บทที่ 3 : การป้องกันการเจาะระบบ Part3

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

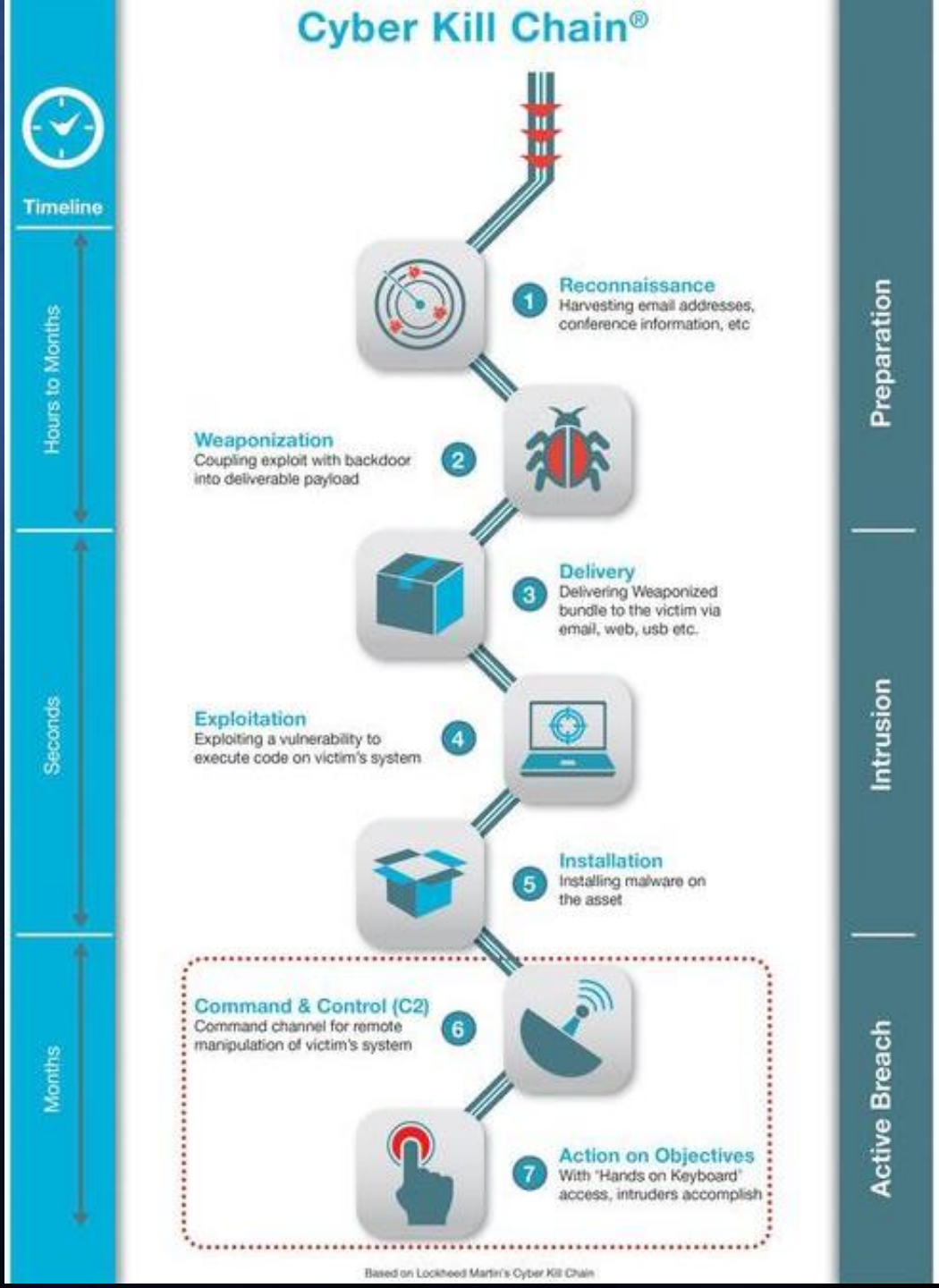
Agenda

Cyber Kill Chain

Cyber Kill Chain

ถูกคิดค้นโดย Lockheed Martin บริษัทด้านอากาศยาน การป้องกัน ความมั่นคงปลอดภัย และเทคโนโลยีระดับสูงชื่อดังของสหรัฐฯ เพื่อบรรยายถึงขั้นตอนของการเจาะระบบเพื่อโจมตีไซเบอร์

