Password Cracking
&
Malware

Sommario

Traccia principale

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 per recuperare la loro versione in chiaro.

Sentitevi liberi di utilizzare qualsiasi dei tool visto.

L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate precedentemente.

Consegna

1. Screenshot dell'SQL injection già effettuata
2. Due righe di spiegazione di cos'è questo cracking (quale tipologia / quale meccanismo sfrutta)
3. Screenshot dell'esecuzione del cracking e del risultato

Traccia facoltativa

Hai appena scoperto che l'azienda che segui come consulente di sicurezza ha un computer con Windows 7 è stato infettato dal malware WannaCry. Cosa fai per mettere in sicurezza il tuo sistema?

Consegna

- Per prima cosa occorre intervenire tempestivamente sul sistema infetto
- In seguito, preparare un elenco delle varie possibilità di messa in sicurezza del sistema
- Per ogni possibilità valutare i pro e i contro

Premesse

Preparazione del laboratorio virtuale

Per l'installazione e configurazione della DVWA si rimanda al report M2\W8\D2_&_D3
Per avviare i servizi da Kali Linux

1. sudo service mysqld start
2. sudo service apache2 start
3. systemctl start mariadb.service
4. accedere tramite browser http://127.0.0.1/dvwa/login.php

In alternativa, avviare la macchina Metasploitable2, quindi accedere attraverso il link, in questo caso dato dall'indirizzo IP http://192.168.1.105/dvwa/login.php

Definizione di Hash

Un hash è il risultato di una funzione crittografica che prende in input una stringa di lunghezza variabile (come una password) e restituisce una stringa di lunghezza fissa. Questo processo viene utilizzato per trasformare dati in una rappresentazione "unidirezionale", il che significa che non è possibile (o almeno dovrebbe essere molto difficile) risalire all'input originale a partire dall'hash generato.

Gli hash vengono spesso utilizzati per memorizzare password in maniera sicura nei database: invece di salvare la password in chiaro, viene memorizzato l'hash. Quando un utente inserisce la sua password, questa viene nuovamente hashata e confrontata con l'hash salvato nel database. Se i due valori corrispondono, l'utente viene autenticato.

Cos'è MD5?

MD5 (Message Digest Algorithm 5) è un algoritmo di hashing molto popolare che produce un hash a 128 bit (32 caratteri esadecimali). È stato sviluppato negli anni '90 ed è stato a lungo utilizzato per garantire l'integrità dei dati e per memorizzare password in modo sicuro.

Un esempio di hash MD5 potrebbe essere il seguente:

- Input: password123
- Hash MD5: 482c811da5d5b4bc6d497ffa98491e38

Perché MD5 non è sicuro?

Negli anni, MD5 è stato soggetto a numerose vulnerabilità, in particolare:

1. Collisioni: È possibile trovare due input diversi che generano lo stesso hash. Questo compromette la sicurezza dell'algoritmo.
2. Velocità di calcolo: MD5 è molto veloce da calcolare. Inizialmente questo era un vantaggio, ma oggi significa che è possibile eseguire attacchi brute-force o dictionary molto rapidamente.
3. Attacchi pre-calcolati: Esistono enormi database online chiamati rainbow tables che contengono milioni di hash MD5 pre-calcolati per password comuni. Questo permette di decifrare una password hashata con MD5 semplicemente confrontandola con questi database.

Windows 10 e 11 e MD5

Sistemi operativi moderni come Windows 10 e Windows 11 hanno abbandonato l'uso di MD5 per la memorizzazione delle password, preferendo algoritmi più robusti come SHA-256 o soluzioni crittografiche avanzate come bcrypt, scrypt o PBKDF2. Questi algoritmi sono progettati per essere più lenti da calcolare, il che rende molto più difficile eseguire attacchi brute-force o utilizzare rainbow tables per decifrare gli hash.

