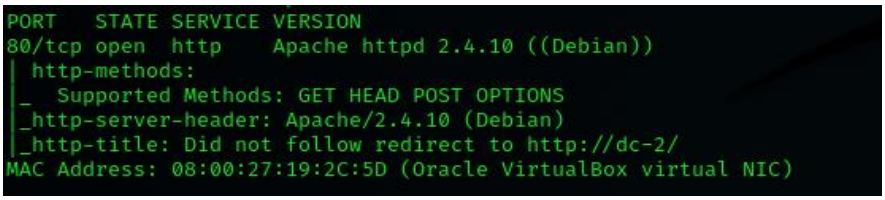
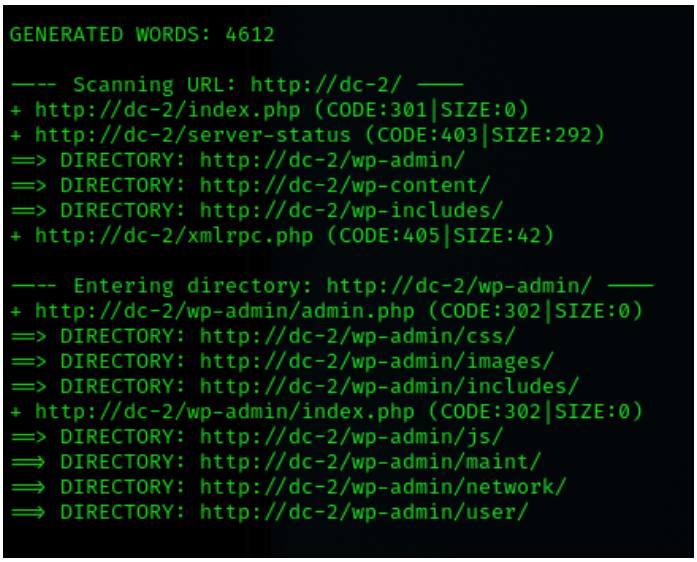
REPORT DC-2

STEP 1 Individuazione target(tool netdiscover)

STEP 2 SCANSIONE DEI SERVIZI (TOOL NMAP)

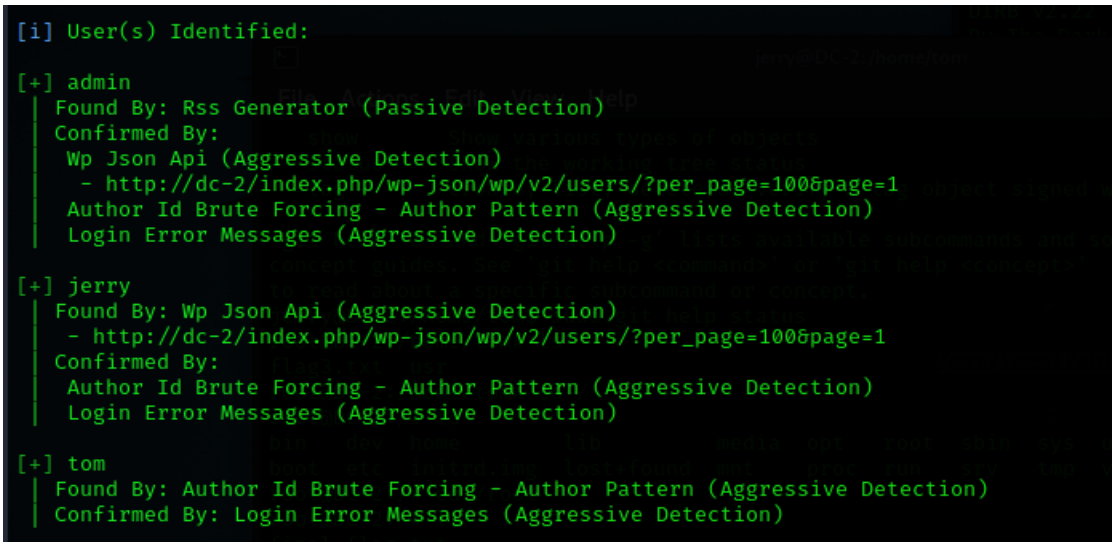


STEP 3 (enum content tool Dirb)



STEP 4

Una volta a conoscenza del CMS utilizzato era Wordpress procediamo con una scansione delle Vulnerabilità mediante il tool WPSCAN seguita dall' enumerazione degli USERS.



