Network Security

Stuff and stories of real hackers

OWASP, TU

Slide at :
https://github.com/human-divanshu/talks/tree/master/

Disclaimer and Ethics

This is for educational purpose only. Do not try any of this on a live network.

Always remember

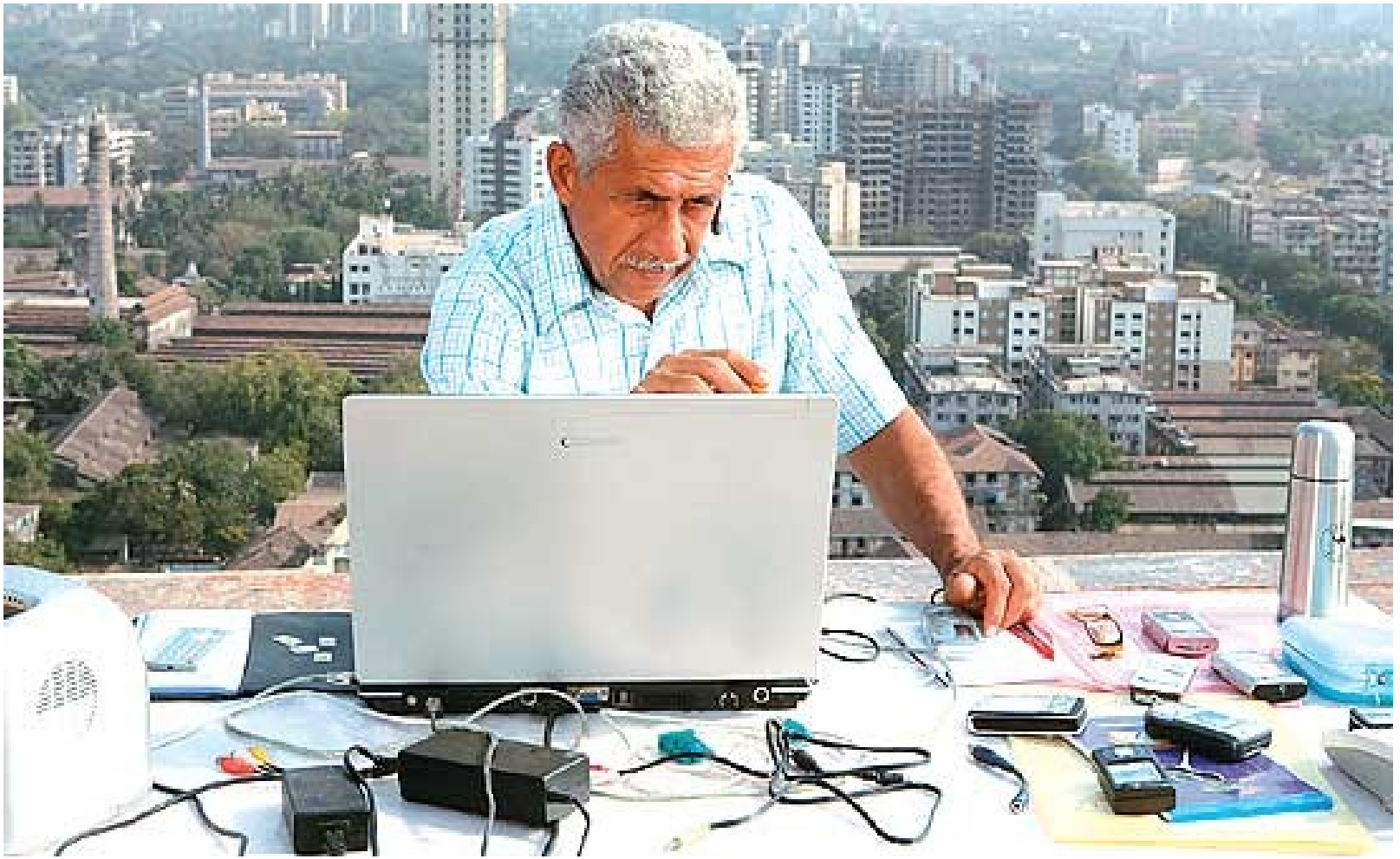
“With great power comes great responsibility”

