



การจัดการความมั่นคงปลอดภัยทางข้อมูล

Information Security Management

Chapter 5 : Hacking

เนื้อหา

- ความรู้พื้นฐานเกี่ยวกับการเจาะระบบ
- ขั้นตอนการเจาะระบบ
- การลาดตระเวนหาข่าว (Reconnaissance)
- การค้นหาเป้าหมาย (Scanning)
- การเจาะเข้าระบบ (Exploitation)
- การรักษาช่องทางเข้าระบบ (Maintaining Access)

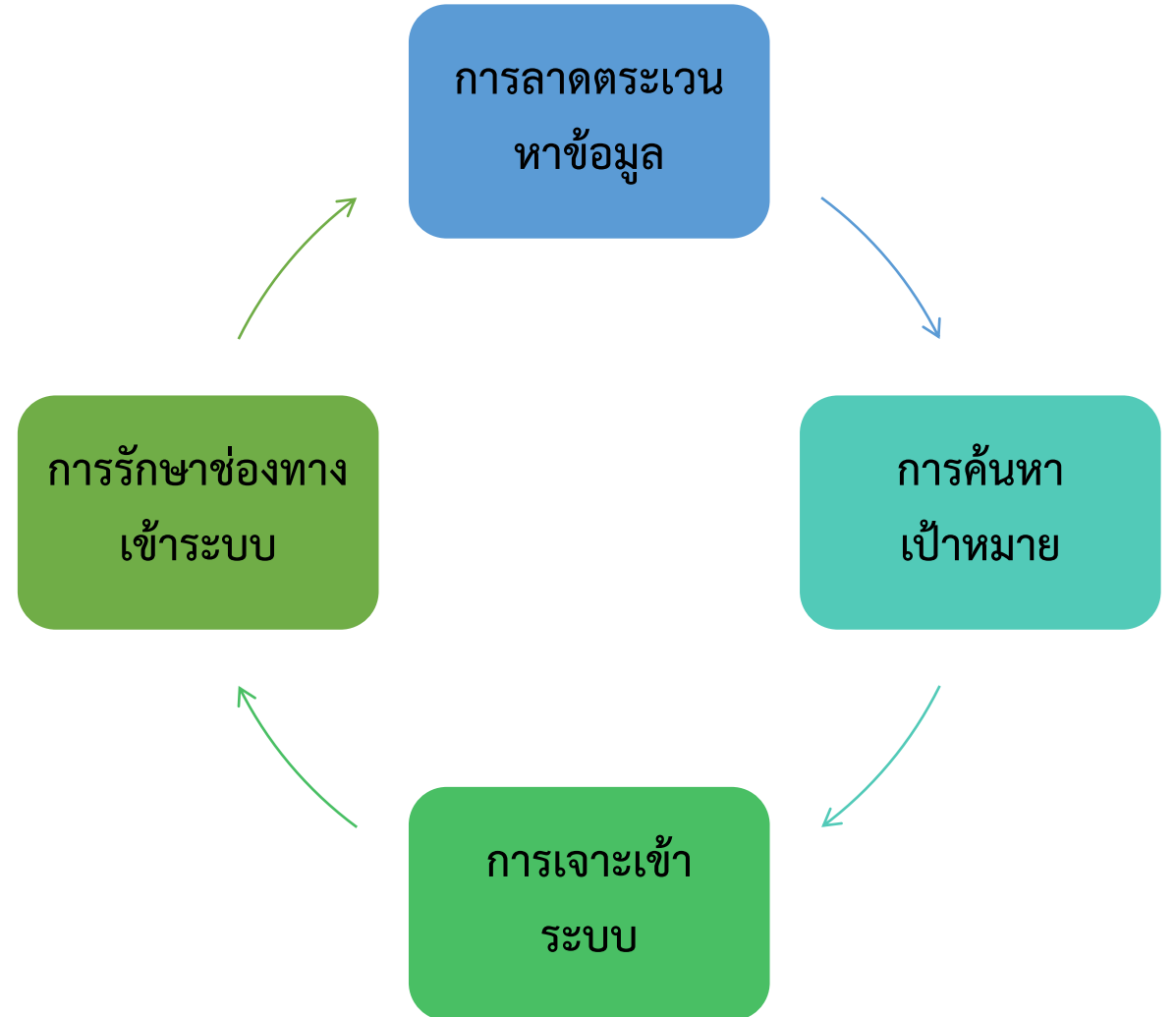
ความรู้พื้นฐานเกี่ยวกับการเจาะระบบ

เมื่อก่อนการสอนเทคนิคการแฮคระบบเป็นเรื่องต้องห้าม แต่ปัจจุบันเริ่มเปลี่ยนไป เนื่องจากคนเริ่มเห็นคุณค่าของการทดลองเจาะระบบ และหลายองค์กรใช้ในการประเมินความเสี่ยงของตนเอง

