การทดสอบความปลอดภัยของระบบจำลองยุทธ

Cyberrange Simulation System Penetration Testing

นายวัชระ จึงมงคลสวัสดิ์

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยี ไทย-ญี่ปุ่น
พ.ศ. 2559

การทดสอบความปลอดภัยของระบบจำลองยุทธ

Cyberrange Simulation System Penetration Testing

นายวัชระ จึงมงคลสวัสดิ์

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรบัณฑิต สาขาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีไทย - ญี่ปุ่น
ปีการศึกษา 2559

คณะกรรมการสอบ

..... ประธานกรรมการสอบ
(ผศ.ดร.นรังสรรค์ วิไลสกุลยง)

..... กรรมการสอบ
(ผศ.ตรีรัตน เมตต์การุณ์จิต)

..... อาจารย์ที่ปรึกษา
(ดร.ปราณิสา อิศรเสนา)

..... ประธานสหกิจศึกษาสาขาวิชา
(อาจารย์อมรพันธ์ ชมกลิ่น)

ชื่อโครงงาน	การทดสอบความปลอดภัยของระบบจำลองยุทธ Cyberrange Simulation System Penetration Testing
ผู้เขียน	นายวัชระ จึงมงคลสวัสดิ์
คณะวิชา	เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ
อาจารย์ที่ปรึกษา	อาจารย์ปราณิสา อิศรเสนา
พนักงานที่ปรึกษา	คุณวัชรพล วงศ์อภัย
ชื่อบริษัท	บริษัท ไซเบอร์ตรอน จำกัด
ประเภทธุรกิจ/สินค้า	Cybersecurity ,SOC Operation

บทสรุป

ปัจจุบันความปลอดภัยทางเทคโนโลยีสารสนเทศเป็นปัจจัยสำคัญอย่างหนึ่งในการดำเนินธุรกิจ เพราะว่าข้อมูลสำคัญนั้นย่อมเป็นความลับและมีค่า จึงเป็นไม่ได้เลยที่จะยอมให้ข้อมูลเหล่านั้นตกไปอยู่ในมือของผู้ไม่หวังดี ปกติในหลาย ๆ องค์กรก็ได้ดำเนินการป้องกันเซิร์ฟเวอร์และเครือข่ายภายในแล้ว แต่ลืมที่จะป้องการในส่วนของเว็บเซิร์ฟเวอร์ของตัวเองที่อยู่ใน demilitarized Zone ก็สามารถใช้เป็นเครื่องมือในการเข้าสู่ระบบภายในได้โดยเฉพาะผ่านทางโปรแกรมที่ไม่มีความปลอดภัยและไม่สามารถหาผู้พัฒนาต่อได้

ในการทดสอบเจาะระบบของระบบจำลองยุทธนั้น ซึ้งเป็นผลิตภัณฑ์ของบริษัทจึงต้องทำให้มีความปลอดภัยต่อตัวระบบมากขึ้น โดยในการทดสอบเจาะระบบจะทำให้ทราบถึงช่องโหว่ที่เกิดขึ้นต่อตัวระบบ Cyberrange หรือระบบจำลองยุทธและได้มีการแก้ไขถึงช่องโหว่นั้นได้ทันทำให้ระบบ Cyberrange มีความปลอดภัยต่อตัวระบบและต่อตัวผู้ใช้งาน

กิตติกรรมประกาศ

ในการจัดทำโครงงานสหกิจครั้งนี้สำเร็จลุล่วงไปด้วยดีด้วยความเมตตาช่วยเหลือเป็นอย่างดีจากบุคคลหลายท่าน ผู้มีพระคุณท่านแรกคือ ท่านอาจารย์ปราณิสา อิศรเสนา ผู้ให้ความรู้ และให้คำแนะนำปรึกษาที่ดีตลอดมา จนจัดทำโครงงานสหกิจศึกษาเสร็จสมบูรณ์ไปได้ด้วยดี ท่านที่สองคือ ท่านอาจารย์วัชรพล วงศ์อภัย ผู้ให้คำแนะนำปรึกษาในการจัดทำโครงงานสหกิจศึกษา และให้ความช่วยเหลือในการแก้ปัญหาต่าง ๆ จนเสร็จสิ้น

ขอขอบพระคุณบริษัท ไซเบอร์ตรอน จำกัดที่ให้โอกาสในการฝึกและปฏิบัติงานทำให้ได้ประสบการณ์จากการปฏิบัติงานจริง และให้ความรู้หลาย ๆ อย่างจากการได้ร่วมฝึกอบรมเป็นข้อมูลในการจัดทำโครงงานนี้สำเร็จลุล่วงไปได้ด้วยดี ขอบพระคุณ

สารบัญ

สารบัญ

สารบัญ

สารบัญรูป

สารบัญรูป

สารบัญตาราง

บทที่ 1 บทนำ

1.1 ชื่อและที่ตั้งของสถานประกอบการ

1.1.1 ชื่อสถานประกอบการ

ชื่อภาษาไทย : บริษัท ไซเบอร์ตรอน จำกัด

ชื่อภาษาอังกฤษ : Cyber Range Co., Ltd.

