การจัดการความมั่นคงปลอดภัยทางข้อมูล

Information Security Management

Chapter 5 : Hacking

เนื้อหา

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

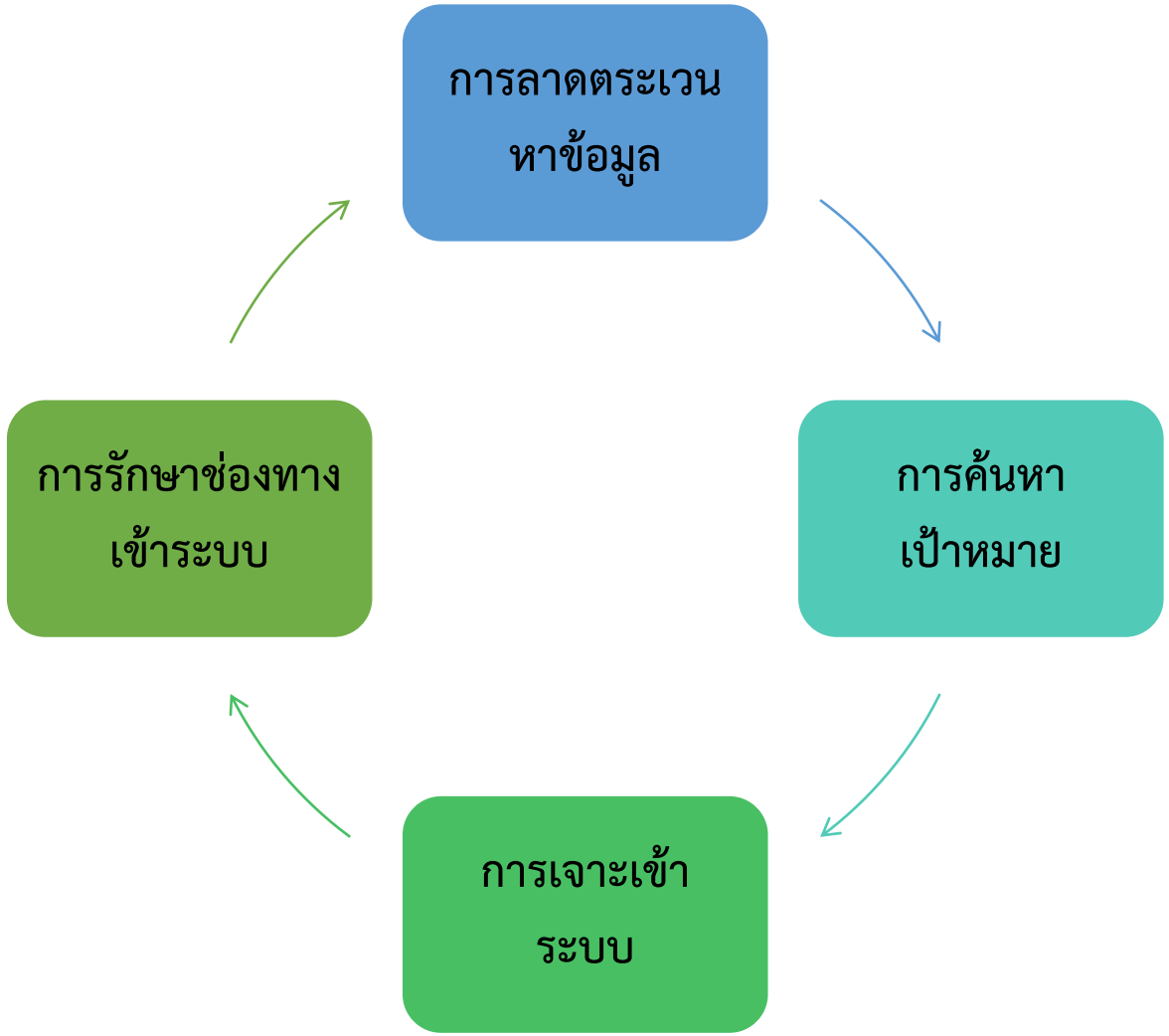
ความรู้พื้นฐานเกี่ยวกับการเจาะระบบ

เมื่อก่อนการสอนเทคนิคการแฮคระบบเป็นเรื่องต้องห้าม แต่ปัจจุบันเริ่มเปลี่ยนไป เนื่องจากคนเริ่มเห็นคุณค่าของการทดลองเจาะระบบ และหลายองค์กรใช้ในการประเมินความสี่ยงของตนเอง

