Lab3

LAB.1

1.การสแกนหาโฮสต์ที่ออนไลน์ในเครือข่ายเดียวกันโดยใช้ ARP

A screen shot of a computer

Description automatically generated

2.การใช้ **UDP Ping** เพื่อทดสอบว่าโฮสต์ออนไลน์

A screen shot of a computer

Description automatically generated

3.การใช้ **ICMP Echo Request**เพื่อทดสอบว่าโฮสต์ออนไลน์อยู่หรือไม่

A screen shot of a computer

Description automatically generated

4.ส่วนอันนี้เหมือนข้อ3ครับแต่ทำการส่งไปหลายเครื่อง

A computer screen shot of a computer

Description automatically generated

5.การใช้ **ICMP Timestamp Request** เพื่อทดสอบว่าโฮสต์ออนไลน์อยู่หรือไม่

A screen shot of a computer

Description automatically generated

Lab.2

1.เป็นการscaanดูรายละเอือดของเป้าหมายโดยใช้UI

A screenshot of a computer

Description automatically generated

2.อันนี้เป็นการบอกว่ามรPort ไหนเปิดอยู่บ้างถ้าเปิดจะเป็นสีเขียว

A screenshot of a computer

Description automatically generated

3.ดูโครงสร้างของnetwordของเป้าหมาย

A screenshot of a computer

Description automatically generated

4.ดูรายละเอียดและสถานะของเป้าหมาย

A screenshot of a computer

Description automatically generated

5.อันนี้คือสิที่เราได้ทำการscanไปง่ายคือประวิติ

A screenshot of a computer

Description automatically generated

Lab.3

1.การสแกนแบบเจาะลึกที่ช่วยให้เราได้ข้อมูลเกี่ยวกับระบบเป้าหมายแบบละเอียด เช่น ระบบปฏิบัติการ,

เวอร์ชันซอฟต์แวร์ที่รันอยู่, การเชื่อมต่อในเครือข่าย รวมถึงพอร์ตที่เปิดอยู่

A computer screen shot of a computer program

Description automatically generated

A screenshot of a computer screen

Description automatically generated

2.เป็นการscanดูOSและรายละเอือดต่างๆของเครื่องเป้าหมาย

A computer screen shot of a computer program

Description automatically generated

3.เป็นการscript เพื่อใช้ในการดึงข้อมูลต่างๆจากเป้าหมายเช่น Os,Port เป็นต้น

A screen shot of a computer

Description automatically generated

Lab.4

1.เราทำการเข้ามาหน้าการตั้งค่าของFirewallของwindows

A screenshot of a computer

Description automatically generated

2.เป็นการscanเหมือนรูปแบบอื่นแต่จะมีความพิเศษต้องที่จะสามารถหลีกเลี่ยงการตรวจจับของFIrewall ได้

A computer screen shot of a computer

Description automatically generated

3.อันนี้จะเป็นการscan โดยใช้ wireshark

A screenshot of a computer

Description automatically generated

4.เป็นการscanผ่านfirewallโดยทำตัวในดูเหมือนทราฟฟิกปกติ

A computer screen shot of a computer

Description automatically generated

5.เป็นการscanที่เราจะเอาแค่TCP

A screenshot of a computer

Description automatically generated

6.เป็นการแบ่งแพ็กเก็ตให้เล็ก\*\*ในที่จะมีขนาด 8ไบต์\*\*เพื่อหลบเลี่ยงการตรวจจับ

A screen shot of a computer

Description automatically generated

7.ที่คุณกำลังวิเคราะห์แพ็กเก็ตเครือข่ายที่เกี่ยวข้องกับ **fragmentation** ซึ่งหมายถึงการแบ่งข้อมูลออกเป็นชิ้นเล็ก ๆ เพื่อส่งผ่านเครือข่าย

A screenshot of a computer

Description automatically generated

8.การสแกนเครือข่ายโดยใช้ IP address แบบสุ่มพื่อหลอกให้เหมือนมีหลายคนกำลังสแกนจากที่ต่างๆ กัน

A computer screen shot of a computer

Description automatically generated

9.ตรงนี้คือscanที่ได้จากข้อก่อนหน้า

A screenshot of a computer

Description automatically generated

10.คำสั่งนี้จะทำการสแกนเครือข่ายโดยไม่ทำการ ping ตรวจสอบ และปลอมแปลงที่อยู่ MAC

A computer screen shot of a computer

Description automatically generated

11.ตรงนี้คือscanที่ได้จากข้อก่อนหน้า

A screenshot of a computer

Description automatically generated

LAB.5

1.เป็นเครื่องมือการตรวจสอบความปลอดภัยและเจาะระบบ ซึ่งรวมถึงการค้นหาช่องโหว่

A screenshot of a computer

Description automatically generated

2.คำสั่งนี้จะทำการสแกนเครือข่ายเพื่อค้นหาพอร์ตที่เปิด, ระบุตัวระบบปฏิบัติการ, ตรวจสอบเวอร์ชันของบริการที่ทำงาน, และเก็บผลลัพธ์ในไฟล์ XML ชื่อ Test