รูปที่ 1.1 สัญลักษณ์บริษัท

1.1.2 ที่ตั้งสถานประกอบการ

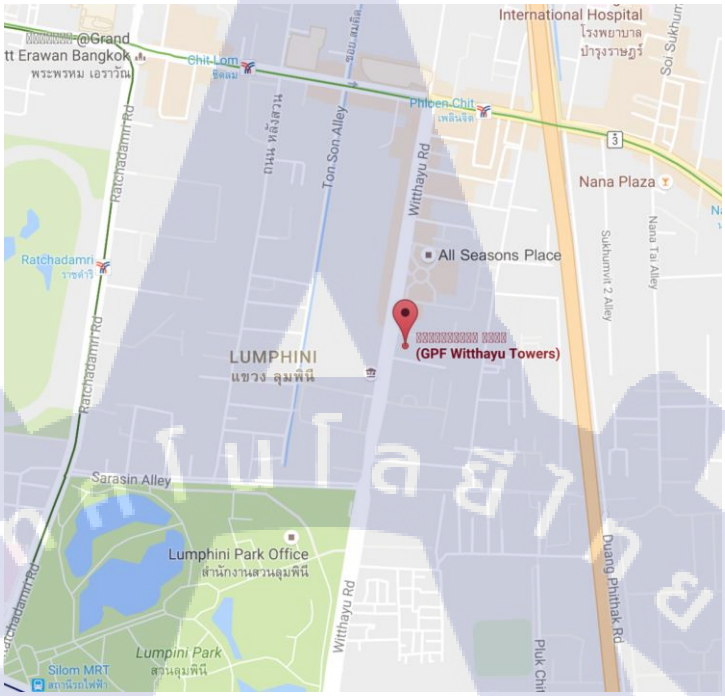
ที่อยู่ : 93/1 อาคารจีพีเอฟวิทยุ ทาวเวอร์ บี, ห้อง 805 ชั้นที่ 8 ถนนวิทยุ แขวงลุมพินี เขตปทุมวัน กรุงเทพมหานคร 10330

โทรศัพท์ : 02-651-5099

โทรสาร : 02-651-5098

อีเมล : contact@Cyber Range.co.th

เว็บไซต์ : http://Cyber Range.co.th

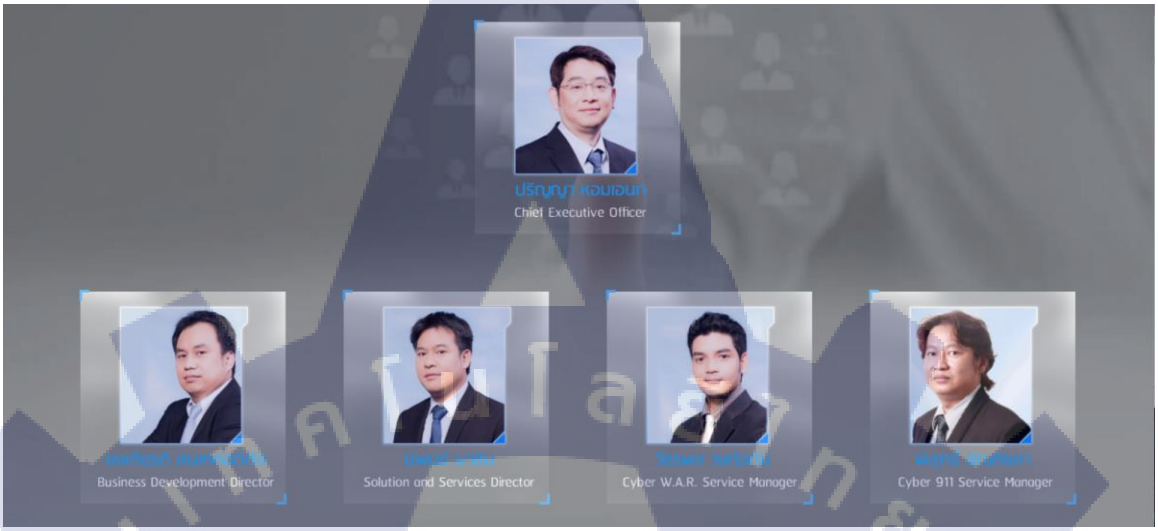


รูปที่ 1.1.2 สถานที่ตั้งสถานประกอบการ

1.2 ลักษณะธุรกิจของสถานประกอบการ หรือการให้บริการหลักขององค์กร

บริษัท ไซเบอร์ตรอน จำกัด เกิดจากการร่วมทุนระหว่าง บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด และ บริษัท เจนเนอรัล อิเลคทรอนิค คอมเมอร์ซ เซอร์วิสเซส จำกัด เพื่อผนึกกำลังร่วมกันให้บริการศูนย์เฝ้าระวังภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์รูปแบบใหม่ ที่เน้นการตอบสนองต่อภัยคุกคามและเข้าแก้ไขปัญหาให้กับลูกค้าอย่างรวดเร็ว (Responsive Security) พร้อมบริการโซลูชั่นระบบจำลองยุทธ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber W.A.R.) ในทุกมิติ เช่น Offensive, Defensive, Forensic, Security Audit และ Cyber Intelligence โดยผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ที่มีประสบการณ์กว่า 20 ปี และได้รับวุฒิบัตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับสากล เช่น CISSP, GCIH, GREM, GXPN, OSCP และอื่นๆ อีกมากมาย