การเจาะระบบ เป็นส่วนหนึ่งของกระบวนการรักษาความปลอดภัยขององค์กร เพราะเป็นการประเมินความเสี่ยงผ่านมุมมองของศัตรู ทำให้เรามีเวลานารปิดช่องโหว่ของระบบที่ค้นพบได้ก่อน

ความรู้พื้นฐานเกี่ยวกับการเจาะระบบ

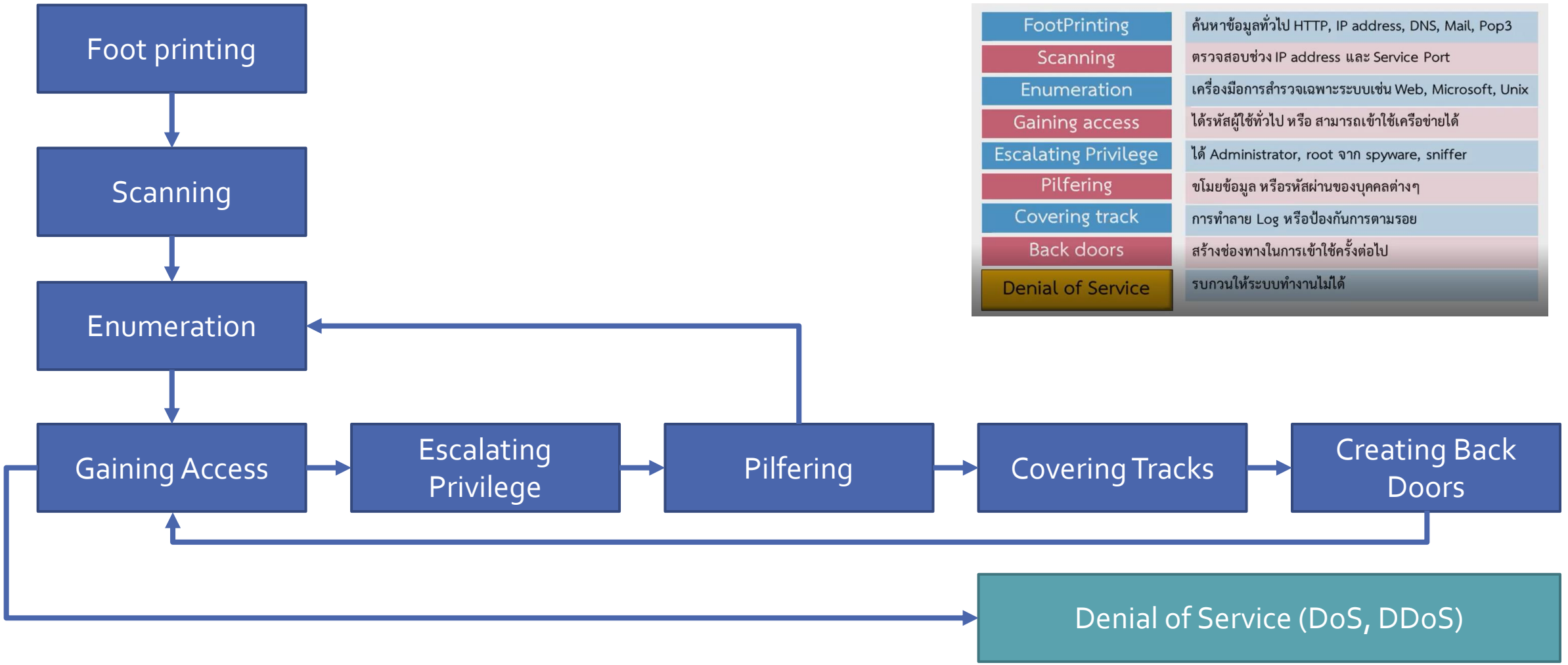
การใช้ประโยชน์จากช่องโหว่ (Vulnerability) ของระบบคอมพิวเตอร์ ซึ่งโดยปกติจะผิดกฎหมาย นอกเสียจากว่าได้รับอนุญาตในการเจาะระบบ ซึ่งจะเรียกว่า การทดสอบเจาะระบบ (Pen-test)



