configurare tutto

3. Analisi forense

Descrizione: Analizzare il sistema per capire come è avvenuta l'infezione.

Pro	Contro
Aiuta a prevenire futuri attacchi	Richiede competenze tecniche e tempo
Può identificare vulnerabilità	Non sempre permette il recupero dei file

4. Uso di tool di decrittazione

Descrizione: Utilizzare strumenti gratuiti per decifrare i file (se disponibili).

Pro	Contro
Possibile recupero senza pagare	Funziona solo con versioni note del ransomware
Gratuito	Non garantito, può fallire

3.Conclusioni

Nella seconda parte dell'esercitazione ho cercato di spiegare come il ransomware WannaCry è pericoloso e si diffonde rapidamente. Ho cercato di spiegare e di dimostrare come sia indispensabile un intervento tempestivo e che la soluzione migliore e più sicura sia il formattare il dispositivo infettato ripristinando il backup. Di conseguenza è di fondamentale importanza creare sempre backup recenti e aggiornati in modo che in seguito ad un eventuale attacco si possa fare un ripristino quanto più recente è possibile evitando di perdere molti dati e/o ore di lavoro per ritornare al punto di partenza oltre eventualmente ad uno storico.

È importante rafforzare la sicurezza:

- Aggiornare Windows e software
- Usare antivirus e firewall
- Formare il personale contro phishing e allegati sospetti