Chapter 1 - Basic Cybersecurity Knowledge

Part 1 Basic Cyber Security Knowledge

การรักษาความปลอดภัยของข้อมูล

1. Confidential (ข้อมูลเป็นความลับ)
   การกำหนดให้ผู้ที่ได้รับอนุญาตเท่านั้นที่เข้าถึงข้อมูลได้
2. Integrity (ข้อมูลมีความถูกต้องสมบูรณ์)
   ข้อมูลคงอยู่ในสภาพเดิม ไม่ถูกแก้ไข เปลี่ยนแปลง หรือทำลายระหว่างส่งข้อมูล
   หากเกิดการแก้ไข ทำให้ข้อมูลนั้นไม่มีความน่าเชื่อถือและนำไปใช้ต่อไม่ได้
3. Availability (ข้อมูลพร้อมใช้งาน)
   ระบบพร้อมใช้งานอยู่เสมอ สามารถนำข้อมูลมาใช้งานได้ในเวลาที่ควรใช้

การป้องกันการรักษาความปลอดภัยของข้อมูล

1. Prevention
   การป้องกันข้อมูล จากการถูกทำลายหรือเปลี่ยนแปลง รวมทั้งการเข้าถึงข้อมูลอย่างไม่ถูกต้อง
2. Detection
   การตรวจจับความผิดปกติที่เกิดขึ้นกับระบบ ซึ่งอาจเป็นการโจมตีที่ไม่เคยเจอมาก่อน
   เมื่อตรวจพบการโจมตีต้องระบุได้ว่าสิ่งใดถูกโจมตีและโจมตีมาจากทางไหน
3. Response
   การรับมือหรือแก้ไขปัญหากับการโจมตีหรือการสูญเสีย

ประเภทการโจมตีของ Exploit

Exploit คือ การอาศัยจุดได้เปรียบจากช่องโหว่ของระบบ เพื่อสร้างความเสียหายให้กับเป้าหมาย
แบ่งการโจมตีของ Exploit เป็น 2 ประเภท ได้แก่

1. Remote exploit
   การโจมตีที่ไม่จำเป็นต้องเข้าถึงหน้าเครื่อง โดยการส่ง code ผ่านเครือข่ายของเหยื่อ
2. Local exploit
   การโจมตีที่จำเป็นต้องเข้าถึงหน้าเครื่อง เพื่อเพิ่มระดับการเข้าถึงของ Hacker ที่มีการใช้สิทธิ์ที่ไม่ควรใช้ได้

เป้าหมายการโจมตีของ Hacker

1. Access Attack
   การเข้าถึงข้อมูล แล้วนำมาเผยแพร่ทำให้เกิดความเสียหายต่อบุคคลหรือองค์กรนั้น ทำให้เสียคุณสมบัติของ Confidentiality
2. Modification And Repudiation
   การทำลาย แก้ไข เพิ่มเนื้อหา หรือทำให้ข้อมูลเกิดการบิดเบือนหรือไม่มีความน่าเชื่อถือ ไม่สามารถนำข้อมูลไปใช้ต่อได้ ทำให้เสียคุณสมบัติของ Integrity
3. Denial Of Service (DoS) And Distributed Denial Of Service(DDoS)
   การโจมตีเพื่อทำให้ไม่สามารถใช้งานระบบได้ ทำให้เสียคุณสมบัติของ Availability

Part 2 Kali Linux

Kali Linux คืออะไร ?

ระบบปฏิบัติการ Linux ที่ผู้พัฒนาสามารถดัดแปลง แก้ไข และเปิดเผยข้อมูลได้ แต่ไม่สามารถนำไปขายต่อได้ ซึ่งได้รับความนิยมมากที่สุดในการทดสอบเจาะระบบ และถูกสร้างขึ้นมาสำหรับ cybersecurity ทั้งนี้ Kali Linux เป็นอีกหนึ่ง OS ที่รับรองในการติดตั้งได้หลาย environment เช่น VirtualBox, VMWare, Parallel Desktop

Part 3 Malware

Malware คืออะไร ?

มาจากคำว่า Malicious Software คือ โปรแกรมใด ๆ ที่มุ่งร้ายต่อระบบ ไม่ว่าจะเป็นรูปแบบใดก็ตาม เช่น trojan, backdoor, virus, worm, ransomware

โดย trojan และ backdoor เป็นที่ Hacker เอาไว้ทำทางเข้าสู่ระบบเป้าหมาย ซึ่งหลอกให้เป้าหมายติดตั้ง trojan หรือ backdoor บนเครื่องของเป้าหมาย

ทั้งนี้ virus และ worm ใช้เพื่อทำลายระบบและใช้เพื่อเป็น trojan และ backdoor ภายในเครือข่ายได้

Backdoor คืออะไร ?

เป็นโปรแกรมที่ Hacker ติดตั้งไว้บนเครื่องเหยื่อ เพื่อให้ Hacker เข้าถึงเครื่องเหยื่อเมื่อไหร่ก็ได้ โดยเป้าหมายของ backdoor คือ การลบหลักฐานการเข้าถึงเครื่อง การเพิ่ม service เข้าไปในระบบ เพื่อให้เมื่อเปิดเครื่องใหม่ backdoor ก็จะทำงานขึ้นมาใหม่ทันที

Trojan คืออะไร ?