มีทั้งหมด 7 ขั้นตอน แบ่งเป็น 3 เฟส



Ref: https://www.techtalkthai.com/introduction-to-cyber-kill-chain/

Phase 1: ขั้นเตรียมการ (Preparation)

1. ลาดตระเวน (Reconnaissance : Recon)
2. เตรียมอาวุธ (Weaponization)

Step1: ลาดตระเวน (Reconnaissance : Recon)

- แฮ็คเกอร์จะเริ่มต้นเก็บรวบรวมข้อมูลของเป้าหมายให้ได้มากที่สุดก่อนเริ่มการโจมตี โดยอาจค้นหาข้อมูลจากโลกอินเทอร์เน็ต โซเชียลเน็ตเวิร์ค เป็นต้น
- เป็นขั้นตอนที่เป้าหมายยังไม่รู้ตัว
- เครื่องมือที่ใช้ เช่น Google, SHODAN, Maltego, nmap, the Harvester, เทคนิค Social Engineering

Shodan Developers Monitor View All...

SHODAN

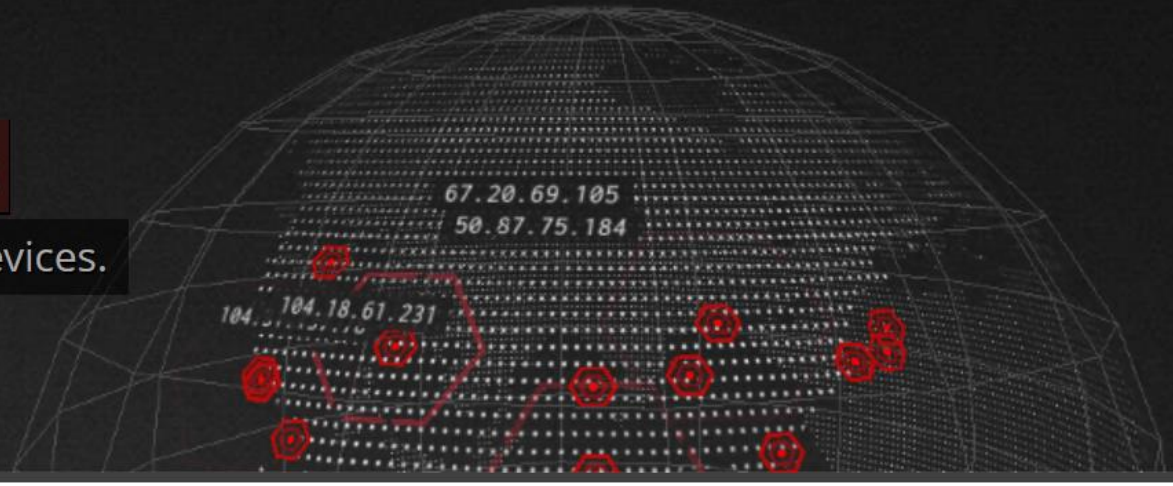
Explore Pricing Enterprise Access

New to Shodan? Login or Register

The search engine for Webcams

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

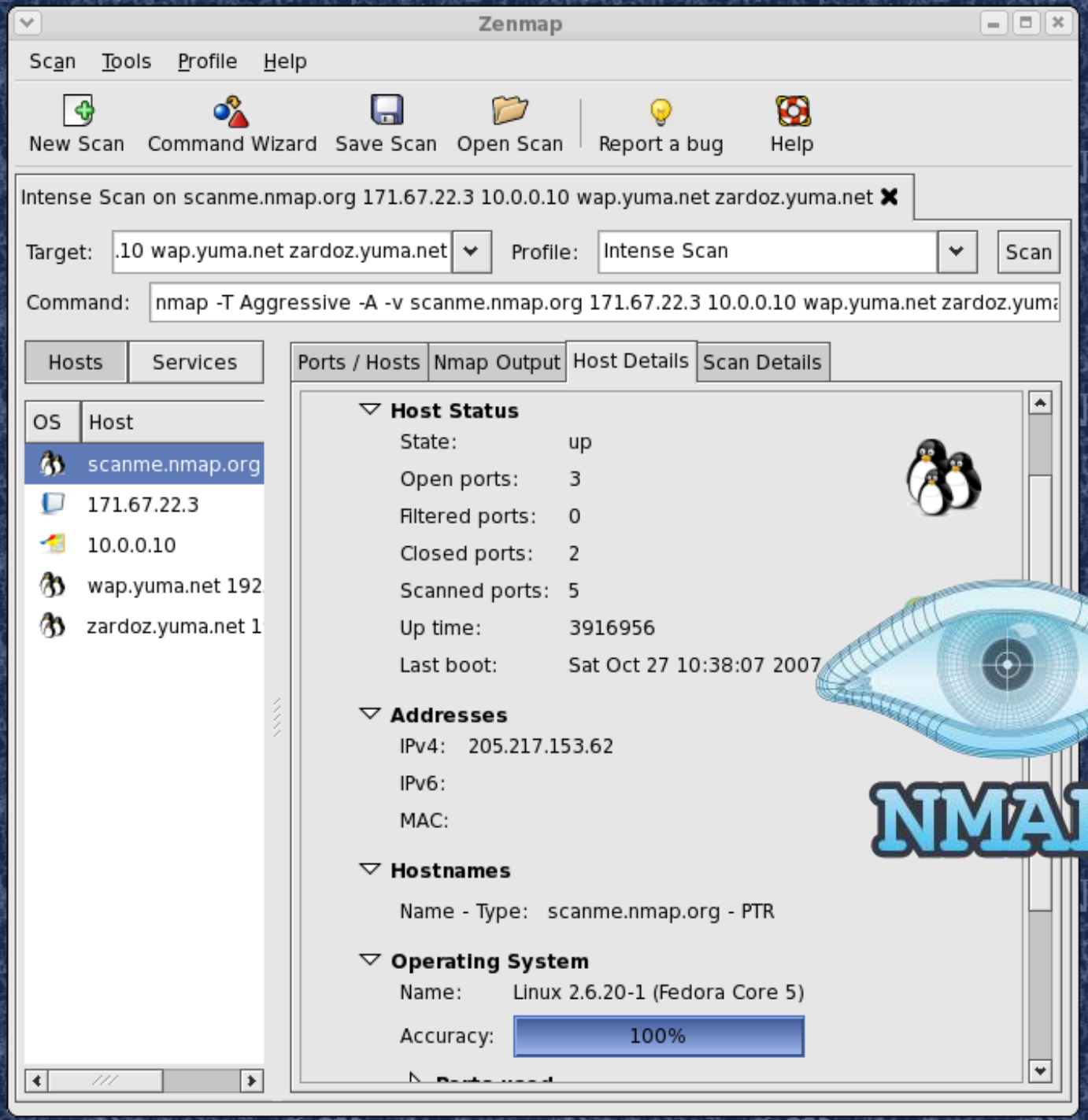
Monitor Network Security

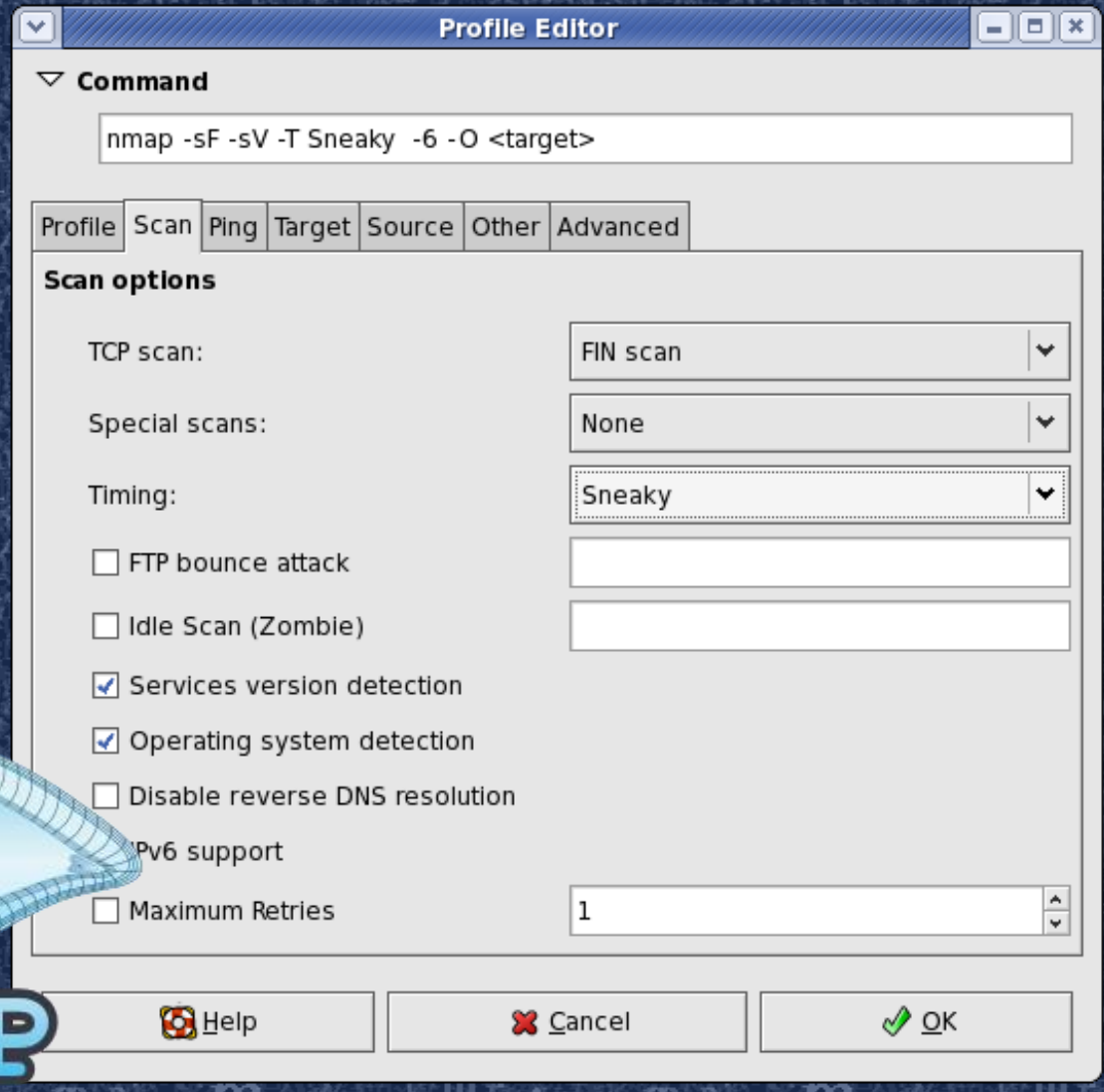
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

SHODAN


Zenmap
Scan Tools Profile Help
New Scan
Command Wizard
Save Scan
Open Scan
Report a bug
Help
Intense Scan on scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net
Target: .10 wap.yuma.net zardoz.yuma.net
Profile: Intense Scan
Scan
Command: nmap -T Aggressive -A -v scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma
Hosts
Services
OS
Host
scanme.nmap.org
171.67.22.3
10.0.0.10
wap.yuma.net 192
zardoz.yuma.net 1
Ports / Hosts
Nmap Output
Host Details
Scan Details
Host Status
State: up
Open ports: 3
Filtered ports: 0
Closed ports: 2
Scanned ports: 5
Up time: 3916956
Last boot: Sat Oct 27 10:38:07 2007
Addresses
IPv4: 205.217.153.62
IPv6:
MAC:
Hostnames
Name - Type: scanme.nmap.org - PTR
Operating System
Name: Linux 2.6.20-1 (Fedora Core 5)
Accuracy: 100%