1.3 รูปแบบการจัดองค์กรและการบริหารองค์กร



รูปที่ 1.3 โครงสร้างองค์กร

1.4 ตำแหน่งและหน้าที่งานที่นักศึกษาได้รับมอบหมาย

ตำแหน่ง : Technic Vulnerability and Testing Web Developer

หน้าที่งาน : พัฒนาระบบจำลองยุทธ์ Cyberrange, ออกแบบโจทย์ที่ใช้กับระบบจำลองยุทธ์, ติดตั้งระบบจำลองยุทธ์, ออกแบบ Script ให้ทำงานแบบ Automate

1.5 พนักงานที่ปรึกษา และ ตำแหน่งของพนักงานที่ปรึกษา

พนักงานที่ปรึกษา : นายวัชรพล วงศ์อภัย

ตำแหน่ง : Product Manager

เบอร์โทร : 085-115-9593

อีเมล : watcharaphon.wo@Cyber Range.co.th

1.6 ระยะเวลาที่ปฏิบัติงาน

ระยะเวลา ตั้งแต่วันที่ 30 พฤษภาคม พ.ศ. 2559 ถึงวันที่ 30 กันยายน พ.ศ. 2559 การปฏิบัติงานรวมระยะเวลาทั้งสิ้นประมาณ 18 สัปดาห์

1.7 วัตถุประสงค์หรือจุดมุ่งหมายของการปฏิบัติงาน

- เพื่อศึกษาและพัฒนาความรู้การทำงานจากสถานปฏิบัติงานจริง
- การทำงานของเว็บแอปพิลเคชันจำลองสถานการณ์ สามารถทำงานได้อย่างสมบูรณ์และเหมือนจริงที่สุด
- พัฒนาองค์ความรู้ของผู้ฝึก โดยใช้ระบบจำลองยุทธ์ Cyberrange
- ออกแบบโจทย์ที่ใช้ในการฝึกของระบบจำลองยุทธ์

1.8 ผลที่คาดว่าจะได้รับจากการปฏิบัติงานหรือโครงงานที่ได้รับมอบหมาย

- สามารถนำความรู้ที่เรียนมาประยุกต์ใช้ในการปฏิบัติงานจริงได้
- สามารถทำงานเป็นทีมและมีระบบได้
- สามารถเข้าใจวัฒนธรรมการทำงานภายในองค์กรได้
- สามารถแก้ไขปัญหาเฉพาะหน้าได้
- สามารถรับผิดชอบต่อหน้าที่และเวลาได้
- สามารถเพิ่มประสิทธิภาพในการทำงานของตัวนักศึกษาได้
- สามารถป้องกัน และแนะนำผู้อื่นถึงภัยทางไซเบอร์ได้

บทที่ 2 ทฤษฎีและเทคโนโลยีที่ใช้ในการปฏิบัติงาน

2.1 ทฤษฎีที่ใช้ในการปฏิบัติงาน

2.1.1 Computer Network

Computer Network คือระบบเครือข่ายคอมพิวเตอร์ หมายถึงการเชื่อมต่อคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไปเข้าด้วยกันด้วยสายเคเบิลซึ่งทำให้คอมพิวเตอร์สามารถรับส่งข้อมูลแก่กันและกันได้ ในการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์หลายๆ เครื่องเข้ากับเครื่องคอมพิวเตอร์ขนาดใหญ่ที่เป็นศูนย์กลาง โดยเรียกคอมพิวเตอร์ที่เป็นศูนย์กลางนี้ว่า โฮสต์ (Host) และเรียกคอมพิวเตอร์ขนาดเล็กที่เข้ามาเชื่อมต่อว่า ไคลเอนต์ (Client/Terminal) รูปแบบของเน็ตเวิร์คแบ่งได้เป็น 3 ลักษณะ ดังนี้

2.1.1.1 LAN (Local Area Network)

LAN (Local Area Network) คือ กลุ่มของคอมพิวเตอร์ที่เชื่อมต่อกันในพื้นที่จำกัด เช่น ภายในตึกสำนักงาน หรือภายในโรงงาน ส่วนมากจะใช้สายเคเบิ้ลในการติดต่อสื่อสารกัน

2.1.1.2 MAN (Metropolitan Area Network)

MAN (Metropolitan Area Network) คือ การนำระบบ LAN หลายๆ LAN ที่มีพื้นที่อยู่ใกล้เคียงกันมาเชื่อมต่อกัน ให้มีขนาดใหญ่ขึ้น เช่นเชื่อมต่อกันในเมือง หรือในจังหวัด เป็นต้น