เป็นโปรแกรมแปลกปลอมที่เข้ามาในเครื่อง โดยจะ download โปรแกรมหรือซอฟต์แวร์ตัวอื่นมาด้วย เมื่อติดตั้งลงเครื่องเสร็จ trojan ก็จะขโมยข้อมูลหรือลบข้อมูลออกจากเครื่องหรือทำให้เครื่องเหยื่อช้าลง

วิธีป้องกัน Trojan

- เข้าเว็บไซต์ที่น่าเชื่อถือและการไม่ติดตั้งซอฟต์แวร์จากแหล่งที่มาที่ไม่ใช่ผู้ผลิตจริง ๆ
- การอัพเดต Antivirus อยู่ตลอดเวลา
- การอัพเดตระบบปฏิบัติการ

Viruses และ Worms คืออะไร ?

ใช้เพื่อติดกับระบบและแก้ไขระบบให้ Hacker สามารถเข้าถึงเครื่องได้ง่าย ทั้งนี้ virus และ worm มีการนำ trojan และ backdoor ผูกไปด้วยเพื่อฝังทางเข้าให้กับ Hacker แล้วค่อยกระจายต่อไป โดย worm กระจายตัวจากระบบสู่ระบบแบบอัตโนมัติ แต่ virus ใช้โปรแกรมอื่นในการแพร่กระจายตัว

APT คืออะไร ?

ปฏิบัติการที่มีเป้าหมายชัดเจนและโจมตีอย่างซับซ้อน มักเริ่มจากการใช้ malware ซึ่งโจมตีด้วย UNKOWN Vulnerability(0day) และ KNOWN Vulnerability(UNKNOWN Attack) คือ รู้ช่องโหว่แต่ไม่รู้ว่าโจมตีแนวไหน

Ransomware คืออะไร ?

เป็น malware ที่เข้าไปยังเครื่องเป้าหมาย จากนั้นเข้ารหัสเครื่องเป้าหมายเพื่อให้เหยื่อที่เป็นเจ้าของเครื่องเปิดเครื่องหรือดูข้อมูลภายในเครื่องไม่ได้

Part 4 Backup Data

Backup

คือ การคัดลอกหรือทำสำเนาข้อมูลต้นฉบับที่เป็นส่วนสำคัญของระบบ เก็บไว้ตามระยะเวลาต่าง ๆ โดยส่วนใหญ่มักเก็บไว้ใน tape เพราะรองรับข้อมูลได้จำนวนมาก

ประโยชน์ของการ backup

- นำข้อมูลเก่ากลับมาใช้งานเมื่อเกิดเหตุขัดข้องใด ๆ
- เป็นแผนสำรองกรณีที่ข้อมูลผิดพลาดขณะกำลัง upgrade ระบบ
- ป้องกันการเกิดข้อมูลสูญหายที่เกิดจากภัยทางธรรรมชาติ หรือเหตุการณ์ไม่คาดคิด
- ใช้เพื่อเปรียบเทียบข้อมูลระหว่างอดีตและปัจจุบัน

ประเภทของการ Backup

1. Full Backup หรือ Normal Backup
    - backup ข้อมูลที่พร้อมใช้งานได้ด้วยตัวเองทันที ไม่จำเป็นต้องพึ่ง backup ไฟล์อื่น
    - ข้อดี คือ โอกาสผิดพลาดน้อยและการใช้งาน restore ก็สามารถทำได้ทันที
    - ข้อเสีย คือ ใช้เวลา backup นาน เพราะ backup ข้อมูลทั้งหมด และไฟล์มีขนาดใหญ่มาก

2. Incremental Backup
    - backup เฉพาะข้อมูลที่แตกต่างจากข้อมูล backup เดิม (ไม่ได้ backup ทั้งหมด)
    - ข้อดี คือ ใช้เวลาน้อยกว่า Full Backup
    - ข้อเสีย คือ ใช้เวลาอย่างมากในการ restore ข้อมูล
3. Differential Backup
    - backup เฉพาะข้อมูลที่เพิ่มเข้าไปจาก Full Backup
    - ข้อดี คือ ใช้เวลา restore น้อยกว่า Incremental Backup
    - ข้อเสีย คือ ใช้พื้นที่มากกว่า Incremental Backup
4. Synthetic Full Backup
    - backup ตาม Incremental Backup และมีรวม backup เก่า ๆ ในช่วงระยะเวลาหนึ่ง
    - ข้อดี คือ มีความสมบูรณ์ในการใช้งานมากกว่า Incremental Backup
    - ข้อเสีย คือ ใช้พื้นที่จัดเก็บมหาศาล (แต่น้อยกว่า Full Backup)

Part 5 DR Site

DR Site คืออะไร ?