STEP 5

Adesso creiamo una wordlist mirata tramite il tool cewl

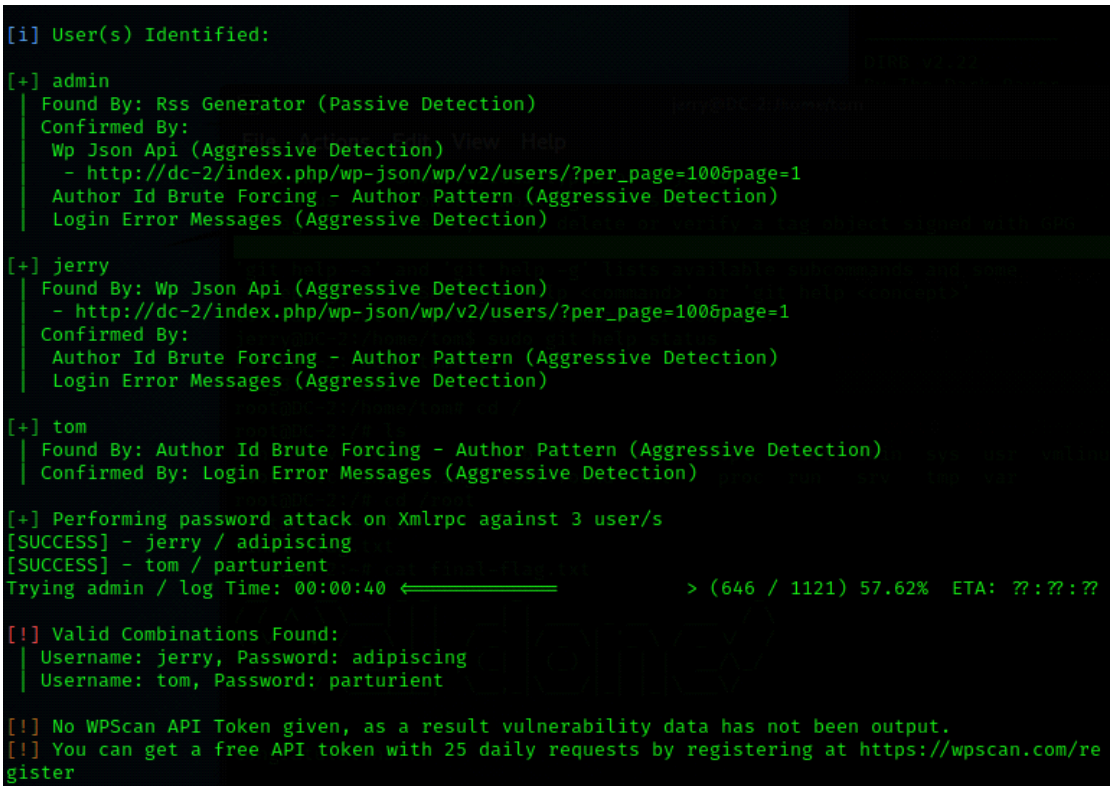
command:

cewl http://dc-2 -w wlist.txt

STEP 6

Procediamo con l'attacco a Dizionario mediante WPSCAN tramite il comando:

wpscan --url http://dc-2 -P wlist.txt



STEP 7

Adesso accediamo alla pagina del login ed effettuiamo l’accesso tramite jerry. Troviamo la seconda flag che ci consiglia di provare ad effettuare l’accesso tramite un altro metodo.

STEP 8

Accediamo tramite ssh con l’utente Tom e troviamo la 3 Flag. Ci rendiamo conto che ci troviamo in una rbash(restricted bash) nella quale possiamo utilizzare solo 2 comandi: ls e vi (Vim). Per bypassare rbash utilizziamo utilizziamo un metodo di " escape " tramite VI poi digitiamo:

set shell=/bin/bash

invio

:shell

così facendo siamo riusciti a cambiare la rbash. Qui ci accorgiamo che non basta perché i comandi classici della bin/bash non funzionano, da qui deduciamo che potrebbe esserci un problema con il settaggio della variabile d ambiente PATH, eseguendo un controllo è effettivamente cosi quindi andiamo a esportare con il comando EXPORT esportiamo la shell nel path corretto. Una volta fatto ciò riusciamo a loggarci con jerry.

STEP 9

Con il comando " sudo -l " vediamo che jerry può eseguire il comando " git " come amministratore senza una password. Sfruttando ciò tramite un'iniezione di codice all' interno della pagina del manuale di git digitando:

/bin/bash

Invio

Così facendo riusciamo a loggarci come root e a trovare l'ultima flag.

Abbiamo completato il Privilege Escalation !!