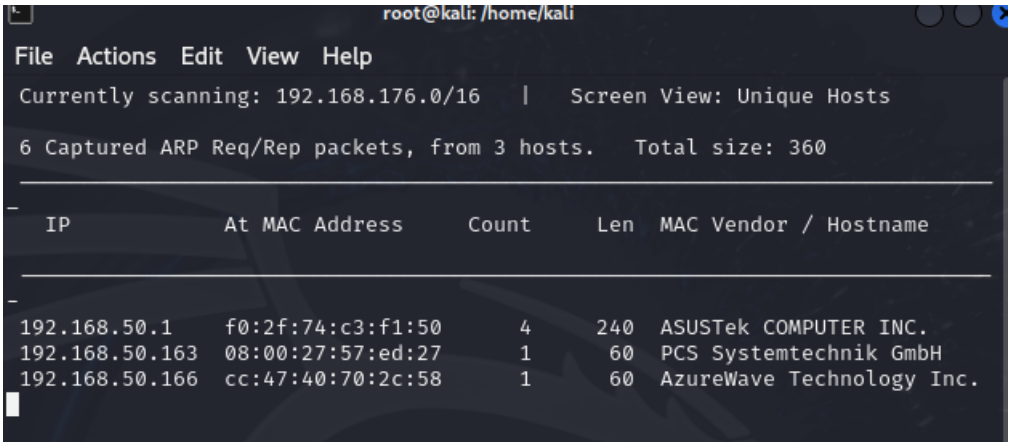
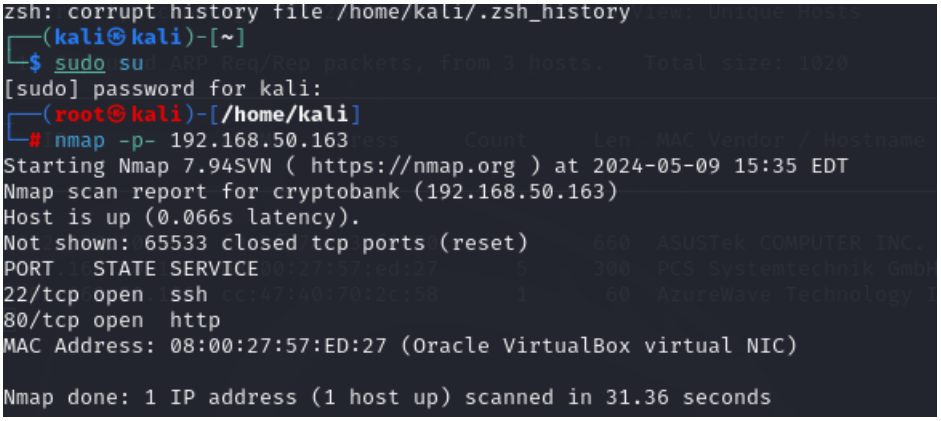
Benvenuti alla presentazione ufficiale della nuova piattaforma bancaria di Crypto Banking. La piattaforma che permetterà di poter conservare e gestire i propri Crypto asset è ospitata in un server Linux con servizio DHCP attivo.
La presente CTF Challenge presenta diverse flag da poter ottenere:
-Root flag del server
-Creazione di un account
-Dump delle credenziali OS
-Dump delle credenziali WebApp
-Schedulare un Task/Job
Portare effettiva evidenza dell'ottenimento di ogni risultato.

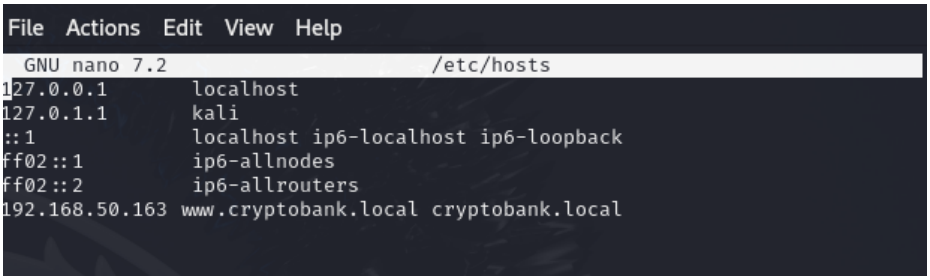
1) Per trovare l'IP della macchina: netdiscover→ IP 192.168.50.163