Profile Editor
Command
nmap -sF -sV -T Sneaky -6 -O <target>
Profile
Scan
Ping
Target
Source
Other
Advanced
Scan options
TCP scan: FIN scan
Special scans: None
Timing: Sneaky
FTP bounce attack
Idle Scan (Zombie)
Services version detection
Operating system detection
Disable reverse DNS resolution
IPv6 support
Maximum Retries
1
Help
Cancel
OK

NMAP

Maltego – Interactive Data Mining

Step 2: เตรียมอาวุธ (Weaponization)

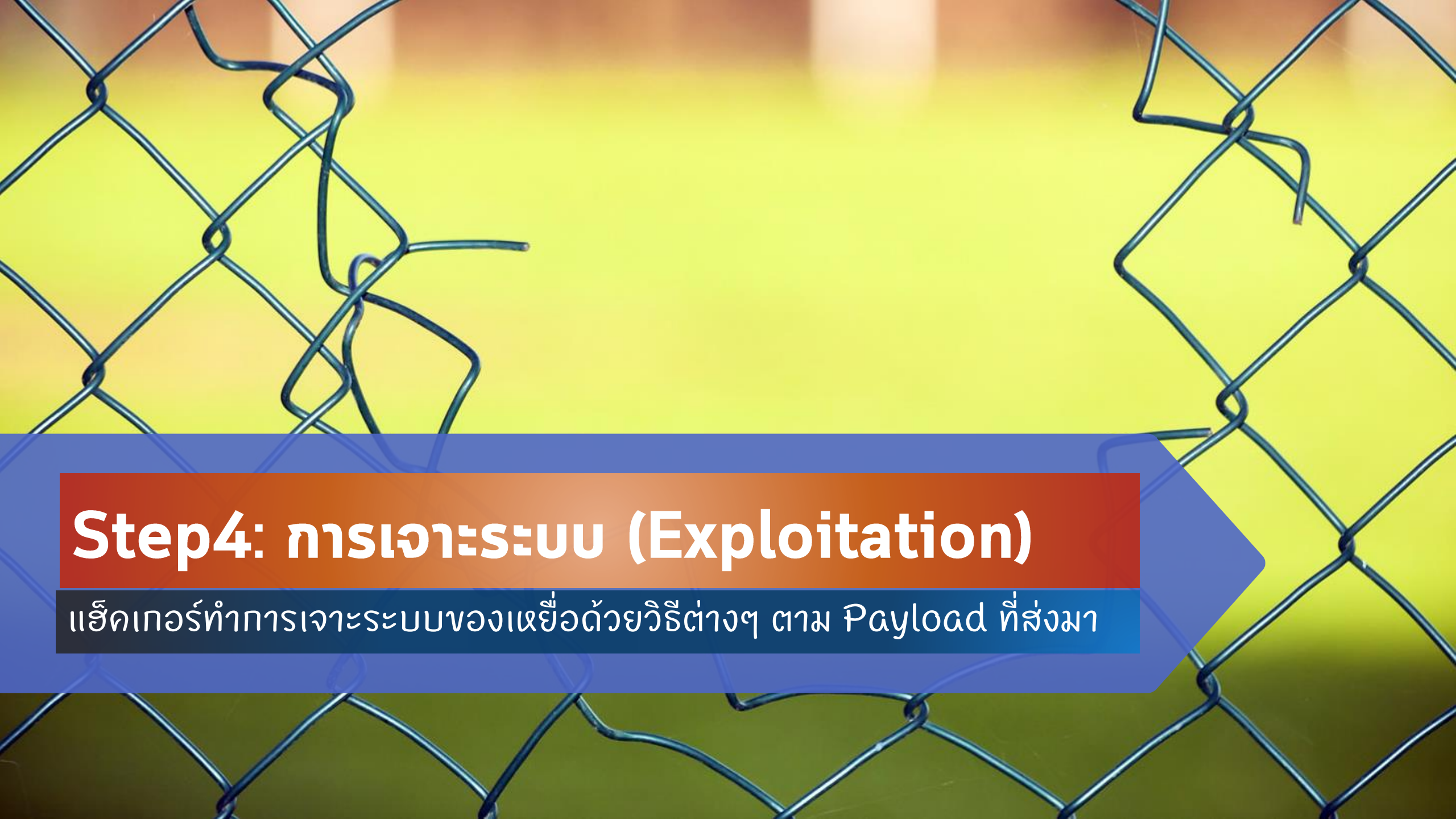
- แฮ็คเกอร์จะเตรียมหาวิธีเจาะระบบและเตรียม Malicious Payload เพื่อส่งไปยังเหยื่อที่เล็งไว้
- ขั้นตอนนี้เหยื่อจะยังไม่รู้ตัว
- เครื่องมือที่ใช้ได้แก่ มัลแวร์ หรือเครื่องมือในการเจาะระบบทั้งหลาย เช่น Metasploit หรือเครื่องมืออื่น ๆ