Disaster Recovery Site เป็นสถานที่สำหรับ backup ไฟล์และ service หลักขององค์กร ที่ทำให้องค์กรบริการธุรกิจต่อไปได้ เมื่อสำนักงานใหญ่เกิดความเสียหายจากภัยธรรมชาติหรือจากมนุษย์ ดังนั้นการจะสร้าง DR Site นั้นจำเป็นต้องใช้กำลังเงินจำนวนมหาศาล ซึ่งขึ้นอยู่กับประเภทของ DR Site ที่องค์กรเลือก

ประเภทของ DR Site

1. Hot site
    - ข้อมูลหรือระบบใด ๆ เหมือนกับระบบหลักที่ใช้งานในสำนักงานใหญ่
    - ข้อดี คือ downtime น้อยสุด
    - ข้อเสีย คือ ใช้เงินมากสุด

2. Cold site เป็นระบบที่ใช้เงินน้อยสุด แต่ downtime มีเยอะมากที่สุด
    - สำรองระบบเพียงแค่ HVAC (Heating, Ventilation, Air Conditioning), network และระบบไฟฟ้า รวมถึง backup data ไว้เพียงเล็กน้อยเท่านั้น
    - ข้อดี คือ ใช้เงินน้อยสุด
    - ข้อเสีย คือ downtime มากสุด
3. Warm site
    - site ที่อยู่กึ่งกลางระหว่าง Hot และ Cold โดย backup ข้อมูลเป็นระยะและระบบพร้อมระดับหนึ่ง
    - ข้อดี คือ ใช้งานได้เร็วกว่า Cold site
    - ข้อเสีย คือ downtime มากกว่า Hot site

Part 6 Risk

<u>Risk คืออะไร ?</u>

ความเสี่ยง ซึ่งคำนวณมาจาก มูลค่าความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินขององค์กร (Lots of asset) x ความเป็นไปได้ที่จะเกิดขึ้น (likelihood หรือ probability) ทั้งนี้ Lots of asset นั้นไม่ได้มองเป็นแค่มูลค่าเงิน แต่มองในมุมมองของชื่อเสียงด้วย

<u>Risk Assessment (การประเมินความเสี่ยง)</u>

ประกอบไปด้วย 4 ส่วน คือ

1. Identification
   เป็นการกำหนดค่าสินทรัพย์ (asset) แต่ละตัวว่ามีผลกระทบต่อธุรกิจมากน้อยแค่ไหน
2. Assessment
   เป็นการคำนวณค่า risk ของแต่ละ asset ตาม Lots และ Likelihood
3. Prioritize
   เป็นการนำความเสี่ยงทั้งหมด มาจัดอันดับว่า ควรแก้ไขความเสี่ยงใดก่อนหลัง
   โดยคำนึงถึงเวลาและทรัพยากรที่ใช้แก้ไขความเสี่ยงเป็นหลัก
4. Treatments
   เป็นการลดความเสี่ยง โดยใช้วิธีการหรืออุปกรณ์ที่ช่วยควบคุมความปลอดภัยของ Risk แต่ละ asset

<u>Risk Treatments (การกำจัดความเสี่ยง)</u>

มีวิธีการรักษา ดังต่อไปนี้

1. Risk Retention (Risk Acceptance)
   ใช้งาน asset, process จะทำเมื่อไม่คุ้มค่าต่อการจัดการควบคุมหรือป้องกันความเสี่ยง
2. Risk reduction
   การปรับปรุงที่ลดอัตราสูญเสียหรือการเกิดโอกาสที่ทำให้เกิด risk ในระดับที่องค์กรยอมรับได้
3. Risk Sharing (Risk Transfer)
   การกระจายความเสี่ยงหรือโอนความเสี่ยงไปให้กับผู้อื่นแบ่งความรับผิดชอบ
4. Risk avoidance
   การเลิกใช้งาน asset หรือ process เพื่อไม่ให้เกิดความเสี่ยงกับ asset

Part 7 Policies, Standards, และ Procedures

Security Policies คือ ข้อตกลงโดยรวมขององค์กร เพื่อรักษาความปลอดภัย

Security Policies คือ มาตรฐานการดำเนินงานให้เป็นไปตาม Policies เพื่อให้บริหารธุรกิจต่อได้

Procedures คือ ขั้นตอนการดำเนินงานตาม standard ที่กำหนด ให้ใกล้เคียงกับการทำงานจริงมากที่สุด

Part 8 Logging

Log คือ การบันทึกการทำงานหรือเหตุการณ์ที่เกิดขึ้น ทั้งจากฝั่ง client ฝั่ง server และ application

Syslog Protocol

คือ protocol ที่ถูกใช้ใน Unix/Linux server และอุปกรณ์ network แล้วเป็น protocol ที่ใช้สำหรับเก็บภายในเครื่องและส่ง log ออกมายังภายนอก โดยส่ง log ออกมาจากเครื่อง เพื่อส่งไปยังส่วนกลาง มีผลดีดังต่อไปนี้

1. รวมศูนย์การวิเคราะห์ log ไว้ที่เดียว ทำให้เห็นภาพรวมเหตุการณ์ของทั้งองค์กรได้ง่ายขึ้น
2. หาก server ถูกโจมตีก็ไม่ต้องกังวลว่า log จะถูกลบ เพราะได้สำรองไว้ที่ส่วนกลางแล้ว
3. การเก็บข้อมูลไว้ที่ส่วนกลาง ทำให้ลบ log เครื่องต้นทางได้เลย ทำให้ประหยัดพื้นที่ของเครื่องแต่ละเครื่อง

*โดยปกติ Log ของ Linux จะถูกเก็บไว้ที่ /var/log/

Windows Log

Windows Log แตกต่างจาก Unix/Linux โดย log message ถูกสร้างและส่งไปยัง event subsystem โดย Windows เก็บ event ในลักษณะของ evt, evtx file ข้อดี คือ filter ได้โดย Windows Log จะแบ่งออกเป็น