Svolgimento della traccia principale

Creazione del file con i dati

Per l'individuazione delle credenziali trovati si rimanda al report M4W13D5 **Exploit DVWA - XSS e SQL injection**

```
ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Creare un file di testo, preferibilmente sul desktop, che si potrebbe chiamare hash.txt con **nano**

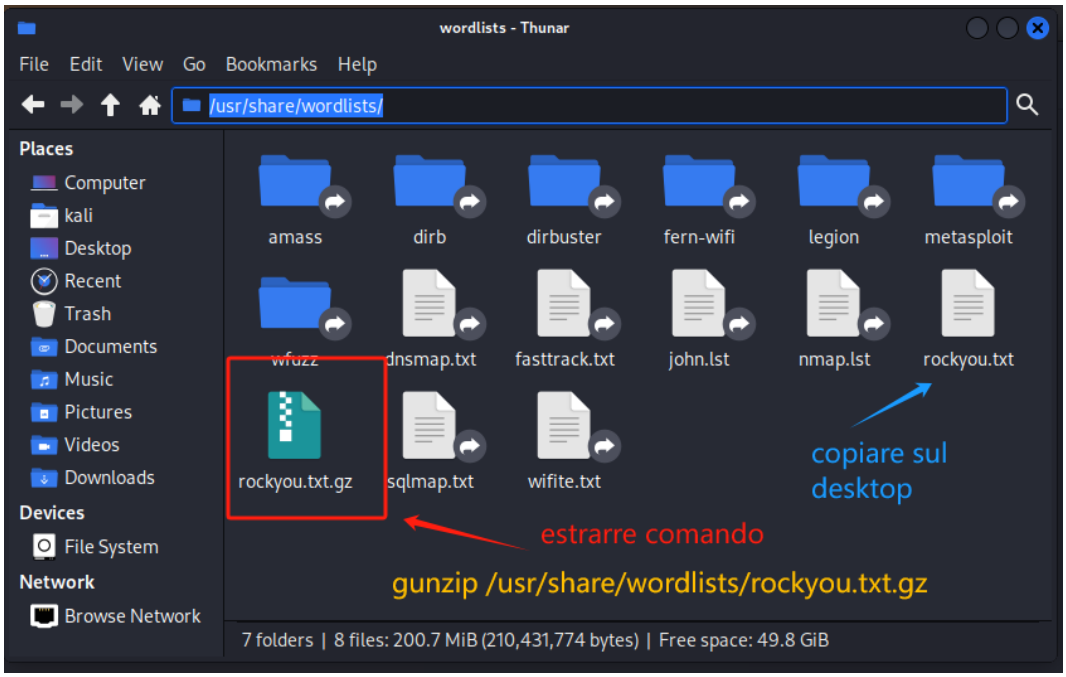
```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nano hash.txt
[sudo] password for kali:

┌──(kali㉿kali)-[~/Desktop]
└─$ cat hash.txt
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```

```
File  Actions  Edit  View  Help
 GNU nano 8.1
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```

Preparare la wordlist rockyou.txt



John the Ripper

John the Ripper (spesso abbreviato in John) è un software open-source progettato per il cracking delle password. Supporta una vasta gamma di algoritmi di hashing, tra cui MD5, SHA-1, bcrypt, e molti altri. John può utilizzare varie tecniche per decifrare gli hash, come attacchi brute-force o dictionary attacks, ed è uno strumento molto popolare in ambito pentesting (test di penetrazione).

john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt /home/kali/Desktop/hash.txt

1. **john**: Questo esegue il programma John the Ripper. Se John è installato correttamente, questo comando richiama lo strumento.
2. **--format=raw-md5**: Specifica il formato dell'hash che John deve decifrare. In questo caso, il formato è MD5 raw, che significa che gli hash nel file non contengono alcun tipo di salatura o prefisso (sono hash MD5 puri).
3. **--wordlist=/home/kali/Desktop/rockyou.txt**: Questo specifica il file wordlist che John utilizzerà per il dictionary attack. In un dictionary attack, John confronterà gli hash con le possibili password presenti nel file wordlist. Il file /home/kali/Desktop/rockyou.txt è una delle wordlist più popolari, contenente milioni di password comunemente utilizzate. Se la tua wordlist contiene la password originale, John sarà in grado di craccare l'hash.
4. **/home/kali/Desktop/hash.txt**: Questo è il file che hai creato e contiene gli hash MD5 che vuoi decifrare. John userà gli hash in questo file per cercare di trovare le password corrispondenti utilizzando la wordlist specificata.

```
┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt /home/kali/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
abc123           (?)
letmein          (?)
charley          (?)
4g 0:00:00:00 DONE (2024-10-08 20:35) 40.00g/s 28800p/s 28800c/s 38400C/s my3kids..soccer9
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Conclusione

In questo esercizio, è stato utilizzato un **dictionary attack** per il cracking delle password. Il meccanismo sfrutta una lista di password comuni (wordlist), come rockyou.txt, confrontando ciascuna password con l'hash MD5 fornito. Se la password nella wordlist genera lo stesso hash, John the Ripper la identifica come la password in chiaro corrispondente.

Svolgimento Esercizio Facoltativo

Cos'è WannaCry

WannaCry è un ransomware che ha colpito computer in tutto il mondo nel maggio 2017. È stato uno dei più gravi attacchi informatici della storia recente, causando danni significativi a numerose organizzazioni e sistemi.

1. **Funzionamento di WannaCry**
    - **Crittografia dei File:** WannaCry crittografa i file degli utenti, rendendoli inaccessibili. Dopo la crittografia, il ransomware visualizza un messaggio che richiede un riscatto in Bitcoin per ottenere la chiave di decrittazione.
    - **Vulnerabilità Sfruttata:** Sfrutta una vulnerabilità nel protocollo SMB (Server Message Block) di Windows, nota come EternalBlue, che consente al malware di propagarsi rapidamente tra i computer sulla stessa rete.
    - **Meccanismo di Diffusione:** WannaCry si diffonde automaticamente attraverso reti locali e Internet, infettando computer vulnerabili senza la necessità di interazione da parte dell'utente.
2. **Dettagli Tecnici**
    - **Tipo di Malware:** È classificato come ransomware, una categoria di malware progettata per bloccare l'accesso ai dati dell'utente fino al pagamento di un riscatto.
    - **Estensioni dei File:** I file crittografati da WannaCry sono generalmente rinominati con estensioni come .WNCRY.
    - **Richiesta di Riscatto:** Il ransomware richiede un pagamento in Bitcoin, con istruzioni su come effettuare il pagamento. Spesso include una scadenza, aumentando la pressione sull'utente per pagare.