2.1.1.3 WAN (Wide Area Network)

WAN (Wide Area Network) คือ กลุ่มของคอมพิวเตอร์ที่เชื่อมต่อกันแบบกว้างขวาง อาจจะเป็นภายในประเทศ หรือระหว่างประเทศเป็นการใช้ หลายๆ LAN หรือหลายๆ MAN ซึ่งอยู่คนละพื้นที่ เชื่อมต่อเข้าหากัน เช่น สำนักงานที่ New York เชื่อมต่อกับที่ London การติดต่อสื่อสารกัน อาจจะใช้ตั้งแต่สายโทรศัพท์จนกระทั่งถึงดาวเทียม

2.1.2 Internet

2.1.2.1 Internet คืออะไร

Internet มาจากคำว่า “International network” ซึ่งหมายถึง เครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่ เชื่อมโยงเครือข่ายคอมพิวเตอร์ทั่วโลกเข้าไว้ด้วยกัน เพื่อให้เกิดการสื่อสาร และการ

แลกเปลี่ยนข้อมูลร่วมกัน โดยอาศัยตัวเชื่อมเครือข่ายภายใต้มาตรฐานการเชื่อมโยงเดียวกัน นั่นก็คือ TCP/IP Protocol ซึ่งเป็นข้อกำหนดวิธีการติดต่อสื่อสารระหว่างคอมพิวเตอร์ในระบบเครือข่าย

2.1.2.2 ประวัติความเป็นมาของ อินเตอร์เน็ต

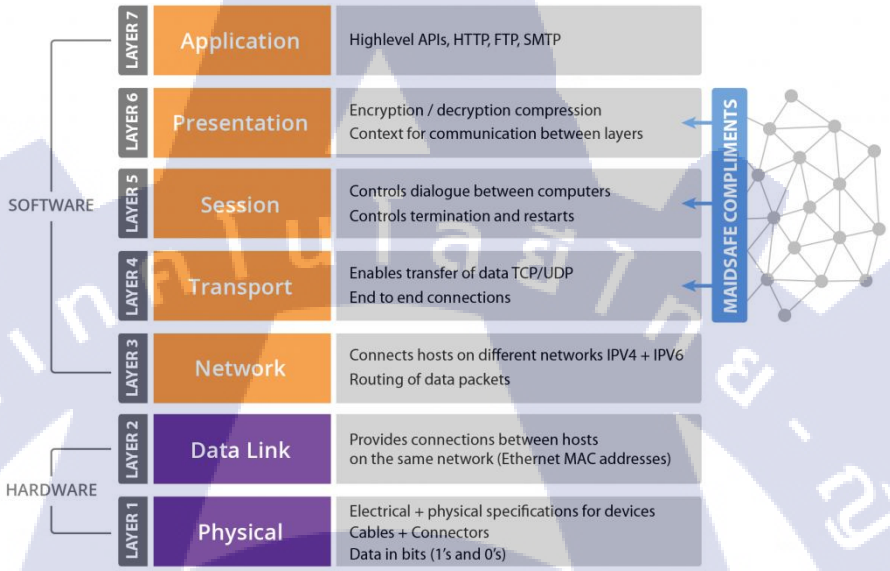
อินเตอร์เน็ต มีพัฒนาการมาจาก อาร์พาเน็ต (Arp Anet เรียกสั้น ๆ ว่า อาร์พา) ที่ตั้งขึ้นในปี 2512 เป็นเครือข่ายคอมพิวเคอร์ของกระทรวงกลาโหม สหรัฐอเมริกา ที่ใช้ในงานวิจัยด้าน ทหาร (ARP : Advanced Research Project Agency) มาถึงปี 2515 หลังจากที่เครือข่ายทดลอง อาร์พาประสบความสำเร็จอย่างสูง และได้มีการปรับปรุงหน่วยงานจากอาร์พามาเป็นดาร์พา (Defense Advanced Research Project Agency: DARPA) และในที่สุดปี 2518 อาร์พาเน็ตก็ขึ้น ตรงกับหน่วยการสื่อสารของกองทัพ (Defense Communication Agency) ในปี 2526 อาร์ พาเน็ตก็ได้แบ่งเป็น 2 เครือข่ายด้านงานวิจัย ใช้ชื่ออาร์พาเน็ตเหมือนเดิม ส่วนเครือข่ายของ กองทัพใช้ชื่อว่า มิลเน็ต (MILNET : Millitary Network) ซึ่งมีการเชื่อมต่อโดยใช้โพรโตคอล TCP/IP (Transmission Control Protocol/Internet) เป็นครั้งแรก ในปี 2528 มูลนิธิวิทยาศาสตร์ แห่งชาติของอเมริกา (NSF) ได้ ให้เงินทุนในการสร้างศูนย์ซูเปอร์คอมพิวเตอร์ 6 แห่ง และใช้ ชื่อว่า NSFNETและพอมาถึงปี 2533 อาร์พารองรับภาระที่เป็นกระดูกสันหลัง (Backbone) ของ ระบบไม่ได้ จึงได้ยุติอาร์พาเน็ต และเปลี่ยนไปใช้ NSFNET และเครือข่ายขนาดมหึมาจนถึง ทุกวันนี้ และเรียกเครือข่ายนี้ว่า อินเตอร์เน็ต โดยเครือข่ายส่วนใหญ่จะอยู่ในอเมริกาและ ปัจจุบันนี้มีเครือข่ายย่อยมากถึง 50,000 เครือข่ายทีเดียว และคาดว่า ภายในปี 2543 จะมีผู้ใช้อินเตอร์เน็ตทั้งโลกประมาณ 100 ล้านคน หรือใกล้เคียงกับประชากรในโลกทั้งหมด