1. System log
   คือ log ประเภท program ที่ถูกติดตั้งในเครื่อง, OS log
2. Security log
   คือ log ที่เกี่ยวกับความปลอดภัยของ OS
3. Application log
   คือ log ประเภท Windows system component
4. Setup log
   คือ log ประเภทการ update หรือติดตั้ง Application เพิ่มเติม
5. Forward Events
   คือ log จาก server อื่นที่ถูกส่งมายัง server แต่ละตัวมี event ID เป็นตัวกำกับและบอกประเภทของ Log ซึ่งการ search log โดยกำหนด event id ทำให้หา log ได้สะดวกมากขึ้น

Syslog

Syslog-ng คือ Open Source ที่ถูกสร้างมาเพื่อจัดการ syslog protocol ใน Unix/Linux โดยนำ syslogd มาปรับแต่งเพิ่มเติม

Part 9 Defense in-Depth และ Defense in Breadth

Defense in-Depth

เน้นป้องกันในลักษณะ Network Layer โดยออกแบบระบบ network ให้มีการป้องกันในหลายขั้น โดยป้องกันตาม traffic ที่เข้ามา เมื่อผู้โจมตีผ่านด่านที่หนึ่งได้ ก็มีด่านสองมากรองและป้องกันต่อ ทำให้ผู้โจมตีทำงานได้ยาก

Defense in Breadth

เน้นป้องกันในลักษณะ Application Layer โดยเครื่องมือที่ใช้ป้องกันจะเน้นไปตามภัยคุกคามของ application นั้น แล้วยังมีการส่ง log ไปยังส่วนกลางเพื่อคอยเฝ้าระวังอีกด้วย

Part 10 Security Models

Security Models

ถูกใช้เพื่อควบคุมการเข้าถึง security model โดยกำหนดว่าใครสามารถกระทำใด ๆ กับ data ได้บ้าง

Bell-LaPadula Model

เน้นที่ความลับข้อมูลที่ผู้ใช้งานสามารถสร้าง content ได้เฉพาะที่ security level ของตัวเองหรือเหนือจากตัวเอง

Biba Model

เน้นไปที่ความถูกต้องของข้อมูล ผู้ใช้ไม่สามารถเขียนไปในระดับ integrity level ที่สูงกว่าของตัวเองได้ แต่สามารถอ่านใน integrity level ที่เท่ากับหรือมากกว่าตัวเองได้

Clark–Wilson model

คล้ายกับ Biba Model โดยเน้นที่ความถูกต้องของข้อมูล แต่กำหนดการทำงานที่แตกต่างอย่างชัดเจน เน้นไปในเรื่อง Separation of Duty

Chinese Wall Model

เน้นไม่ให้เกิดความขัดแย้งด้านผลประโยชน์

Part 11 Network Security Device

Network Security Device

อุปกรณ์ security ต่าง ๆ ที่ถูกสร้างขึ้นมาเพื่อป้องกันการโจมตีที่อาจเกิดขึ้นกับระบบได้ ได้แก่

1. Intrusion Detection System (IDS)
   เป็นเครื่องมือตรวจสอบพฤติกรรมที่ผิดปกติ
2. Intrusion Prevention System (IPS)
   เป็นเครื่องมือตรวจพฤติกรรมที่ผิดปกติและป้องกันการโจมตี
3. Firewall
   เป็นเครื่องมือที่ป้องกันการเชื่อมต่อในลักษณะต่าง ๆ
4. Honeypot
   เป็นเครื่องมือที่ล่อให้ผู้โจมตีคิดว่าอยู่ในเครื่องจริง จากนั้นเก็บข้อมูลการโจมตี
5. Security Information and Event Management (SIEM)
   เป็นเครื่องมือที่ค้นหาพฤติกรรมผิดปกติจาก log

Part 12 Client-side exploitation & defending

Client-Side Exploitation

การโจมตีที่ฝั่ง client โดยหลอกลวงให้เข้าใช้งานเว็บไซด์แล้วให้ผู้ใช้งานกดเรียกใช้งาน วิธีการป้องกันการโจมตีมีดังต่อไปนี้

1. ไม่เปิด file หรือ link ของคนแปลกหน้าหรือผู้ที่ไม่น่าเชื่อถือ
2. update application ทั้งหมดให้เป็น version ล่าสุดอยู่เสมอ
3. config application ให้มีความปลอดภัย

ในส่วนเครื่องมือสำหรับป้องกัน มีดังต่อไปนี้

1. Antivirus
   ป้องกัน malware ในลักษณะ blacklist
2. Endpoint Protection Platform
   ป้องกัน malware ในลักษณะ whitelist
3. Endpoint Detection Platform
   ตรวจจับพฤติกรรม เพื่อวิเคราะห์พฤติกรรมที่ผิดปกติ

Chapter 2 - Basic Network

Part 1 IPv4

IPv4

IP (Internet Protocol Address) มีหน้าที่เป็นหมายเลขที่ใช้ในระบบเครือข่าย เป็นหมายเลขประจำเครื่องคอมพิวเตอร์ เพื่อให้อุปกรณ์บนระบบเครือข่ายรู้จักกัน สื่อสารกันได้ และส่งข้อมูลให้กับเครื่องได้อย่างถูกต้อง โดยปกติ IP จะเป็น IPv4 โดยเป็นหมายเลขที่มีทั้งหมด 32 บิต แบ่งออกเป็น Class ดังนี้