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



FootPrinting	ค้นหาข้อมูลทั่วไป HTTP, IP address, DNS, Mail, Pop3
Scanning	ตรวจสอบช่วง IP address และ Service Port
Enumeration	เครื่องมือการสำรวจเฉพาะระบบเช่น Web, Microsoft, Unix
Gaining access	ได้รหัสผู้ใช้ทั่วไป หรือ สามารถเข้าใช้เครือข่ายได้
Escalating Privilege	ได้ Administrator, root จาก spyware, sniffer
Pilfering	ขโมยข้อมูล หรือรหัสผ่านของบุคคลต่างๆ
Covering track	การทำลาย Log หรือป้องกันการตามรอย
Back doors	สร้างช่องทางในการเข้าใช้ครั้งต่อไป
Denial of Service	รบกวนให้ระบบทำงานไม่ได้

การลาดตระเวนหาข่าว (Reconnaissance)

ถือเป็น**ขั้นตอนที่สำคัญที่สุด** ในกระบวนการเจาะระบบ ในการให้เวลากับการเก็บรวบรวมข้อมูลเกี่ยวกับเป้าหมายซึ่งจะทำให้ได้ข้อมูลที่เป็นประโยชน์อย่างมากในขั้นตอนถัดไป โดยสามารถทำได้หลากวิธี เช่น

การการลาดตระเวนหาข่าวด้วย Google

site:

intitle, allintitle:

inurl, allinurl:

cache:

filetype:

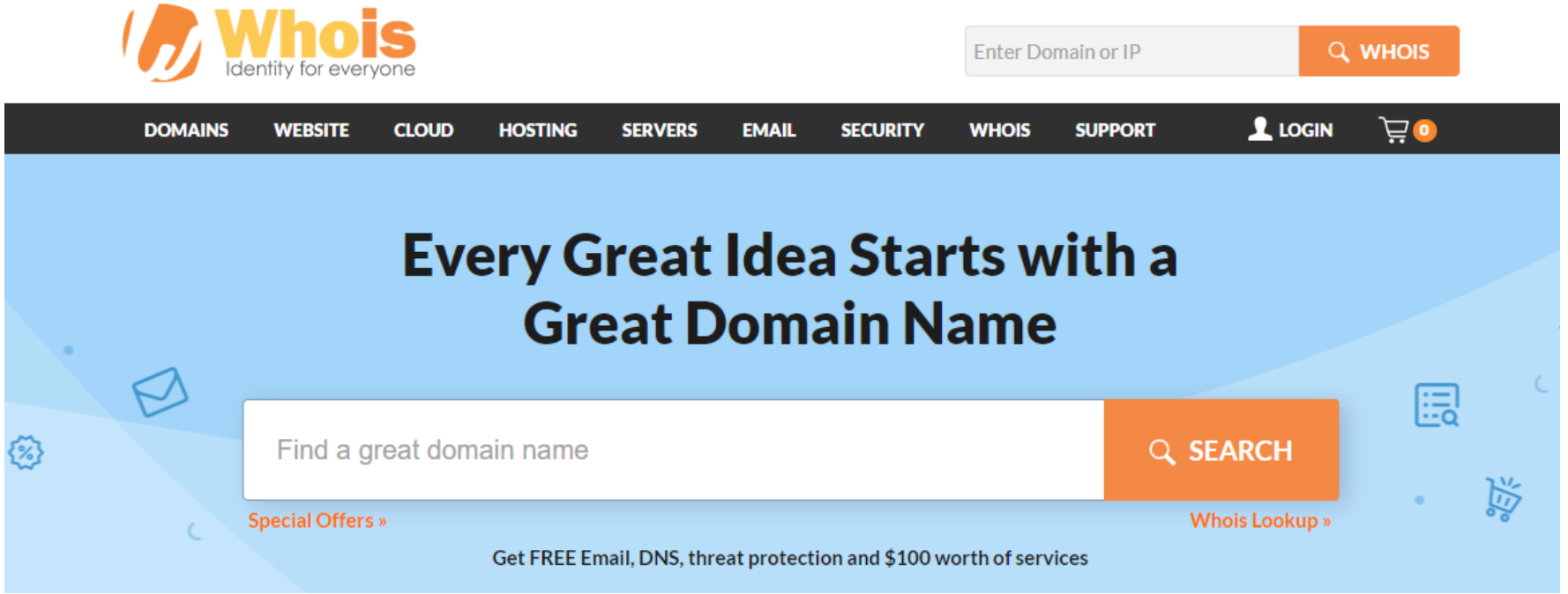
related:

การการลาดตระเวนหาข่าวด้วย HTTrack

เป็นเครื่องมือที่ใช้ในการ ก๊อปปี้เว็บไซต์ทีละหน้ามาไว้ที่เครื่องของเรา ทำให้สะดวกในการวิเคราะห์อย่างละเอียด ในขั้นตอนนี้ควรระวังเพราะจะถูกตรวจจับได้ง่าย การรันโปรแกรมนี้ควรได้รับอนุญาตเสียก่อน

การการลาดตระเวนหาข่าวด้วย WHOIS

เป็นเครื่องมือที่ใช้งานง่ายและมีประสิทธิภาพในการเก็บข้อมูล ทำให้เราสามารถเข้าถึงข้อมูลเฉพาะของเครื่องเป้าหมาย เช่น หมายเลขไอพี โฮสต์เนม และผู้ติดต่อพร้อมที่อยู่



การการลาดตระเวนหาข่าว

และยังมีอีกหลากหลายเครื่องมือ เช่น

- NETCRAFT
- NS Lookup
- Dig

การค้นหาเป้าหมาย (Scanning)

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

1. สำรวจระบบว่าเครื่องใดเปิดใช้งานอยู่
2. สำรวจพอร์ตของระบบที่เปิดใช้งาน
3. สแกนระบบเพื่อหาช่องโหว่

และดำเนินการทำรายการบัญชีเป้าหมายที่เป็นหมายเลขไอพี เพื่อขออนุมัติการโจมตีจากเจ้าของเสียก่อน เนื่องจากขั้นตอนต่อไปจะสร้างผลกระทบต่อเป้าหมายได้

การค้นหาเป้าหมาย (Scanning)