2.1.3 Intranet

Intranet คือ ระบบเครือข่ายภายในองค์กร เป็นบริการ และการเชื่อมต่อคอมพิวเตอร์เหมือนกับ Internet แต่จะเปิดให้ใช้เฉพาะสมาชิกในองค์กรเท่านั้น เป็นการจำกัดขอบเขตการใช้งาน ดังนั้นระบบอินเทอร์เน็ตในองค์กร ก็คือ "อินทราเน็ต" นั่นเอง บางครั้งถูกเรียกว่า Campus network, Local internet, Enterprise network เป็นต้น

2.1.4 OSI Model

OSI Model คือ โครงสร้างการสื่อสารของข้อมูลที่กำหนดขึ้นในแต่ละชั้น ในการสื่อสารข้อมูลจะเรียกว่า Layer หรือ “ชั้น” รูปแบบของการสื่อสารข้อมูลจะประกอบด้วยชั้นย่อยๆ 7 ชั้นดังนี้



รูปที่ 2.1 รูปแบบของ OSI Model

2.1.4.1 Layer 1 Physical Layer

Physical Layer เป็นชั้นล่างสุด และเป็นชั้นเดียวที่มีการเชื่อมต่อทางกายภาพระหว่างคอมพิวเตอร์สองระบบที่ทำการรับส่งข้อมูล ใน Layer ที่ 1 นี้จะมีการกำหนดคุณสมบัติทางกายภาพของฮาร์ดแวร์ที่ใช้เชื่อมต่อระหว่างคอมพิวเตอร์ทั้งสอง เช่น สายที่ใช้รับส่งข้อมูล เป็นต้น

2.1.4.2 Layer 2 Data link Layer

Data link Layer เป็นชั้นที่ทำหน้าที่เชื่อมต่อการรับส่งข้อมูลในระดับฮาร์ดแวร์ โดยเมื่อมีการสั่งให้รับข้อมูลจากใน Layer ที่ 3 ลงมา Layer ที่ 2 จะทำหน้าที่แปลคำสั่งนั้นให้เป็นคำสั่งควบคุมฮาร์ดแวร์ที่ใช้รับส่งข้อมูล ทำการตรวจสอบข้อผิดพลาดในการรับส่งข้อมูลของระดับฮาร์ดแวร์ และทำการแก้ข้อผิดพลาดที่ได้ตรวจพบ ข้อมูลที่อยู่ใน Layer ที่ 2 จะอยู่ในรูปของ Frame

2.1.4.3 Layer 3 Network Layer

Network Layer ทำหน้าที่เชื่อมต่อคอมพิวเตอร์ ที่เข้าหากันผ่านระบบเครือข่าย พร้อมทั้งเลือกหรือกำหนดเส้นทางที่จะใช้ในการรับส่งข้อมูลระหว่างกัน และส่งผ่านข้อมูลที่ได้รับไปยังอุปกรณ์ในเครือข่ายต่าง ๆ

2.1.4.4 Layer 4 Transport Layer

Transport Layer ทำหน้าที่เชื่อมต่อการรับส่งข้อมูลระดับสูงของ Layer ที่ 5 มาเป็นข้อมูลที่รับส่งในระดับฮาร์ดแวร์ เช่น แปลงค่าหรือชื่อของเครื่องคอมพิวเตอร์ในเครือข่ายให้เป็น network address พร้อมทั้งเป็นชั้นที่ควบคุมการรับส่งข้อมูลจากปลายด้านส่งถึงปลายด้านรับข้อมูล ให้ข้อมูลมีการไหลลื่นตลอดเส้นทางตามจังหวะที่ควบคุมจาก Layer ที่ 5

2.1.4.5 Layer 5 Session Layer

Session Layer ทำหน้าที่ควบคุม “จังหวะ” ในการรับส่งข้อมูลของคอมพิวเตอร์ทั้งสองด้านที่รับส่งแลกเปลี่ยนข้อมูลกันให้มีความสอดคล้องกัน (Synchronization) และกำหนดวิธีที่ใช้ในการรับส่งข้อมูล เช่น อาจจะเป็นในการสลับกันส่ง (Half Duplex) หรือการรับส่งข้อมูลพร้อมกันทั้งสองด้าน (Full Duplex)