A computer screen shot of a computer

Description automatically generated

3.การค้นหาหมายเลขหรือโมดูลที่เกี่ยวข้องกับการสแกนพอร์ตสามารถใช้เพื่อสแกนและค้นหาพอร์ตที่เปิดบนเครื่องหรือระบบที่เป็นเป้าหมาย

A screenshot of a computer

Description automatically generated

4.เราไปเพื่อเราจะไปset สิ่งเราจะทำการscan แล้วทำการrun

A screen shot of a computer program

Description automatically generated

5.แสดงรายละเอือดต่างๆของระบบ

A screenshot of a computer screen

Description automatically generated

6.เป้าดูว่ามีport เปิดอยู่บ้าง



A screenshot of a computer screen

Description automatically generated

7.เราไปเพื่อเราจะไปset สิ่งเราจะทำการscan แล้วทำการrun

A screen shot of a computer screen

Description automatically generated

Lab4

LAB.1

1. nbtstat -a ดูข้อมูลเกี่ยวกับชื่อของคอมพิวเตอร์ในเครือข่ายที่เราต้องการตรวจสอบ โดยจะบอกชื่อคอมพิวเตอร์และสถานะต่างๆ

A computer screen shot of a black screen

Description automatically generated

nbtstat -c ดูรายชื่อคอมพิวเตอร์ที่เครื่องของคุณเคยติดต่อด้วยในเครือข่าย โดยจะแสดงชื่อ NetBIOS และที่อยู่ IP ของเครื่องเหล่านั้น

A computer screen shot of white text

Description automatically generated

2. net use ใช้เพื่อเชื่อมต่อหรือยกเลิกการเชื่อมต่อกับไดรฟ์หรือโฟลเดอร์ที่แชร์ในเครือข่าย

A black screen with white text

Description automatically generated

LAB.2

1.ดึงข้อมูลจากอุปกรณ์ที่รองรับ SNMPโดยใช้โปรโตคอลเวอร์ชัน 1และรหัสผ่านคอมมูนิตี้ชื่อว่า D เพื่อดึงข้อมูลการตั้งค่าหรือสถานะของอุปกรณ์นั้น

A screenshot of a computer

Description automatically generated

อันนี้เหมือนกันต่างนิดหน่อยตรงที่เป็น v2 ที่จะมีการจัดการข้อมูลที่ดีกว่าแหละไวกว่าและมีความปลอดภัยมากกว่า

A screenshot of a computer

Description automatically generated

LAB.3

1.เป็นที่ใช้ Connect แต่อย่าลืมใส่userด้วยนะ

A screenshot of a computer

Description automatically generated

2.ที่นี้จะเห็นได้ว่าเราเข้ามาได้แล้ว

A screenshot of a computer

Description automatically generated

3.เราจะเข้าไปหาข้อมูลที่อยู่ไนเครื่อง

A screenshot of a computer

Description automatically generated

4.อันนี้คือเข้าไปแก้ไขไฟล์

A screenshot of a computer

Description automatically generated

เราสามารถเข้าไปแก้ไขได้

A screenshot of a computer program

Description automatically generated

LAB.4

1.เราจะทำการสร้างroles

A screenshot of a computer

Description automatically generated

2.เราจะทำการติดตั้งNSF เข้าไปในserver

A screenshot of a computer

Description automatically generated

3.การสแกนพอร์ตเฉพาะ (ในที่นี้คือพอร์ต **2049**) บนโฮสต์

A computer screen with white text

Description automatically generated

4.เข้าไปที่ /.SuperEnum แล้วทำการเพิ่มข้อมูล “192.168.179.136” ลงในไฟล์ Target.txt

A screenshot of a computer

Description automatically generated

5.แล้วทำการเรียกเครื่องมือชื่อ SuperEnum จากนั้นเอา Target.txt ใส่เข้าไปเพื่อในการ Test

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

6.เป็นการscan port ที่ใช้บริการผ่านRPC

A screenshot of a computer program

Description automatically generated

Lab.5

1. เช็กว่าโดเมนตั้งค่าไปใช้ Name Server ไหน

A computer screen shot of a computer code

Description automatically generated

2.จากข้อก่อนเราจะเห็นได้ว่ามันมี Name Server ที่เราสนใจ เราจะเอาเอามาทำการดูข้อมูลของDNS