โดยใช้เทคนิคต่างๆ เช่น

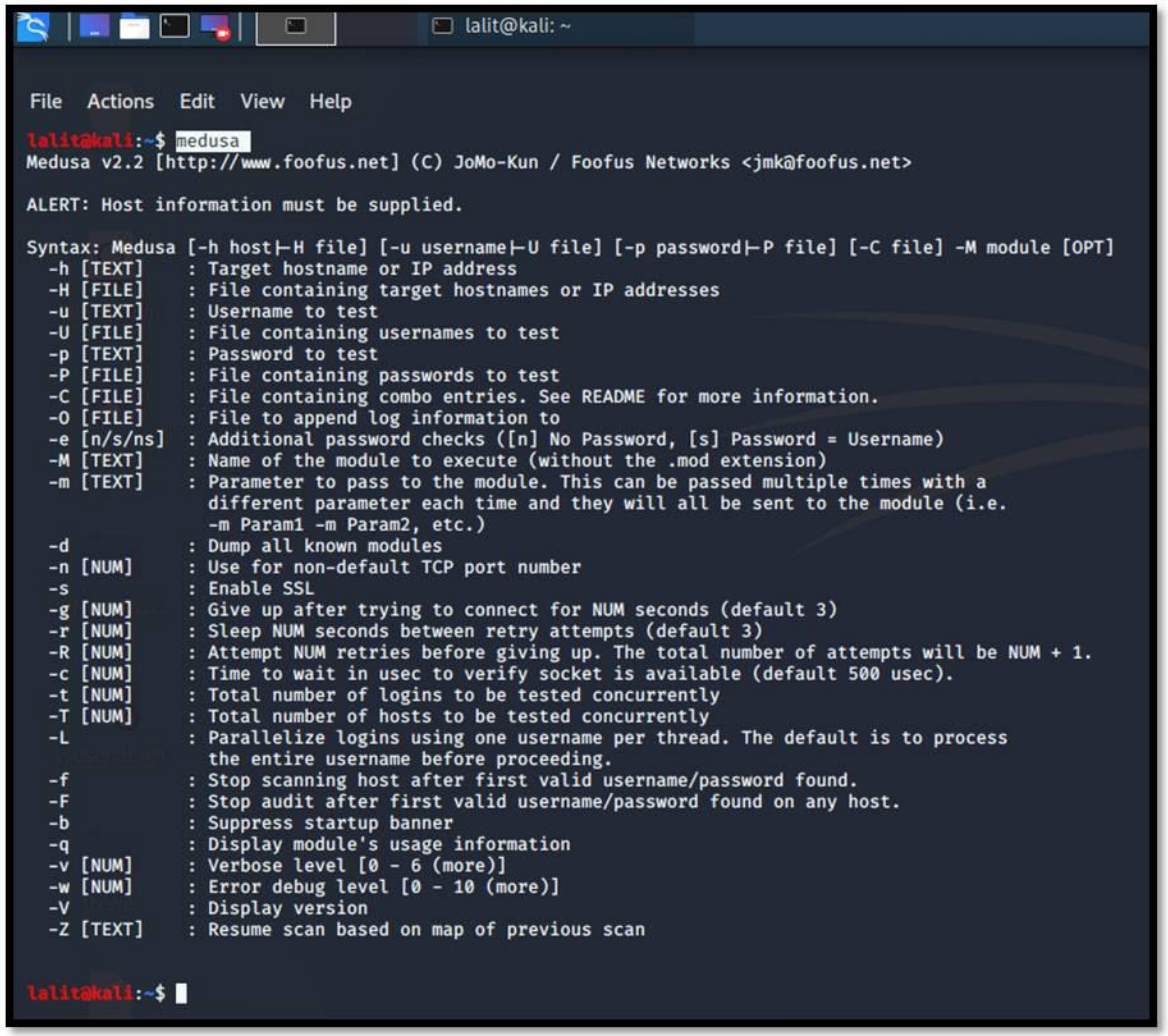
- Ping and ping Sweeps เป็นการทดสอบส่งข้อมูลเล็กๆ ไปยังเป้าหมายเพื่อดูว่ามีการตอบกลับมาหรือไม่
- Port Scanning เป็นการตรวจสอบเครื่องเป้าหมายว่ามีบริการอะไรที่เปิดเอาไว้บ้าง
- การใช้เครื่องมือ NMAP

การเจาะเข้าระบบ (Exploitation)

เป็นกระบวนการในการเจาะเข้าระบบและควบคุมระบบ ซึ่งจะเป็นกระบวนการในการใช้ประโยชน์จากช่องโหว่หรือจุดอ่อนที่ระบบเป้าหมายมี ซึ่งขั้นตอนนี้ถือเป็น**ขั้นตอนที่ท้ายทายมากที่สุด** ซึ่งจะต้องใช้ความรู้ความสามารถของผู้โจมตีเป็นหลัก ประกอบกับเครื่องมือที่ใช้ในการเจ้าเข้าระบบก็มีให้ใช้งานหลากเครื่องมือ เช่น