การเจาะระบบ เป็นส่วนหนึ่งของกระบวนการรักษาความปลอดภัยขององค์กร เพราะเป็นการประเมินความเสี่ยงผ่านมุมมองของศัตรู ทำให้เรามีเวลานารปิดช่องโหว่ของระบบที่ค้นพบได้ก่อน

ความรู้พื้นฐานเกี่ยวกับการเจาะระบบ

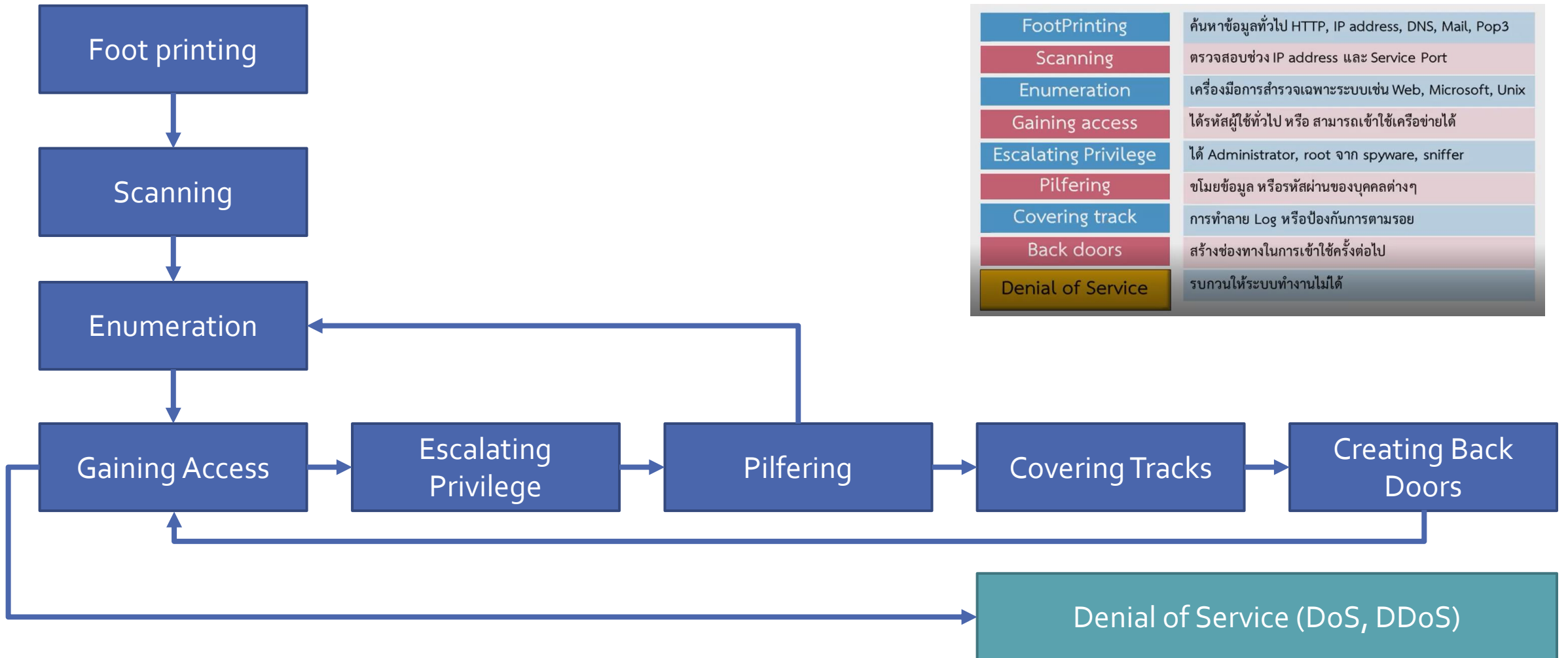
การใช้ประโยชน์จากช่องโหว่ (Vulnerability) ของระบบคอมพิวเตอร์ ซึ่งโดยปกติจะผิดกฎหมาย นอกเสียจากว่าได้รับอนุญาตในการเจาะระบบ ซึ่งจะเรียกว่า การทดสอบเจาะระบบ (Pen-test)