- Class A คือ 1.0.0.1 - 127.255.255.254
- Class B คือ 128.0.0.1 - 191.255.255.254
- Class C คือ 192.0.1.1 - 223.255.254.254
- Class D คือ 224.0.0.0 - 239.255.255.255 ใช้สำหรับงาน multicast
- Class E คือ 240.0.0.0 - 255.255.255.254 ถูกสำรองไว้ ยังไม่มีการใช้งาน

Part 2 OSI Model

OSI Model (Open Systems Interconnection Model)

คือ รูปแบบการสื่อสารแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์ต่าง ๆ แบ่งการทำงานออกเป็น 7 Layers (Layer 1 - 3: ติดต่อผ่าน Hardware, Layer 4 - 7: ติดต่อผ่าน Software) โดย Layer ทั้ง 7 มีดังต่อไปนี้

1. Physical Layer
   - รับส่งข้อมูลผ่านสื่อกลาง
   - ข้อมูลใน layer: Bits
2. Data Link Layer
   - รับส่งข้อมูลระหว่าง network device
   - ข้อมูลใน layer: Frame
3. Network Layer
   - รับส่งข้อมูลระหว่าง computer กับ network device
   - ข้อมูลใน layer: Packet
4. Transport Layer
   - ควบคุมการรับส่งข้อมูลระหว่าง Client และ Server
   - ข้อมูลใน layer: Segment
5. Session Layer
   - sync การใช้งานของ session แต่ละ connection
6. Presentation Layer
   - แปลงค่าข้อมูลให้เป็นรหัสต่าง ๆ
7. Application Layer
   - แสดงค่าข้อมูลให้กับ user ได้เห็น

Part 3 Network Topology

Topology

คือ การเชื่อมต่อ network เข้าด้วยกัน

BYOD

Bring Your Own Device (BYOD) เป็นการนำอุปกรณ์ส่วนตัวใด ๆ นำมาใช้ในองค์กร หากองค์กรไม่แยกการใช้งานระหว่างเครื่องของภายในบริษัทกับเครื่องส่วนตัวอาจเป็นจุดอ่อนขององค์กรได้ ดังนั้น BYOD ในทุกองค์กรควรมีแยกวง network สำหรับการใช้งานโดยทั่วไป กับ network ภายในองค์กรซึ่งการเข้าถึงเครือข่าย ควรถูกเข้าถึงได้โดยเครื่องที่อนุญาต เพื่อให้ไม่เกิดปัญหาในการควบคุมการเข้าถึง network ขององค์กร เพื่อลดความเสี่ยงที่อาจจะเกิดจากการใช้งาน BYOD

Part 4 IPv6

IPv6 คืออะไร ?

การติดต่อสื่อสารระหว่างเครื่องแต่ละเครื่องในอินเตอร์เน็ต โดยติดต่อผ่าน IP Address ทั้งนี้ IP Address ที่ใช้อยู่ คือ IPv4

ความแตกต่างระหว่าง IPv4 และ IPv6

- มีการเปลี่ยนรูปแบบ Header ใหม่
- มี security จากภายใน packet
- Quality of Service(QoS)
- การจัดการ IP แบบอัตโนมัติ
- ส่วนเสริมของ Header แบบใหม่
- IPSec

Part 5 การเชื่อมต่อและใช้งาน IPv6 Network

<u>การเชื่อมต่อระหว่าง IPv4 กับ IPv6</u>

ปัจจุบัน IPv6 เริ่มมาใช้งานแทนหรือร่วมกับ IPv4 แล้ว การทำงานของ Router IPv6 ทำงานร่วมกับ Router IPv4 ได้หลายวิธีดังนี้

1. Dual Stacks
   ส่งข้อมูลการทำงานตาม Application ที่ใช้งาน
   ถ้า Application นั้นใช้ข้อมูลเป็น IPv4: ใช้งาน IPv4 Stack ส่งข้อมูล
   ถ้า Application นั้นใช้ข้อมูลที่เป็น IPv6: ใช้งาน IPv6 Stack ส่งข้อมูล
   ซึ่งการทำงานของ Dual Stacks ง่ายแต่ก็ไม่สามารถทำบ่อย โดยใช้ได้กับ Router ที่รองรับทั้ง IPv4 และ IPv6
2. Tunneling
   เมื่อรับ Packet จาก Client (IPv6) ก็เพิ่ม Header ของ IPv4 เข้าที่ด้านบนของ IPv6 packet จากนั้นส่งต่อไปยัง Router (IPv4) จากนั้นส่งต่อ packet ในรูปแบบ IPv4 ไปยัง Router (IPv4)
   เมื่อถึง Router ปลายทาง (IPv6) แล้ว ก็ถอด Header ของ IPv4 ออก ให้อยู่ในลักษณะของ IPv6 packet อีกครั้งหนึ่ง จากนั้น IPv6 Router จะส่ง Packet ไปยังเครื่องเป้าหมายอีกครั้งหนึ่ง
3. Translation
   Translation ทำได้ 2 แบบ
   - แบบที่ 1 ทำที่ endpoint:
     ใช้ host เพิ่ม translation function เข้าไปใน Protocol Stack อย่าง Network Layer, TCP Layer หรือ Socket Layer อย่างใดอย่างหนึ่ง
   - แบบที่ 2 ทำที่ Network Device:
     ใช้ Router, Gateway ที่ต้องมีเครื่องมือแปลง IPv6 เป็น IPv4 และจัดการ IPv6 ให้เป็น IPv4