A computer screen shot of a computer

Description automatically generated

3.เครื่องมือสำหรับตรวจสอบข้อมูล **DNS** แต่ใช้งานง่ายกว่า dig ในบางกรณี

A screenshot of a computer program

Description automatically generated

LAB.6

1.ใช้ตรวจสอบว่าในเซิร์ฟเวอร์อีเมลมีรายชื่อผู้ใช้งานอะไรอยู่บ้าง โดยจะส่งคำสั่งไปยังเซิร์ฟเวอร์

A screenshot of a computer screen

Description automatically generated

2.ใช้ตรวจสอบว่าเซิร์ฟเวอร์อีเมลเปิดให้ **“ส่งเมลต่อ”**หรือไม่ ซึ่งหมายความว่าเซิร์ฟเวอร์อนุญาตให้ใครก็ได้ส่งอีเมลผ่านมัน โดยไม่ต้องยืนยันตัวตน

A screen shot of a computer

Description automatically generated

3.ใช้ตรวจสอบว่าเซิร์ฟเวอร์ SMTP รองรับคำสั่งอะไรบ้างเช่น HELO, EHLO, VRFY, EXPN เป็นต้น

A computer screen with white text

Description automatically generated

LAB.7

1.lab นี้เราจะทำการscan server นะครับ

A screenshot of a computer program

Description automatically generated

2.เราจะทำการเอาIPของเครื่องเป้าหมายไปใส่

A screenshot of a computer program

Description automatically generated

3.ที่เราจะทำการใส่ Domain & Password ของเป้าหมาย

A screenshot of a login

Description automatically generated

4.เราจะได้เห็นได้ว่าใน Domain แสดงรายละเอืยดที่อยู่ข้างใน

A screenshot of a computer

Description automatically generated

5.เวลาเราทำการเอาเมาไปชี้จะแสดงรายละเอืยดของipเครื่องนั้น

A white paper with black text

Description automatically generated

Lab5

LAB.1

1.เราจะทำการเข้าไปที่เว็ป <https://cwe.mite.org/> เพื่อจะเค้าไปดูของข้อมูลCWR-284 \*\*เป็นเว็ปที่รวมข้อมูลที่จุดอ่อนในซอฟต์แวร์\*\*

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

2.อันนี้เป็นข้อมูลที่อยู่ในไฟล์ cwe-284

A screenshot of a computer

Description automatically generated

3.เราจะเข้าไปดู cwe top 25 ในปี 2024

A screenshot of a computer program

Description automatically generated

4.อันนี้เราจะเห็นข้อมูลที่เป็นจุดอ่อนของ

A screenshot of a computer program

Description automatically generated

Lab.2

\*\*ก่อนทำนะครับต้องทำการติดตั้งก่อนนะครับ Docker \*\*

<https://www.kali.org/docs/containers/installing-docker-on-kali/>

<https://www.geeksforgeeks.org/how-to-install-docker-in-kali-linux/>

เลือกสักอันนะครับ แต่ถ้ารีบๆก็ sudo apt update -y && sudo apt insytall docker.io sudo systemctl enable docker --now sudo usermod -aG docker $USER logout docker pull mikesplain/openvas จากนี้น่าจะทำต่อได้แล้วนะครับ

\*\*\*ในกรณีที่ไม่สามารถlog in ได้ยังมีอีก1วิธีที่ผมใช้นะครับ

<https://infotechys.com/installing-openvas-on-kali-linux/>

ทำตามแบบใจเย็นนะครับเพราะมันใช้เวลาแต่ถ้าเบื่อก็อ่านข้อมูลข้างในแล้วทำความเข้าใจด้วยนะครับผม\*\*\*

1.ให้เรานำ 127.0.0.1:9392 ไปค้นหาดูนะครับจะได้หน้านี้มาแล้วทำการใส่รห้สตามนี้\*\*\*อันนี้ผมมีการเปลื่ยนรหัสด้วยนะครับ\*\*\* admin/admin

A screenshot of a sign in

Description automatically generated

2.กดไปที่ scan -->> Tasks

A screenshot of a computer

Description automatically generated

3.ให้กดไปตรงที่อยู่ในกรอบสีแดงจากให้คลิก Tack Wizard

A screenshot of a computer

Description automatically generated

4.แล้วทำการใส่ไปIP ของเครื่องเป้าหมาย

A screenshot of a computer

Description automatically generated

5.จะได้หน้าแบบนี้มา

A screenshot of a computer

Description automatically generated

ส่วนเหลือที่จะเป็นการแสดงรายละเอียดต่างๆจำพวก Host QoD เป็นต้นๆ \*\*\*ไม่มีรูปนะครับเพราะมันไฟล์มันเสียแล้ว\*\*\*