ประเภทของผู้โจมตีระบบ

ผู้โจมตี	ระดับความชำนาญ	แรงจูงใจ
แฮคเกอร์ (Hacker)	ปานกลาง - สูง	เพื่อปรับปรุงระบบรักษาความปลอดภัย
แคร็คเกอร์ (Cracker)	ปานกลาง - สูง	เพื่อทำลายระบบ
สคริปต์คิดดี้ (Script-kiddy)	ต่ำ	เพื่อให้ได้การยอมรับ
สายลับ (Spy)	สูง	เพื่อให้ได้เงิน
พนักงาน (Employee)	หลากหลาย	หลากหลาย
ผู้ก่อการร้าย (Terrorist)	ปานกลาง - สูง	เพื่ออุดมการณ์ทางการเมือง

ขั้นตอนการเจาะระบบ



การลาดตระเวนหาข่าว (Reconnaissance)

ถือเป็นขั้นตอนที่สำคัญที่สุด ในกระบวนการเจาะระบบ ในการให้เวลากับการเก็บรวบรวมข้อมูลเกี่ยวกับเป้าหมายซึ่งจะทำให้ได้ข้อมูลที่เป็นประโยชน์อย่างมากในขั้นตอนถัดไป โดยสามารถทำได้หลากหลายวิธี เช่น

การการลาดตระเวนหาข่าวด้วย Google

site:

intitle, allintitle:

inurl, allinurl:

cache:

filetype:

related:



EASY HACK TRICKS



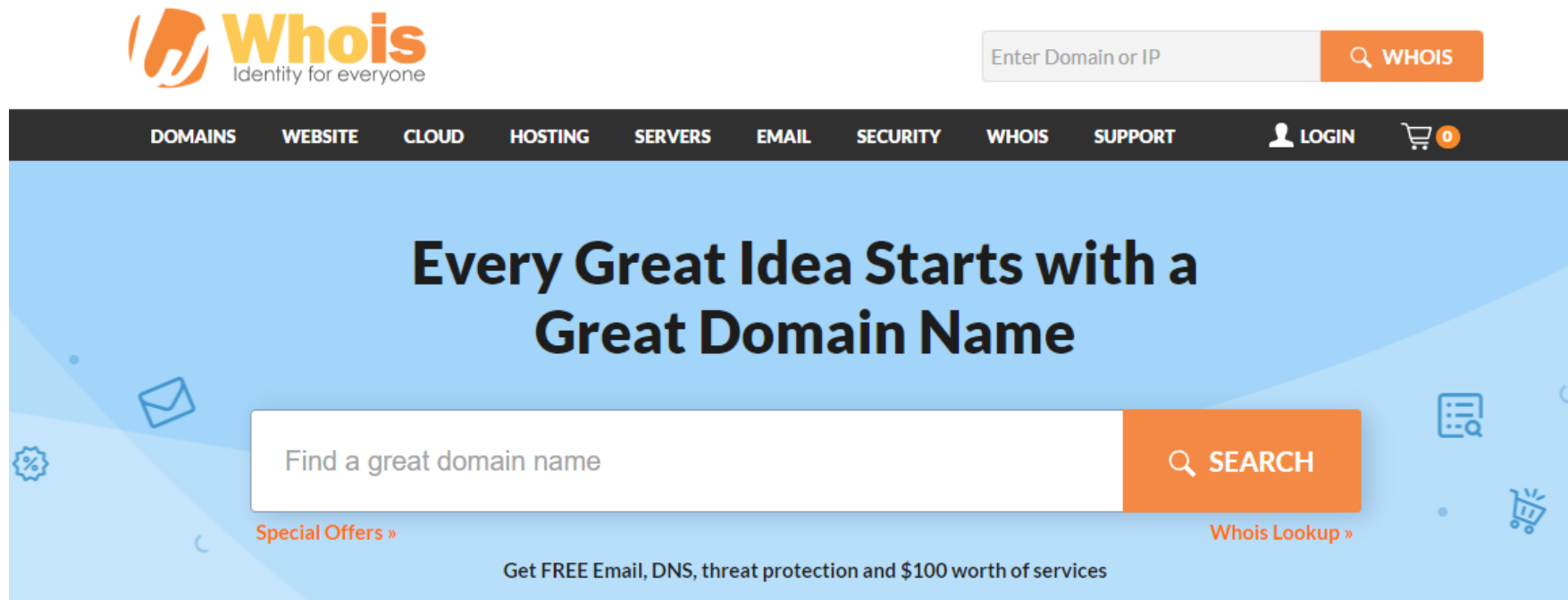
การการลาดตระเวนหาข่าวด้วย HTTrack

เป็นเครื่องมือที่ใช้ในการ ก๊อปปี้เว็บไซต์ที่
ละหน้ามาไว้ที่เครื่องของเรา ทำให้สะดวกในการ
วิเคราะห์อย่างละเอียด ในขั้นตอนนี้ ควรระวัง
เพราะจะถูกตรวจจับได้ง่าย การรันโปรแกรมนี้
ควรได้รับอนุญาตเสียก่อน



การการลาดตระเวนหาข่าวด้วย WHOIS

เป็นเครื่องมือที่ใช้งานง่ายและมีประสิทธิภาพในการเก็บข้อมูล ทำให้เราสามารถเข้าถึงข้อมูลเฉพาะของเครื่องเป้าหมาย เช่น หมายเลขไอพี โฮสต์เนม และผู้ติดต่อพร้อมที่อยู่



The screenshot displays the Whois website interface. At the top left is the logo for Whois, featuring an orange flame-like icon and the text "Whois Identity for everyone". To the right of the logo is a search bar with the placeholder text "Enter Domain or IP" and an orange button labeled "WHOIS". Below the logo and search bar is a dark navigation bar with white text for various services: DOMAINS, WEBSITE, CLOUD, HOSTING, SERVERS, EMAIL, SECURITY, WHOIS, and SUPPORT. On the right side of this bar are icons for a user profile labeled "LOGIN" and a shopping cart with a "0" inside. The main content area has a light blue background with the headline "Every Great Idea Starts with a Great Domain Name" in bold black text. Below the headline is a large white search bar with the placeholder text "Find a great domain name" and an orange button labeled "SEARCH". At the bottom of the page, there are two links: "Special Offers »" on the left and "Whois Lookup »" on the right. A footer at the very bottom reads "Get FREE Email, DNS, threat protection and \$100 worth of services".

การการลาดตระเวนหาข่าว

และยังมีอีกหลากหลายเครื่องมือ เช่น

- NETCRAFT
- NS Lookup
- Dig

การค้นหาเป้าหมาย (Scanning)

หลังจากเก็บรวบรวมข้อมูลแล้ว ในขั้นตอนนี้จะเป็นการจัดระเบียบของข้อมูลที่รวบรวมมา เช่น การจัดกลุ่มของเป้าหมายตามหมายเลขไอพี โฮสต์เนม หรือ URL ก็ตาม เสร็จแล้วเราจะดำเนินการ สแกนระบบ โดยแบ่งเป็น 3 ขั้นตอน ดังนี้

1. ตรวจสอบระบบว่าเครื่องใดเปิดใช้งานอยู่
2. ตรวจสอบพอร์ตของระบบที่เปิดใช้งาน
3. สแกนระบบเพื่อหาช่องโหว่

และดำเนินการทำรายการบัญชีเป้าหมายที่เป็นหมายเลขไอพี เพื่อขออนุมัติการโจมตีจากเจ้าของเสียก่อน เนื่องจากขั้นตอนต่อไปจะสร้างผลกระทบต่อเป้าหมายได้

การค้นหาเป้าหมาย (Scanning)

โดยใช้เทคนิคต่างๆ เช่น

- Ping and ping Sweeps เป็นการทดสอบส่งข้อมูลเล็กๆ ไปยังเป้าหมายเพื่อดูว่ามี การตอบกลับมาหรือไม่
- Port Scanning เป็นการตรวจสอบเครื่องเป้าหมายว่ามีบริการอะไรที่เปิดเอาไว้บ้าง
- การใช้เครื่องมือ NMAP