   โดย Network Device ดังกล่าวต้องอยู่ส่วนปลายของ network ที่จะต่อไปที่ network อื่น เพื่อปรับเปลี่ยน IP ให้เป็นไปดังที่เชื่อมต่อ

Part 6 เครื่องมือสำหรับการโจมตี IPv6

IPv6 กับ IPv4 มีความแตกต่างกัน ทำให้การเก็บข้อมูลหรือโจมตีมีการเปลี่ยนแปลง จึงมีเครื่องมือสำหรับการโจมตี IPv6 มีดังนี้

1. Nmap
   เป็นเครื่องมือที่ใช้งานกับ IPv6 ตั้งแต่ version 6 เป็นต้นไป
2. Metasploit
   ยืดเครื่องด้วย Metasploit Framework แล้วทำงานได้หลากหลาย ทั้งนี้ยังมี module ที่ใช้สำหรับ IPv6
3. THC-IPv6
   เป็นชุดเครื่องมือที่ใช้สำหรับ IPv6 โดยเฉพาะ

Part 7 Covert Channel

การใช้ Covert Channel ในการติดต่อสื่อสารระหว่างเครื่องเหยื่อและผู้โจมตี ซึ่งทำให้ไม่สามารถตรวจจับหรือหลบเลี่ยงการตรวจจับการสื่อสารนั้นได้ ซึ่งเป็นที่นิยมในหมู่ Hacker ในปัจจุบัน

Covert Channel คืออะไร ?

คือ การใช้ช่องทางปกติมาใช้ติดต่อในรูปแบบอื่น หรือ การติดต่อสื่อสารระหว่างเครื่องเหยื่อและผู้โจมตี โดย covert channel ใช้เพื่อหลบเลี่ยงการตรวจจับ network filtering เช่น Firewall ซึ่งไม่ใช่การเข้ารหัสข้อมูลแต่ทุกข้อมูลมักถูกแฝงไปกับ payload ของการใช้งาน protocol ทั่วไป

Part 8 VPN คืออะไร

VPN คืออะไร ?

VPN(Virtual Private Network) เป็นการขยาย network ภายในข้ามการใช้งานเครือข่ายภายนอก ทำให้ส่งข้อมูลใดจาก public network ไปยังเครือข่ายภายในได้

คุณสมบัติของ VPN

1. VPN เป็นการใช้งาน network ที่เข้ารหัสข้อมูลทั้งหมด
2. VPN ช่วยเปลี่ยน IP ได้
3. VPN มีเพื่อความปลอดภัยและการป้องกันความเป็นส่วนตัว

VPN ทำงานอย่างไร ?

VPN เชื่อมต่อกับผู้ใช้งาน (client) ผ่านระบบ internet จากนั้น client ใช้ VPN เป็น gateway ไปสู่แหล่งข้อมูลรวมถึงข้อมูลภายในองค์กรที่ VPN Server นั้น

Part 9 Denial of Service (DoS) และ Distributed Denial of Service (DDoS)

Denial of Service

การโจมตีในลักษณะ Denial of Service (DoS) เป็นการโจมตีที่ทำให้เสียคุณสมบัติ Available ที่เป็นหลักของ Cybersecurity ทำให้ระบบเป้าหมายไม่สามารถใช้งานได้

DoS vs. DDoS

- DoS คือ การโจมตีที่มีแหล่งที่มาแค่แหล่งเดียว
- DDoS คือ การโจมตีจากอุปกรณ์จำนวนมาก และมีแหล่งที่มาจากหลายที่

Chapter 3 - Wireless Network

Part 1 Wireless Network - ความรู้พื้นฐานและ WEP

พื้นฐานของ Wireless Network

Wireless LAN ถูกเริ่มพัฒนาและทดลองใช้งานในปี 1980 โดยใช้ความถี่ 900 MHz ต่อมาในปี 1992 ทาง Institute of Electrical and Electronics Engineers (IEEE) ได้แบ่งการใช้งาน Wireless LAN ออกมา 3 กลุ่ม ได้แก่ กลุ่มที่ใช้ความถี่ 2.4 GHz, กลุ่มที่ใช้ความถี่ 5 GHz และกลุ่มที่ใช้ความถี่ย่านอินฟราเรด (infrared)

รูปแบบการเข้ารหัส

Wireless LAN ถูกดักจับข้อมูลได้อย่างง่ายดาย จึงเป็นทางออกที่ดีที่สุดในการป้องกันการถูกดักจับข้อมูลและป้องกันการเข้าใช้งานระบบ Wireless LAN ซึ่งเข้ารหัสตามมาตรฐานดังนี้คือ WEP, WPA และ WPA-2

Wired Equivalent Privacy (WEP)

คือ เข้ารหัสโดยใช้ Algorithm RC4 ที่เข้ารหัสแบบ Symmetric Key Stream

Part 2 WPA และ WPA2

WPA

การเข้ารหัส WPA ถูกพัฒนาเพื่อแก้ไขจุดอ่อนของ WEP โดยมีความปลอดภัยกว่า WEP

WPA2

WPA2 มีพื้นฐานมาจาก WPA (802.11i) โดยเพิ่มความปลอดภัยในส่วนของการเข้ารหัสข้อมูล ทำงานโดยใช้ Cipher block Chaining Message Authentication Code Protocol (CCMP) และใช้ Advanced Encryption Standard (AES) ในการตรวจสอบความถูกต้อง