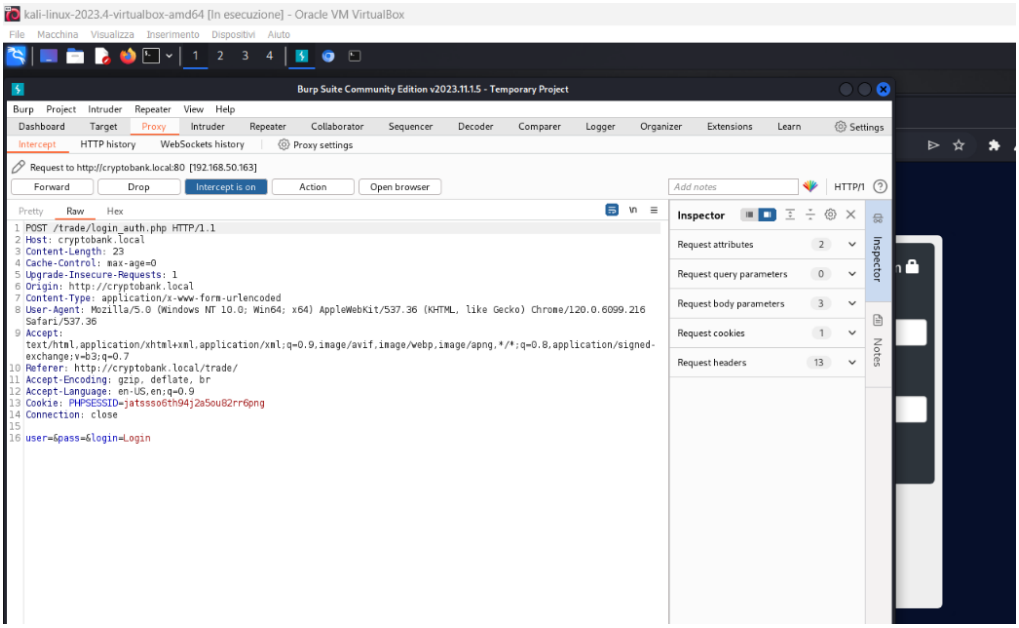
2) Nmap per trovare porte aperte: es. 80 http open



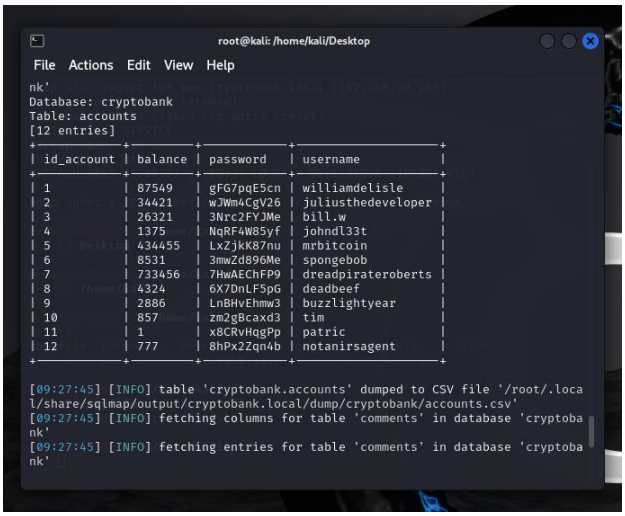
3) Etc/hosts → Ip + www.cryptobank.local



4) Burpsuite → Cliccando su "login" sulla pagina di accesso Cryptobank



5) Dopo aver copiato la richiesta in un file, ho aperto un terminale ed ho avviato sqlmap -r payload.txt –dump. Abbiamo trovato cosi una lista di username e password. Inserendo le credenziali nel login siamo entrati nell'area privata (per esempio di Wlliam Delisle founder e CEO).



6) Nella pagina dei prestiti, ho notato che su ciascuno dei prestiti c'era un parametro GET nell'URL. Ho deciso di controllare per la vulnerabilità di SQL injection.

```
1  GET /trade/applying_loan.php?loan_id=2 HTTP/1.1
2  Host: cryptobank.local
3  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-GB,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Cookie: PHPSESSID=98ibm273alni081qk6rs3oroq6
9  Upgrade-Insecure-Requests: 1
10
11
```

7) Ho provato poi con MSFCONSOLE per un exploit con meterpreter creando una shell, può essere un vettore di attacco utile per ottenere accesso a risorse di sistema o per eseguire codice malevolo sul server remoto.