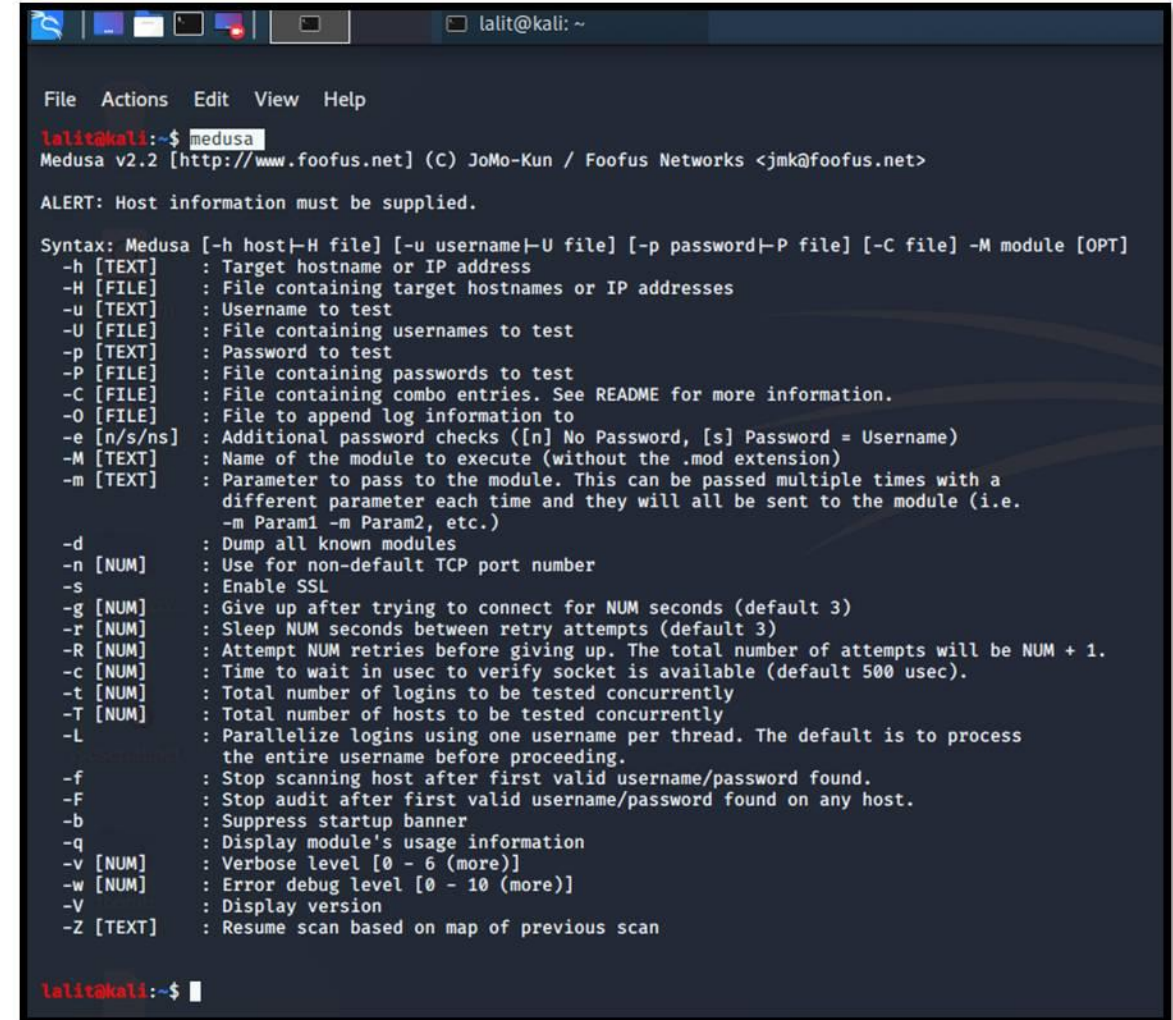


การเจาะเข้าระบบ (Exploitation)

เป็นกระบวนการในการเจาะเข้าระบบและควบคุมระบบ ซึ่งจะเป็กระบวนการในการใช้ประโยชน์จากช่องโหว่หรือจุดอ่อนที่ระบบเป้าหมายมี ซึ่งขั้นตอนนี้ถือเป็นขั้นตอนที่ท้าทายมากที่สุด ซึ่งจะต้องใช้ความรู้ความสามารถของผู้โจมตีเป็นหลัก ประกอบกับเครื่องมือที่ใช้ในการเจาะเข้าระบบก็มีให้ใช้งานหลากหลายเครื่องมือ เช่น