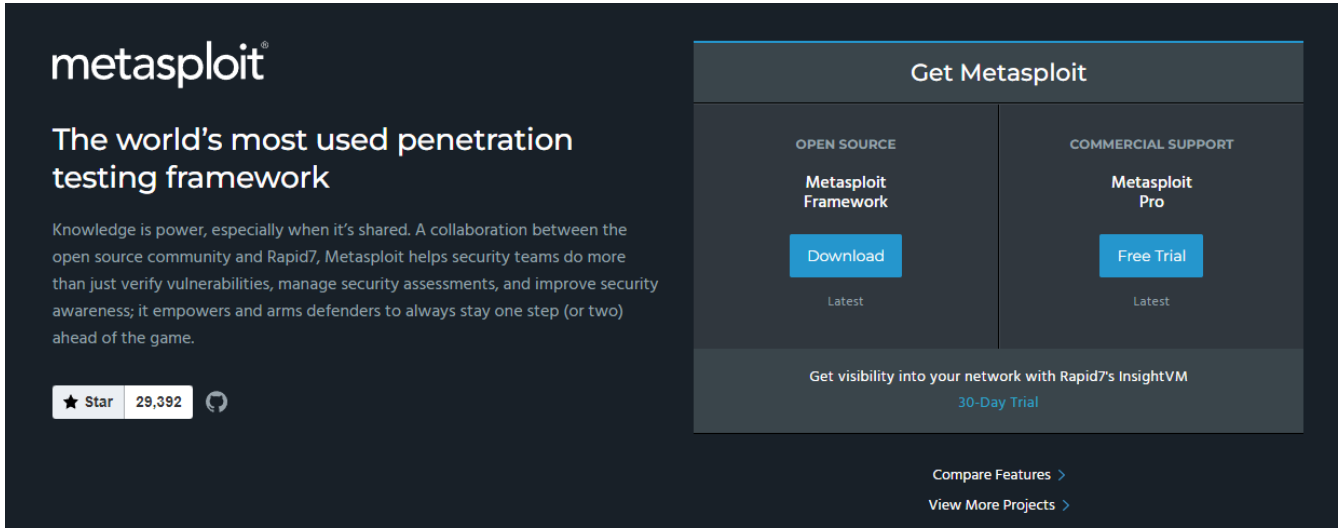
การเจาะเข้าระบบ (Exploitation) : MEDUSA

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



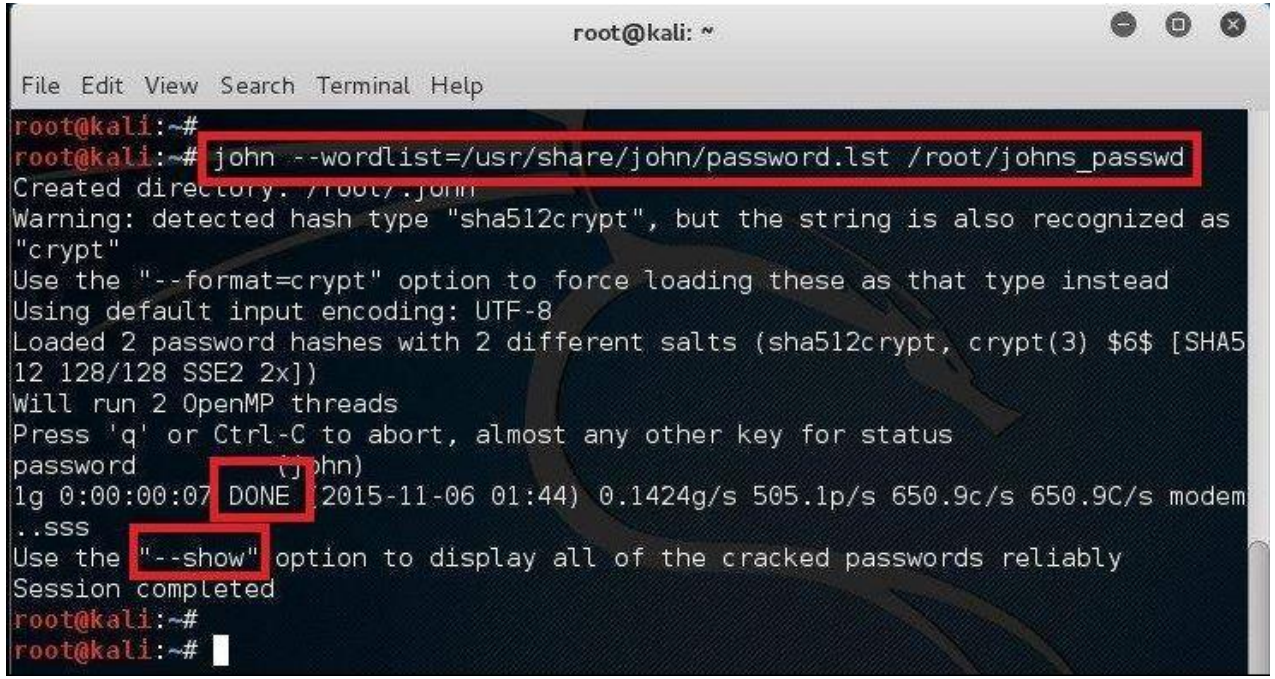
การเจาะเข้าระบบ (Exploitation) : Metasploit