- Uncle Ben

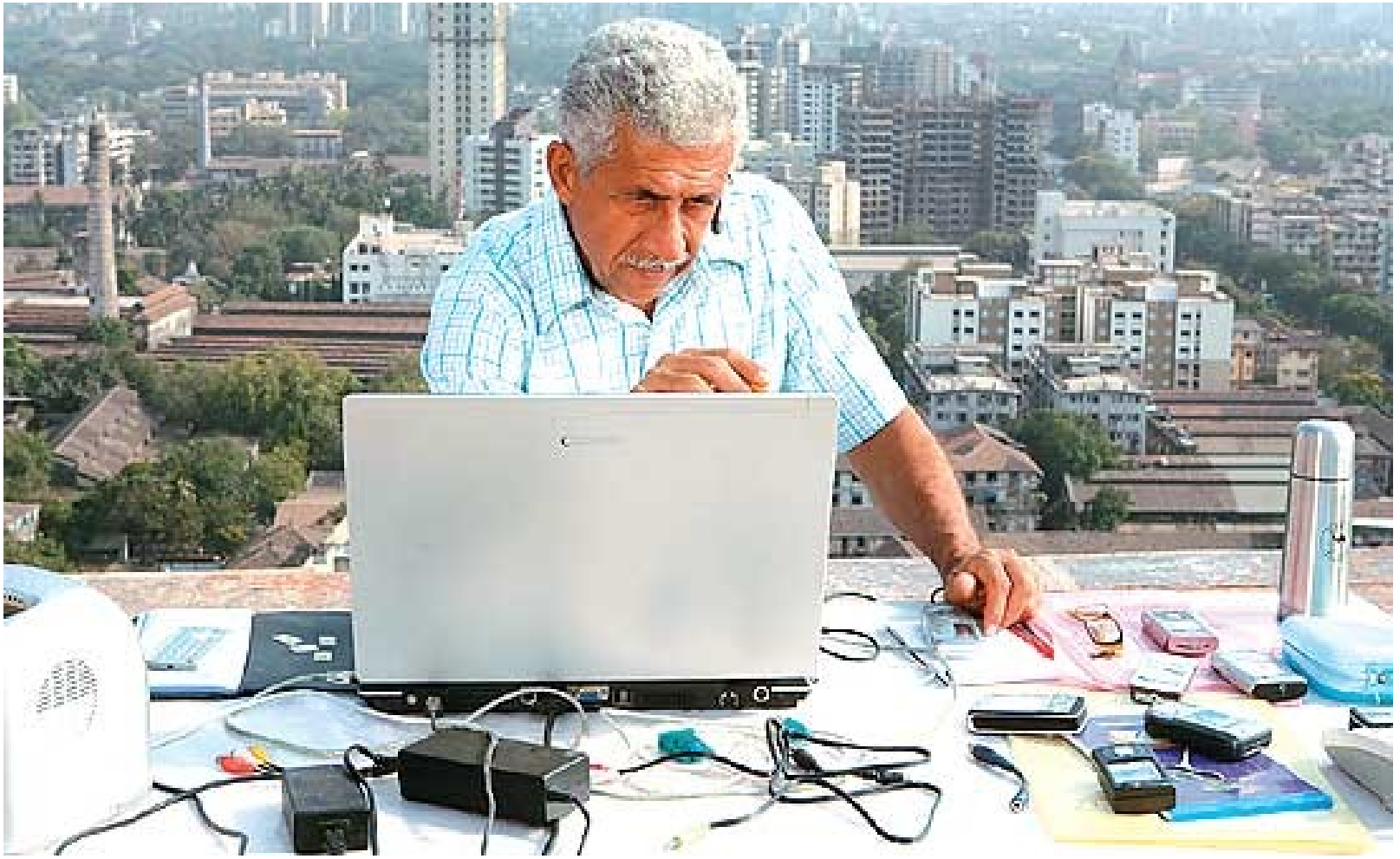
Contents

- Show off things (if not caught)
- 6 months to 1 year in jail
- 3 years to 5 years in jail