2.1.4.6 Layer 6 Presentation Layer

Presentation Layer เป็นชั้นที่ทำหน้าที่ตกลงกับคอมพิวเตอร์อีกด้านหนึ่งในระดับชั้นเดียวกันว่า การรับส่งข้อมูลในระดับโปรแกรมประยุกต์จะมีขั้นตอนและข้อบังคับอย่างไร ข้อมูลที่รับส่งกันใน Layer ที่ 6 จะอยู่ในรูปแบบของข้อมูลชั้นสูงมีกฎ (Syntax)

2.1.4.7 Layer 7 Application Layer

Application Layer เป็นชั้นที่อยู่บนสุดของขบวนการับส่งข้อมูล ทำหน้าที่ติดต่อกับผู้ใช้โดยจะรับคำสั่งต่างๆ จากผู้ใช้ส่งให้คอมพิวเตอร์แปลความหมาย และทำงานตามคำสั่งที่ได้รับในระดับโปรแกรมประยุกต์ เช่น การแปลความหมายของการกดปุ่มบนเมาส์ให้เป็นคำสั่งในการก็อปปี้ไฟล์ หรือ ดึงข้อมูลมาแสดงบนจอภาพ เป็นต้น

2.1.5 Ethical hacker

Ethical hacker หมายถึง ผู้ที่ทำการทดสอบการเจาะระบบโดยใช้วิธีเดียวกันกับที่ hacker ใช้แต่จะ ไม่ทำลายหรือละเมิดสิทธิ โดยจะทำงานอย่างใกล้ชิดกับองค์กรเพื่อปกป้องสินทรัพย์ขององค์กรนั้นๆ โดยขั้นตอนการทดสอบระบบของ Ethical hacker แบ่งออกเป็น 5 ขั้นตอนหลักๆ ดังนี้

2.1.5.1 การสอดส่อง (Reconnaissance)

การสอดส่อง (Reconnaissance) สำหรับ Computer Security แบ่งออกเป็น 2 รูปแบบคือ

2.1.5.1.1 Passive reconnaissance

การสอดส่องแบบนี้เป็นการสอดส่องเพื่อเก็บข้อมูล รูปแบบของการทำงานต่างๆ ของเป้าหมาย โดยปราศจากข้อมูลส่วนบุคคลใดๆ ซึ่งสามารถทำได้อย่างง่ายๆ เช่น การเฝ้าดูตึกของบริษัทเป้าหมายเพื่อจะตรวจสอบเวลาเข้าออกของพนักงาน ในบางครั้งเราอาจเลือกใช้ Google ในการค้นหาตำแหน่งของเป้าหมายเพื่อเก็บข้อมูลให้ได้มากที่สุด

2.1.5.1.2 Active reconnaissance

เป็นการค้นหาข้อมูลของเครือข่ายเป้าหมาย เช่น ตรวจสอบ IP Address หรือรายชื่อ Service และ Port ที่เปิดใช้งาน โดยปกติแล้วการทำ Active reconnaissance มีความเสี่ยงสูงที่จะถูกตรวจพบมากกว่า Passive reconnaissance ทั้งนี้ การทำ Passive reconnaissance และ Active reconnaissance สามารถนำไปสู่การค้นพบข้อมูลที่มีประโยชน์ต่อการโจมตีได้

2.1.5.2 การสแกนระบบ (Scanning)

การสแกนระบบ (Scanning) เป็นการนำข้อมูลที่รวบรวมมาได้จากขั้น Reconnaissance มาอธิบายถึงโครงสร้างต่างๆ ของเครือข่ายเป้าหมาย รูปแบบการทำงานที่ Hacker ส่วนใหญ่ใช้ก็คือการสแกนพอร์ตของเครื่อง Server เช่น การทำ Network Mapper (Nmap) เพื่อตรวจสอบว่าเครื่อง Server ในเครือข่ายเป้าหมายเปิดให้บริการอยู่หรือไม่ รวมถึงการค้นหาช่องโหว่ต่างๆ ของระบบเครือข่ายอีกด้วย ซึ่งหาก Hacker ได้ข้อมูลสำคัญต่าง ๆ ครบถ้วน หรือเพียงบางส่วน เช่น ชื่อเครื่อง Server, หมายเลข IP Address ของเครื่องเป้าหมาย หรือรายชื่อ User Account คนสำคัญ ก็จะทำให้มองเห็นช่องทางในการเจาะระบบเข้าไปได้

2.1.5.3 การเข้าถึงเป้าหมาย (Gaining Access)

การเข้าถึงเป้าหมาย (Gaining Access) คือขั้นตอนที่จะเริ่มเข้าสู่การโจมตีหรือเจาะช่องโหว่ที่ถูกตรวจพบ ข้อมูลที่เก็บรวบรวมอยู่ในระหว่างขั้นตอนการ Reconnaissance และการ Scanning จะถูกนำมาใช้เพื่อให้สามารถเข้าถึงเครื่องหรือเครือข่ายเป้าหมายได้

2.1.5.4 การคงสภาพทางเข้า (Maintaining Access)