เป็นเครื่องมือยอดนิยม เนื่องจากมีความยืนหยุ่น และประสิทธิภาพสูง จะทำการเลือกเป้าหายแล้วทำการโจมตีเพย์โหลด ซึ่ง เพย์โหลดในที่นี้หมายถึง การระบุฟังก์ชันหรือสิ่งที่ต้องการให้เป้าหมายเปลี่ยนแปลง เช่น การเพิ่มผู้ใช้งานให้กับเครื่องเป้าหมาย การเปิด Backdoor ทิ้งไว้ และการติดตั้ง Software ใหม่ลงบนเครื่อง



การเจาะเข้าระบบ (Exploitation) : John The Ripper

เป็นเครื่องมือตรวจสอบความปลอดภัยของรหัสผ่านแบบโอเพ่นซอร์สและการกู้คืนรหัสผ่าน สำหรับระบบปฏิบัติการหลายระบบ



การรักษาช่องทางเข้าระบบ (Maintaining Access)

เมื่อสามารถเข้าถึงระบบได้แล้ว ขั้นตอนถัดไปคือ การค้นหาและขโยมข้อมูลที่สำคัญออกมา และถ้าจุดประสงค์หลักไม่ใช่การทำลายระบบ ก็จะต้องทำการรักษาช่องทางการข้าถึงระบบเอาไว้ แต่ถ้าเป้าหมายหลัก คือการลำลายระบบ หรือทำให้ระบบใช้งานไม่ได้ ขั้นตอนนี้ก็จะไม่จำเป็นต้องดำเนินการ

ซึ่งขั้นตอนการสร้างช่องทางให้กลับขเมาในระบบได้อีกครั้ง โดยที่ผู้ดูแลระบบนั้นมีโอกาสน้อยที่จะเห็นช่องทางนี้ เราจะเรียกว่า **แบ็คดอร์ (Backdoor)**

แบ็คดอร์ (Backdoor)

Backdoor คือ ช่องทางที่โปรแกรมเมอร์หรือผู้พัฒนาระบบสร้างไว้ เพื่อให้สามารถเข้าถึงระบบหรือเครื่องคอมพิวเตอร์ได้โดยไม่ต้องผ่านกระบวนการตรวจสอบปกติที่อนุญาตให้เข้าถึงระบบได้ โดยทั่วไป Backdoor จะถูกสร้างขึ้นโดยการเขียนโปรแกรมซ่อนไว้ในระบบที่ผู้พัฒนาได้ออกแบบไว้

ซึ่งมีจุดประสงค์ เพื่อให้สามารถทดสอบระบบนั้นๆ ได้อย่างสะดวกรวดเร็ว แต่ก็อาจมีผู้ไม่หวังดี ที่ใช้ Backdoor เพื่อเข้าสู่ระบบและสร้างความเสียหายให้แก่ระบบนั้นด้วยเช่นกัน