Module 6.6: Parrot OS: passwords and insecure web

Parrot OS clean version:

Parrot install:

sudo apt install pwgen hashcat john openssl apg libcrack2 passwdqc

Parrot OS already has most of these

cracklib-check is hidden:

/usr/sbin/cracklib-check

1. use /usr/sbin/cracklib-check to check several passwords
2. use pwgen to create 5 passwords, record these for later use
3. use apg to create 5 more passwords, record these as well
4. experiment with the generation format: apg -m 12 -x 16 -n 5 means 5 passwords between 12 and 16 characters.
5. try all of your passwords with cracklib-check (above)
6. go here: https://emn178.github.io/online-tools/sha256.html and generate SHA256 hashes for your 10 passwords
7. create a password entropy checker (see code below)
8. evaluate the entropy of your 10 passwords
9. create a wordlist.txt file with the 10 passwords above, along with pal82 and papaya77
10. create a hashes.txt file with the 10 hashes from above
11. use hashcat to decode the hashes: hashcat -m 1400 -a 0 hashes.txt wordlist.txt
12. show your results: sudo hashcat --show -m 1400 hashes.txt
13. ssh into 10.14.88.83 and recover the hash for the pi user
14. attempt to decode this with hashcat
15. try a remote ssh password attack using hydra
16. use the command ip addr show to find your IP address
17. run python3 -m http.server 8000 to create a local web server
18. verify the local server is running at http://127.0.0.1:8000
19. go to the IP address :8000 to verify the web server is running
20. browse the page while watching the terminal

21. use tcpdump to monitor packets locally
22. capture packets for analysis using wireshark

- 23. use wireshark to analyze the pcap file

Migrated from Apple Server Wiki. Original page ID: Q4V7L1k

Revision #2
Created 2026-09-29 16:00:03 UTC by Admin
Updated 2026-09-29 16:23:12 UTC by Admin