การคงสภาพทางเข้า (Maintaining Access) เมื่อสามารถ Hack เข้าไปในระบบได้แล้ว Hacker มักต้องการที่จะเก็บช่องทางเดิมไว้เพื่อเข้ามาโจมตีในภายหลังได้อีก ทำให้บางครั้งก็ทำการเพิ่มความปลอดภัยให้กับเครื่องหรือระบบเป้าหมายที่ตกเป็นเหยื่อด้วย เพื่อป้องกันการบุกรุกเข้ามาจาก Hacker อื่น โดยได้ทำการเพิ่มช่องทางพิเศษสำหรับตนเองโดยเฉพาะ ด้วยการฝัง Backdoor, Root kits และ Trojan ไว้ในเครื่องของเหยื่อ

2.1.5.5 การลบร่องรอย (Covering Tracks)

การลบร่องรอย (Covering Tracks) คือ เมื่อ Hacker สามารถครอบครองได้อย่างสมบูรณ์และเก็บช่องทางเดิมไว้ใช้ต่อได้แล้ว ก็จะลบหลักฐานในการ Hack และร่องรอยของตัวมันเองออกไป เพื่อซ่อนตัวจากการถูกตรวจสอบจากาผู้ดูแลระบบหรือการเอาผิดทางกฎหมาย

2.1.6 Penetration test

Penetration test คือการทดสอบเพื่อหาช่องทางในการเข้าถึงระบบ (Exploit) ซึ่งการเข้าถึงระบบโดยผ่านช่องโหว่ที่พบอาจเป็น 0day ที่ยังไม่พบการแจ้งเตือนจากผู้ผลิต (Vendor) และการกระทำใดๆที่อาจทำให้ผู้ว่าจ้างได้ทราบถึงความเสี่ยง เสมือนปฏิบัติจริงการเป็นแฮกเกอร์เพื่อเจาะระบบ

2.1.7 Vulnerability Assessment

Vulnerability Assessment คือ การประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ที่ค้นพบ ตามช่องโหว่ที่มีความเสี่ยง ซึ่งส่วนใหญ่แล้วเป็นความเสี่ยงที่ปรากฏต่อสาธารณะแล้วตาม CVE (Common Vulnerabilities and Exposures)

ความแตกต่างทั้ง 2 คำนี้ก็คือ Pen-test นั้นคือการทดสอบเจาะระบบแบบแฮกเกอร์ เพื่อประเมินความเสี่ยงของธุรกิจหรือองค์กรนั้น ส่วน VA จะเน้นตรวจหาช่องโหว่ที่เป็นสาธารณะที่มีการ

เผยแพร่ช่องโหว่นั้นแล้ว เพื่อไม่ให้ถูกโจมตีจากผู้ไม่ประสงค์ดีได้ ทั้งคู่นี้จำเป็นต้องออกรายงานถึงระดับความเสี่ยงให้ผู้ว่าจ้างนั้นได้รู้ถึงภัยอันตรายที่อาจเกิดขึ้น

2.1.8 Open Web Application Security Project (OWASP)

Open Web Application Security Project (OWASP) คือ องค์การไม่แสวงหาผลกำไร (Non-profit organization) ถูกจัดตั้งขึ้นที่ประเทศสหรัฐอเมริกาเมื่อวันที่ 21 เมษายน 2004 โดยมีจุดประสงค์เพื่อเป็นองค์กรสากลที่เป็นศูนย์ร่วมในการร่วมมือจากนักพัฒนาเว็บแอปพลิเคชันทั่วโลกในการสร้างเว็บแอปพลิเคชันให้มีความปลอดภัย โดย OWASP ได้รับการสนับสนุนจากบริษัท IT ชั้นนำทั่วโลกในการจัดสัมนาและการจัดอบรมเกี่ยวกับความปลอดภัยเว็บแอปพลิเคชัน อีกทั้งยังมีเว็บไซต์ที่ใช้ในการเก็บรวบรวมและเผยแพร่ความรู้เกี่ยวกับช่องโหว่ที่พบได้บ่อยและวิธีการป้องกันโดยมีการจัดอันดับ ไว้ 10 อันดับยอดนิยมดังนี้

2.1.8.1 Injection

Injection ช่องโหว่ด้านความปลอดภัยประเภท Injection ถูกพบได้บ่อยและมีผลกระทบด้านความปลอดภัยอย่างรุนแรงต่อเว็บแอปพลิเคชัน ซึ่งช่องโหว่ประเภทนี้ประกอบไปด้วย SQL Injection ที่อนุญาตให้ผู้ไม่หวังดีเรียกดูข้อมูลที่เป็นความลับในฐานข้อมูล หรือแม้กระทั่งลบหรือแก้ไขข้อมูลในฐานข้อมูลบนเว็บไซต์

2.1.8.2 Broken Authentication and Session Management

Broken Authentication and Session Management ช่องโหว่ชนิดนี้ได้แก่ การเก็บข้อมูล password ไว้ใน cookie ของผู้ใช้งานโดยไม่ได้ทำการเข้ารหัส หรือ การแสดงข้อมูล session บน URLที่อาจจะดูแอบดูหรือดักจับจากผู้ไม่หวังดีได้