การเจาะระบบ (Exploitation) : MEDUSA

เป็นเครื่องมือที่ใช้ในการ Crack Password แบบออนไลน์ ซึ่งจะเป็นการโจมตีแบบ บรูทฟอร์ส (brute-force attack) ซึ่งผู้ใช้งานจำเป็นจะต้องมีการป้อน ดิกชันนารี (Password Dictionary File) เพื่อใช้ในการโจมตีเข้าระบบล็อกอิน ต่างๆ เช่น FTP HTTP MS-SQL MySQL POP3



```
lalit@kali:~$ medusa
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

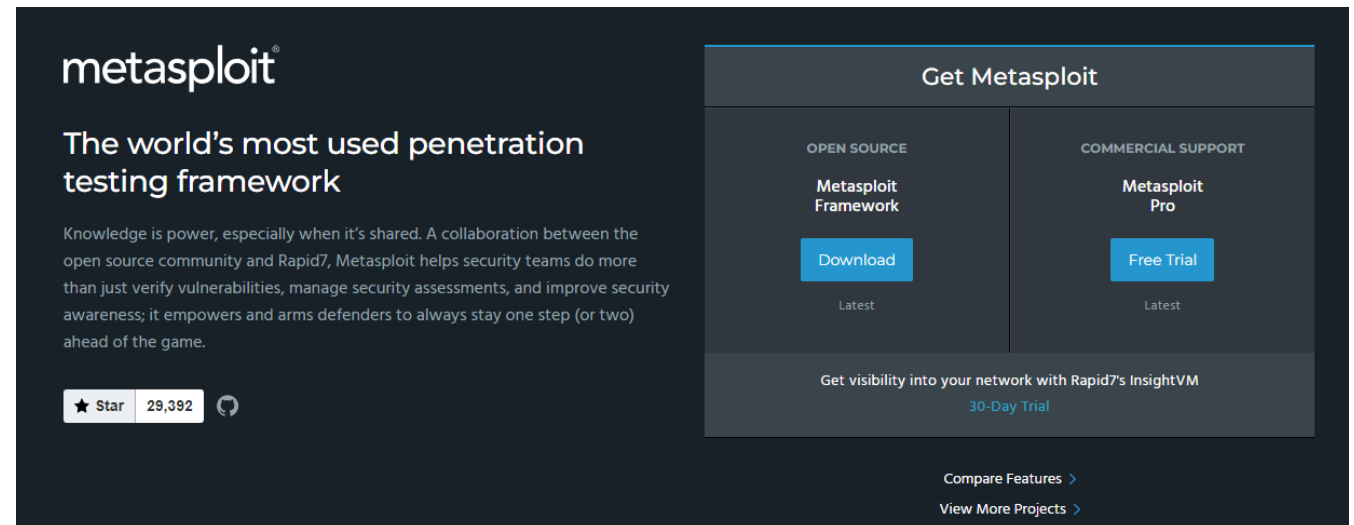
ALERT: Host information must be supplied.

Syntax: Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file] [-C file] -M module [OPT]
-h [TEXT]      : Target hostname or IP address
-H [FILE]      : File containing target hostnames or IP addresses
-u [TEXT]      : Username to test
-U [FILE]      : File containing usernames to test
-p [TEXT]      : Password to test
-P [FILE]      : File containing passwords to test
-C [FILE]      : File containing combo entries. See README for more information.
-o [FILE]      : File to append log information to
-e [n/s/ns]    : Additional password checks ([n] No Password, [s] Password = Username)
-M [TEXT]      : Name of the module to execute (without the .mod extension)
-m [TEXT]      : Parameter to pass to the module. This can be passed multiple times with a
                  different parameter each time and they will all be sent to the module (i.e.
                  -m Param1 -m Param2, etc.)
-d             : Dump all known modules
-n [NUM]       : Use for non-default TCP port number
-s            : Enable SSL
-g [NUM]       : Give up after trying to connect for NUM seconds (default 3)
-r [NUM]       : Sleep NUM seconds between retry attempts (default 3)
-R [NUM]       : Attempt NUM retries before giving up. The total number of attempts will be NUM + 1.
-c [NUM]       : Time to wait in usec to verify socket is available (default 500 usec).
-t [NUM]       : Total number of logins to be tested concurrently
-T [NUM]       : Total number of hosts to be tested concurrently
-L            : Parallelize logins using one username per thread. The default is to process
                  the entire username before proceeding.
-f            : Stop scanning host after first valid username/password found.
-F            : Stop audit after first valid username/password found on any host.
-b            : Suppress startup banner
-q            : Display module's usage information
-v [NUM]       : Verbose level [0 - 6 (more)]
-w [NUM]       : Error debug level [0 - 10 (more)]
-V            : Display version
-Z [TEXT]      : Resume scan based on map of previous scan

lalit@kali:~$
```