Part 3 WPA3

WPA3

WPA3 เป็นวิธีการที่ปลอดภัยและน่าเชื่อถือมากที่สุดในปี 2020 โดยมีการแก้ไขจุดบกพร่องของ WPA2 คือ four-way handshake ที่ไม่สมบูรณ์ ทำให้การเชื่อมต่อ Wi-Fi มีความเสี่ยง

Part 4 Summary Wireless Penetration Testing

วิธีการตรวจสอบความปลอดภัยของ Wireless Network ขององค์กร แบ่งออกเป็น 6 ส่วน ได้แก่

1. Sniffing
   ดักฟังข้อมูลสำคัญที่คุยกันระหว่าง user และข้ามการป้องกันที่ปิดไม่ให้ใช้ protocol ด้วย Covert Channel
2. Rogue Access Point หรือ Evil Twin
   สร้างการจำลอง Wireless Network ของที่มีจริงๆ เพื่อหลอกให้เหยื่อหลงเชื่อและขโมยข้อมูล
3. ปลอมแปลง Mac Address
   เพื่อปลอมเป็นผู้ใช้งานขององค์กรนั้น
4. crack weak key ของ Wireless ถ้า key ของ wireless network
   ตั้งค่าไว้ไม่หนาแน่นพอ อาจทำให้ผู้โจมตีเดาหรือ crack key ได้ง่าย
5. brute force username, password
   ถ้า username เป็นลักษณะเรียง (sequence) และไม่มีกฎการตั้ง password ที่ดีพอ อาจถูกเดาและถูกเข้าถึงระบบโดยไม่ได้รับอนุญาตได้
6. deauthentication attack
   ถูกนำไปใช้ในการประกอบการโจมตีอื่น แต่ถ้ามองที่ตัว deauthentication attack เพียงอย่างเดียวจะมองว่าเป็นการโจมตีเพื่อ DoS มากกว่า

Part 5 Bluetooth

<u>Bluetooth</u>

เป็น wireless protocol ที่ใช้ในความกว้างที่ค่อนข้างจำกัดระหว่างอุปกรณ์ โดย Bluetooth จะทำงานใน ISM Band ที่ 2.4 Ghz โดย Bluetooth Class A มีระยะ 100 เมตร โดยขึ้นอยู่กับความแรงของสัญญาณ แต่ปกติ Bluetooth จะทำงานที่ประมาณ 10 เมตรเท่านั้น ซึ่งทำให้ต้องใช้งานในระยะที่ใกล้

<u>Bluetooth Profile</u>

Bluetooth มีความสามารถที่หลากหลายขึ้นอยู่กับลักษณะการทำงาน เช่น

1. Advanced Audio Distribution Profile (A2DP)
   ส่งสัญญาณเสียงแบบ stereo ระหว่างอุปกรณ์
2. Audio/Video Remote Control Profile (AVRCP)
   ควบคุมภาพและเสียงผ่านอุปกรณ์ Bluetooth
3. Dial-up Networking Profile (DUN)
   เชื่อมต่ออินเทอร์เน็ตผ่านอุปกรณ์ Bluetooth
4. Hands-Free Profile (HFP)
   พูดคุยตลอดจนการควบคุมโทรศัพท์เบื้องต้น เช่น การรับสายโดยใช้อุปกรณ์ Bluetooth
5. Human Interface Device Profile (HID)
   การเชื่อมต่อที่ปลอดภัยสำหรับอุปกรณ์รับ input เช่น คีย์บอร์ด เมาส์

Chapter 4 - Cryptography

Part 1 ความแตกต่างระหว่าง Encoding x Encryption x Hashing

Encoding คือ การเข้ารหัสข้อความหรือการเปลี่ยนแปลงลักษณะการแสดงผลที่มี pattern แน่นอน
Encryption คือ การเข้ารหัสลับข้อความโดยใช้งาน key ที่ user กำหนด
Hashing คือ การสร้างค่าเฉพาะของข้อความใด ๆ โดยแต่ละข้อความมีค่า hash ที่ไม่ซ้ำกัน

Part 2 Encoding Part 1

ASCII Encoding

American Standard Code for Information Interchange (ASCII) โดยปกติ Computer เข้าใจแค่ตัวเลขซึ่ง ASCII code เป็นค่าตัวเลขแทนค่าของตัวอักษร โดยแปลงค่าไปมาระหว่าง ASCII Code กับตัวอักษร (Character) แล้วใช้ ASCII character table แทนค่าของ 32 ตัวอักขระพิเศษ

Base64 Encoding

เปลี่ยนตัวอักษรใด ๆ ให้อยู่ในรูปแบบเดียวกัน อีกทั้งยังแปลงค่าตัวอักษรจีน emoji และรูปภาพให้อยู่ในลักษณะเดียวกัน ทำให้ส่งไปที่ใดก็ได้

Base32 Encoding

Base32 คล้ายกับ Base64 แตกต่างที่ Base32 แทนค่าเพียง A-Z

Base58 Encoding

Base58 คล้ายกับ Base32, Base64 คือ เป็นเครื่องหมายที่ใช้แทนระบบตัวเลขหรือเสียงในการแปลงเพื่อส่งค่าข้อมูล แตกต่างกับ Base64 โดยมีการตัดส่วนที่อาจทำให้เข้าใจผิดได้ง่าย โดยปกติ Base58 ถูกใช้ใน cryptocurrencies