- Networking 101
- IP, Mask, Gateway
- TCP / IP Suite
- **Packet Sniffing**
- **Packet Spoofing**
- Data packet analysis
- Using Wireshark
- **GSM attack demos:**
  - **Call Spoofing**
  - **Call proxy**
- Hosts file and DNS
- Security Architecture
  - Windows
- **Simple redirection attack**
- **Email header spoofing (Fake emails)**
- Proxy, VPN, Tor
- **DoS attack**
- **Phishing attack**
- **Cookie stealing**
- **Session Hijacking**
- **ARP Poisoning**
- **LAN MITM**
- **Sniffing**
- **DNS Poisoning**
- **WAN MITM**
- **Wifi cracking**
- **System password cracking**
  - **Windows / Linux**



Self Initialized Multi-proxy Forwarding Attack



Demo Time

- Miss call attack
- Spoofed call attack
- Multi-proxy call attack

WARNING

DO NOT TRY UNLESS YOU KNOW

WHAT YOU ARE DOING

Prerequisites

- Must know a bit of programming (C / Java / Python / C++)
- Willing to learn
- Networking (Plus point – not required)

Computer hacking

=

(Networking * Programming * Vision)

Two ways to learn

- See demo of some attacks and try to replicate them own your own
- Outcome : Script Kiddie

- Learn concepts behind attacks and design your own attacks
- Outcomes : Elite hacker

Network

- Was designed to exchanged text messages
- What we are doing with it ?
  - Shopping
  - Banking – Online and ATM
  - TV, Cell phone
  - Playing Mini Militia
  - Running rail networks, nuclear power plants, etc

Network
(As per books)

Application
Transport
Network
Data Link
Physical

Network
(As per books)

Application	- HTTP, HTTPS, FTP, PING
Transport	- TCP, UDP
Network	- IP address, Routing, ARP, ICMP
Data Link	- MAC address, Ethernet
Physical	- Wires / Wireless

Network

(From security point of view)

Application	- All of security things are here
Transport	- No security
Network	- Host to host authentication (but rarely used)
Data Link	- No security
Physical	- Password protections

IP Address

- Unique number to identify you on network
- 192.168.1.2

Further research:
- IPv4 and IPv6
- NAT based IP address (Private IP)
- Public IP address
- DHCP and DORA process
- Static IP address
- Class full and class less IP addressing
- Subnet Mask
- Gateway
- MAC address (Hardware address)

Finding local IP

- Windows – ipconfig
- Linux - ifconfig

Activity:

Try to find following:

- Subnet mask
- Gateway
- DNS
- MAC address

DNS

- IP address is hard to remember
- So we use DNS just like your phone contacts
- Google.com is 216.58.196.14

Further research:

- Port numbers
- Port 53
- Services file in Windows and Linux

Finding public IP and path

- Ping
- Traceroute / tracert

Further research:

- ICMP
- IGMP

Ping sweeping

- Checking live hosts on a network
- fping -g 192.168.1.0 192.168.1.255

Further research:

Whats is meaning of ?

- 192.168.1.0 / 24

- 192.168.0.0 / 16

HOSTS file and DNS

(Browser)

Go to example.com

1. Hey, hosts file do you know IP of example.com ?

2. No. Ask DNS about it. (99.9%)

HOSTS file

3. Hey DNS dude, do you know IP of example.com ?

DNS

4. Yes of course. I know everyone. Example.com is x.y.z.k

Where is hosts file ?

- C:/Windows/System32/drivers/etc
- /etc/hosts

Further research:

- Check for HOSTS file in your OS
- Find how to edit it

Simple Redirect Attack

- Sending user to a wrong website
- Redirect demo

Further research:

- Can you redirect all websites to a single website by making just one entry ?

Part of code from a redirection virus

```
...

char entry[ ] = “\n141.0.174.42 google.com”;

...

FILE *fp = fopen(“C:\\Windows\\System32\\drivers\\etc\\hosts”, “a”);

fputs(entry, fp);

fclose(fp);

...
```

Coding:

- Is \\ a typo in path ?

- Write a simple redirection code in language of your choice and check what permission are required to execute it.

Reverse DNS

- Converting to domain name from IP address

Further research:

- Find the domain name of IP address being used in code on previous slide.
- Google about following tools
    - nslookup
    - dig
    - host

Packet Sniffing

- To see data packets (using tools like wireshark)

What happens when you connect to a network ?

- Working of DHCP
- DORA process

Packet Sniffing : DEMO

- Finding packets for DHCP DORA process

Data Packet Analysis

- Reverse engineering a ARP packet