3. Livello di Criticità

- Impatto Globale: WannaCry ha colpito oltre 200.000 computer in più di 150 paesi, causando danni per miliardi di dollari. Le organizzazioni colpite includono ospedali, aziende e istituzioni governative.
- Interruzione dei Servizi: Gli ospedali del Regno Unito, ad esempio, hanno subito gravi interruzioni nei servizi, con pazienti costretti a subire ritardi nelle cure.

4. Cosa Infetta

- Sistemi Operativi: WannaCry principalmente infetta sistemi Windows, in particolare versioni non aggiornate di Windows 7, Windows Server 2008 e Windows XP.
- Dispositivi Vulnerabili: Qualsiasi dispositivo con Windows esposto a Internet e non aggiornato con le ultime patch di sicurezza è a rischio. Anche computer collegati a reti interne non sicure possono essere infettati.

5. Prevenzione e Mitigazione

- Aggiornamenti di Sicurezza: È fondamentale mantenere il sistema operativo e il software aggiornati per chiudere le vulnerabilità sfruttate dal malware. Microsoft ha rilasciato patch di sicurezza per le versioni vulnerabili di Windows.
- Backup Regolari: Implementare strategie di backup regolari per i dati, preferibilmente su dispositivi non connessi alla rete, aiuta a prevenire la perdita di informazioni critiche.
- Formazione degli Utenti: Educare gli utenti sulla sicurezza informatica, in particolare sui rischi di phishing e su come riconoscere attività sospette.
- Utilizzo di Antivirus e Firewall: Installare software antivirus aggiornati e mantenere attivi i firewall per bloccare accessi non autorizzati.

Report

Piano d'Azione per Gestire l'Infezione da WannaCry

1. **Isolamento Immediato**
   Disconnettere il Computer dalla Rete: Rimuovere il cavo Ethernet o disattivare la connessione Wi-Fi.
   Pro: Impedisce la propagazione del malware.
   Contro: Potrebbe interrompere altre attività aziendali.
2. **Valutazione del Danno**
   Controllare i File Infetti: Identificare file crittografati e annotare eventuali messaggi di riscatto.
   Pro: Permette di avere un'idea chiara dell'impatto.
   Contro: Potrebbe rivelare la gravità della situazione.
3. **Backup dei Dati**
   Eseguire un Backup: Salvare i file non crittografati su un dispositivo esterno.
   Pro: Protegge i dati importanti da ulteriori perdite.
   Contro: Non recupera file già crittografati.
4. **Rimozione del Malware**
   Utilizzare Software Antimalware: Scaricare e installare un software antimalware come Malwarebytes.
   Pro: Può rimuovere il malware e ripristinare file.
   Contro: Potrebbe non rilevare tutte le varianti del malware.
5. **Ripristino di Sistema**
   Considerare il Ripristino di Sistema: Riportare il computer a uno stato precedente all'infezione.
   Pro: Potrebbe riportare il sistema a uno stato funzionante.
   Contro: Rischio di perdita di dati recenti.
6. **Formattazione del Disco (Se Necessario)**
   Formattare il Disco e Reinstallare il Sistema: Come ultima risorsa.
   Pro: Pulisce completamente il sistema da malware.
   Contro: Perdita totale di dati; richiede reinstallazione di software.
7. **Messa in Sicurezza del Sistema**
   Aggiornare il Sistema Operativo: Installare aggiornamenti di sicurezza.
   Pro: Chiude le vulnerabilità sfruttate dal malware.
   Contro: Potrebbe non essere disponibile per versioni obsolete.
   Installare un Antivirus: Proteggere il sistema da future infezioni.
   Pro: Fornisce una protezione continua.
   Contro: Non sempre efficace contro ransomware.
   Configurare un Firewall: Bloccare accessi non autorizzati.
   Pro: Aumenta la sicurezza della rete.
   Contro: Richiede configurazione e monitoraggio.
8. **Prevenzione di Futuri Attacchi**
   Formazione degli Utenti: Educare i dipendenti sulla sicurezza informatica.
   Pro: Aumenta la consapevolezza e riduce i rischi.
   Contro: Richiede tempo e risorse per l'implementazione.
   Eseguire Backup Regolari: Implementare strategie di backup.
   Pro: Protegge i dati in caso di futuri attacchi.
   Contro: Richiede spazio di archiviazione e gestione.
   Monitoraggio Attivo: Utilizzare strumenti per rilevare attività sospette.
   Pro: Consente una risposta rapida agli incidenti.
   Contro: Potrebbe generare falsi positivi.

Adottando questo piano d'azione e considerando i pro e contro di ciascuna misura, l'organizzazione può affrontare in modo più efficace l'infezione da WannaCry e migliorare la propria sicurezza informatica per il futuro.