Base62 Encoding

Base62 คล้ายกับ Base32, Base64 แต่ตัดส่วนอักขระบางส่วนทิ้งในระบบที่ไม่อนุญาตหรือไม่เข้าใจ ทำให้คนประมวลผลได้ง่ายมากขึ้น

Base85 Encoding

Base85 ใช้เหมือนกับ Base64 โดยแทนค่าได้หลากหลายมากกว่าใน Base64 ซึ่งถูกนำไปใช้ใน Adobe's PostScript และ PDF file formats

Part 3 Encoding Part 2

Hexadecimal Encoding

Hexadecimal คือการใช้งานในรูปแบบของเลขฐาน 16 โดยแปลงจาก Character ให้กลายเป็น Decimal (ASCII) แล้ว Decimal แปลงเป็น Hexadecimal ได้

Morse Code

เป็นการสื่อสารรูปแบบหนึ่ง ซึ่งเป็นการเข้ารหัสตัวอักษร โดยตามด้วยช่วงสัญญาณที่แตกต่างกัน 2 แบบ คือ dot และ dash หรือ dit และ dah ทั้งนี้ Morse code มักถูกส่งไปเพื่อผ่านสื่อกลาง เช่น electric current, radio waves, visible light, หรือ sound waves

Part 4 Cryptography and Steganography

Cryptography หรือ Cryptology

ในอดีต การเข้ารหัส คือ แลกเปลี่ยนข้อมูลที่เป็นความลับ เพื่อเพิ่มความเป็นส่วนตัวหรือปกปิดข้อมูล ทั้งนี้ได้ถูกนำไปใช้ในสงครามตามชายแดน เพื่อส่งข้อมูลโดยไม่ใช้คำพูด โดยทหารได้สร้างเครื่องหมายและสัญลักษณ์ด้วยแขนและขาเพื่อส่งข้อมูล ทำให้ศัตรูไม่เข้าใจ

เมื่อนำ Cryptography (การเข้ารหัส) รวมกับ Cryptanalysis (การถอดรหัส) เรียกว่า Cryptology ซึ่งหมายถึงกระบวนการหรือส่วนที่เกี่ยวข้องทั้งหมดในการเข้ารหัส

ในปัจจุบัน การเข้ารหัส ใช้เพื่อติดต่อสื่อสารผ่านคอมพิวเตอร์และ network ซึ่งข้อมูลถูกส่งด้วยรูปแบบไม่สามารถเข้าใจได้ ทำให้บุคคลทั่วไปไม่เข้าใจ

เมื่อข้อมูลถูกส่งผ่าน network และผู้รับได้รับข้อมูลที่อยู่ในรูปแบบที่ไม่สามารถเข้าใจได้ถูกเปลี่ยนกลับไปเป็นรูปแบบที่สามารถอ่านเข้าใจได้ โดยปกติเราไม่สามารถเชื่อใจได้ว่า network ที่เราใช้อยู่ปลอดภัย เนื่องจากไม่สามารถรู้ได้ว่า Hacker หรือ Cracker อยู่ใน network วงเดียวกับเราหรือไม่ จึงจำเป็นต้องมีการเข้ารหัสข้อมูลที่ออกจากเครื่องผู้ส่งและการถอดรหัสที่เครื่องผู้รับ

Steganography

การเขียนแบบซ่อน คือ วิธีติดต่อสื่อสารที่ใช้การซ่อนข้อความในช่องทางสื่อสารที่มีอยู่ แสดงว่าใครจะดู ดักจับข้อความที่เราส่งก็ได้ แต่จะไม่รู้ว่าในข้อความทั่วไปนั้นมีข้อความอื่นซ่อนอยู่

Steganography กับ Cryptography มีจุดประสงค์เหมือนกัน คือ พยายามไม่ให้ใครอ่านข้อความเราได้ แต่ Steganography ไม่มีการเพิ่มลด เปลี่ยนแปลงข้อความที่เราต้องการส่งแต่อย่างใด และตรวจจับได้ง่ายกว่า Cryptography แต่บางองค์กรจำกัด algorithm และการใช้งาน Cryptography ทำให้บางครั้งใช้ Steganography แทนเพราะสะดวกและค่อนข้างเร็วกว่า Cryptography

Part 5 Binwalk command

Binwalk

เป็นเครื่องมือที่ใช้ค้นหาไฟล์ binary เช่น ภาพ, เสียงที่อยู่ภายใต้ไฟล์, ไฟล์ zip ที่อยู่ภายใน binary โดยปกติใช้ใน firmware analysis

Part 6 Symmetric Encryption

Symmetric Encryption

การที่ฝ่ายผู้รับและผู้ส่งข้อมูลมี key ที่ใช้เหมือนกัน (secret key) มีหลาย algorithm ที่ใช้รูปแบบนี้ เช่น DES(Data Encryption Standard), AES(Advanced Encryption Standard), RC4, Blowfish

Part 7 Diffie-Hellman

Diffie-Hellman

Diffie-Hellman (DH) เป็นกระบวนการสร้าง แลกเปลี่ยน key ระหว่างผู้สื่อสาร โดยไม่จำเป็นต้องส่ง key นั้นโดยตรง เพื่อป้องกันการถูกดักจับระหว่างส่งข้อมูล ซึ่งทำให้ key นั้นหลุดได้ จึงต้อง share secret ระหว่างกันผ่านช่องทางปกติ