การเจาะระบบ (Exploitation) : Metasploit

เป็นเครื่องมือยอดนิยม เนื่องจากมีความยืดหยุ่น และประสิทธิภาพสูง จะทำการเลือกเป้าหมายแล้วทำการโจมตีเพย์โหลด ซึ่ง เพย์โหลดในที่นี้หมายถึง การระบุฟังก์ชันหรือสิ่งที่ ต้องการให้เป้าหมายเปลี่ยนแปลง เช่น การเพิ่มผู้ใช้งานให้กับเครื่องเป้าหมาย การเปิด Backdoor ทิ้งไว้ และการติดตั้ง Software ใหม่ลงบนเครื่อง



The screenshot shows the Metasploit website landing page. On the left, the 'metasploit' logo is displayed above the text 'The world's most used penetration testing framework'. Below this, a paragraph describes the tool's capabilities. At the bottom left, there is a GitHub star badge showing 29,392 stars. On the right, a 'Get Metasploit' section offers two options: 'Metasploit Framework' (Open Source) with a 'Download' button, and 'Metasploit Pro' (Commercial Support) with a 'Free Trial' button. A footer section promotes 'Rapid7's InsightVM' with a '30-Day Trial' offer. Navigation links for 'Compare Features' and 'View More Projects' are located at the bottom right.

การเจาะระบบ (Exploitation) : John The Ripper

เป็นเครื่องมือตรวจสอบความปลอดภัยของรหัสผ่านแบบโอเพ่นซอร์สและการกู้คืนรหัสผ่านสำหรับระบบปฏิบัติการหลายระบบ

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~#  
root@kali:~# john --wordlist=/usr/share/john/password.lst /root/johns_passwd  
Created directory. /root/.john  
Warning: detected hash type "sha512crypt", but the string is also recognized as  
"crypt"  
Use the "--format=crypt" option to force loading these as that type instead  
Using default input encoding: UTF-8  
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA5  
12 128/128 SSE2 2x])  
Will run 2 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
password (john)  
lg 0:00:00:07 DONE (2015-11-06 01:44) 0.1424g/s 505.1p/s 650.9c/s 650.9C/s modem  
..sss  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed  
root@kali:~#  
root@kali:~#
```

การรักษาช่องทางเข้าระบบ (Maintaining Access)

เมื่อสามารถเข้าถึงระบบได้แล้ว ขั้นตอนถัดไปคือ การค้นหาและขโมยข้อมูลที่สำคัญออกมา และถ้าจุดประสงค์หลักไม่ใช่การทำลายระบบ ก็จะต้องทำการรักษาช่องทางเข้าถึงระบบเอาไว้ แต่ถ้าเป้าหมายหลัก คือการล้าลายระบบ หรือทำให้ระบบใช้งานไม่ได้ ขั้นตอนนี้ก็จะไม่จำเป็นต้องดำเนินการ

ซึ่งขั้นตอนการสร้างช่องทางให้กลับเข้ามาในระบบได้อีกครั้ง โดยที่ผู้ดูแลระบบนั้นมีโอกาส น้อยที่จะเห็นช่องทางนี้ เราจะเรียกว่า [แบ็คดอร์ \(Backdoor\)](#)

แบ็คดอร์ (Backdoor)

Backdoor คือ ช่องทางที่โปรแกรมเมอร์หรือผู้พัฒนาระบบสร้างไว้ เพื่อให้สามารถเข้าถึงระบบหรือเครื่องคอมพิวเตอร์ได้โดยไม่ต้องผ่านกระบวนการตรวจสอบปกติที่อนุญาตให้เข้าถึงระบบได้ โดยทั่วไป Backdoor จะถูกสร้างขึ้นโดยการเขียนโปรแกรมซ่อนไว้ในระบบที่ผู้พัฒนาได้ออกแบบไว้

ซึ่งมีจุดประสงค์ เพื่อให้สามารถทดสอบระบบนั้นๆ ได้อย่างสะดวกรวดเร็ว แต่ก็อาจมีผู้ไม่หวังดีที่ใช้ Backdoor เพื่อเข้าสู่ระบบและสร้างความเสียหายให้แก่ระบบนั้นด้วยเช่นกัน