Phase 2: การบุกรุก (Intrusion)

3. การส่ง (Delivery)
4. การเจาะระบบ (Exploitation)
5. การติดตั้งเครื่องมือ (Installation)

Step 3: การส่ง (Delivery)

- แฮ็คเกอร์ส่ง Malicious Payload ไปยังเหยื่อ ผ่านทางอีเมล เว็บไซต์ หรือ USB ซึ่งใน Payload นี้จะประกอบไปด้วยวิธีการบุกรุกโจมตีมากมายเพื่อใช้เจาะเข้าระบบของเหยื่อ
- การ Phishing เป็นการเปิดทางการโจมตีที่ทรงประสิทธิภาพมากที่สุด



Step4: การเจาะระบบ (Exploitation)

แฮ็คเกอร์ทำการเจาะระบบของเหยื่อด้วยวิธีต่างๆ ตาม Payload ที่ส่งมา

```
root@kali:~# msfconsole
```

METASPLOIT

...EXPLOITATION TOOL...

https://metasploit.com

```
       =[ metasploit v4.17.17-dev                         ]
+ -- --=[ 1817 exploits - 1031 auxiliary - 315 post        ]
+ -- --=[ 539 payloads - 42 encoders - 10 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Step 5: การติดตั้งเครื่องมือ (Installation)

ติดตั้งมัลแวร์บนเครื่องของเหยื่อ (ในกรณีที่แฮ็คเกอร์ใช้มัลแวร์) หรืออะไรบางอย่างเพื่อให้คอยรับคำสั่งและทำการบางอย่างตามที่แฮ็คเกอร์ต้องการ

Phase 3: เก็บเกี่ยวผลลัพธ์ (Active Breach)

6. รับคำสั่งและควบคุม (Command & Control : C&C || C2)
7. เก็บเกี่ยวผลประโยชน์ (Action on Objectives)

Step 6 : รับคำสั่งและควบคุม (Command & Control : C&C || C2)

แฮ็คเกอร์สร้างช่องทางในการรับส่งคำสั่งกับมัลแวร์ที่ติดตั้งไว้ เพื่อให้สามารถจัดการและควบคุมมัลแวร์ให้ทำตามความต้องการ โดยปกติจะใช้ Backdoor เป็นช่องทางรับคำสั่ง

Step 7: เก็บเกี่ยวผลประโยชน์ (Action on Objectives)

เก็บเกี่ยวผลประโยชน์ตามที่ตนเองต้องการจากเหยื่อ เช่น ขโมยข้อมูล เปลี่ยนแปลงแก้ไขข้อมูล หรือทำลายระบบ เป็นต้น

อ้างอิง

- https://www.techtalkthai.com/introduction-to-cyber-kill-chain/
- งานสัมมนา Rex x Blue Pill 2019