2.1.8.3 Cross-Site Scripting *(XSS)*

Cross-Site Scripting (XSS) ช่องโหว่ XSS เกิดจากการอนุญาตให้ผู้ใช้งานฝัง JavaScript ลงในเว็บไซต์ซึ่งนำไปสู่การขโมยข้อมูล session ของผู้ใช้งานคนอื่น แม้ว่า XSS จะไม่มีผลกระทบต่อตัวเว็บแอปพลิเคชันโดยตรง แต่ก่อนให้เกิดความเสียหายต่อผู้ใช้งานเว็บไซต์อย่างรุนแรง

2.1.8.4 Insecure Direct Object References

Insecure Direct Object References คือเกิดจากการที่ผู้พัฒนาอนุญาตให้ผู้ใช้งานเข้าถึงข้อมูลหรือเอกสารที่ไม่สมควร ตัวอย่างเช่น การเข้าถึงข้อมูลธุรกรรมทางการเงินผ่านทาง user id http://www.somebank.com?account_transaction.php?user_id=20 หากผู้ใช้งานสามารถดูธุรกรรมทางการเงินของคนอื่นได้ผ่านการเปลี่ยน user_id จาก 20 เป็น 10 30 40 ใน URL ก็อาจเป็นการทำให้ข้อมูลความลับข้อผู้ใช้งานอื่นรั่วไหล

2.1.8.5 Security Misconfiguration

Security Misconfiguration คือ ช่องโหว่ Security Misconfiguration ซึ่งขอบเขตของช่องโหว่นั้นค่อนข้างกว้างเพราะการตั้งค่าความปลอดภัยนั้นรวมทั้ง web application, web server, web server software, database

2.1.8.6 Sensitive Data Exposure

Sensitive Data Exposure เป็นช่องโหว่เกี่ยวกับการรั่วไหลของข้อมูลที่เก็บอยู่ในเซิร์ฟเวอร์และข้อมูลที่ส่งผ่านอินเทอร์เน็ต ตัวอย่างเช่น การ login เว็บไซต์ที่ไม่ได้ใช้ HTTPS ในการเข้ารหัสข้อมูล การเก็บข้อมูล password หรือข้อมูลที่เป็นความลับโดยไม่ได้เข้ารหัส หรือ การใช้ weak algorithm ในการเข้ารหัส ข้อผิดพลาดเหล่านี้ทำให้ข้อมูลที่เป็นความลับตกอยู่ในสภาวะเสี่ยงต่อการรั่วไหล

2.1.8.7 Missing Function Level Access Control

Missing Function Level Access Control ช่องโหว่นี้เป็นช่องโหว่เกี่ยวกับการจำกัดสิทธิ์ในการใช้งานเว็บแอปพลิเคชัน ตัวอย่างเช่น หากผู้ใช้งานสามารถเข้าถึง admin ได้โดยไม่ได้ทำการ login ด้วย admin account ก็เป็นการอนุญาตให้ใครก็ตามที่เป็น user ของเว็บไซต์สามารถเข้าไปใช้งานฟังก์ชันของ admin ได้โดยไม่ได้รับอนุญาต

2.1.8.8 Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF) ลักษณะของ CSRF คือการที่ผู้ไม่หวังดีสามารถสั่งให้ผู้ใช้งานเว็บแอปพลิเคชันทำกิจกรรมบางอย่าง

2.1.8.9 Using Components with Known Vulnerabilities

Using Components with Known Vulnerabilities ช่องโหว่ประเภทนี้จะเกิดจากการที่เว็บแอปพลิเคชันทำงานร่วมกับส่วนประกอบต่าง ๆ ที่มีช่องโหว่ เช่น libraries หรือ framework ที่มีช่องโหว่ ผู้ดูแลระบบควรตรวจสอบช่องโหว่ต่าง ๆ ที่ประกาศบน http://cve.mitre.org และค่อยอัพเดท patch เพื่อปิดช่องโหว่เหล่านี้หากตรวจพบ

2.1.8.10 Unvalidated Redirects and Forwards Unvalidated

Unvalidated Redirects and Forwards Unvalidated เป็นช่องโหว่ที่อนุญาตให้ผู้ไม่หวังดีทำการ redirect ผู้ใช้งานเว็บไซต์ที่ไปยังเว็บไซต์อันตราย ตัวอย่างเช่น หากเว็บไซต์ธนาคารแห่งหนึ่งมีหน้าที่ใช้ในการ redirect ผู้ใช้งานไปยังเว็บไซต์ย่อยของแต่ละประเทศ

2.1.9 วงจรการทดสอบเจาะระบบ Penetration test Method topology

ในส่วนของขั้นตอนการทดสอบการเจาะระบบของผู้ทดสอบเจาะระบบโดยขั้นตอนการทดสอบเจาะระบบสามารถแบ่งเป็น 3 ขั้นตอนดังนี้

2.1.9.1 วางแผนและเตรียมการ (Planning and Preparation)

วางแผนและเตรียมการ (Planning and Preparation) คือ ขั้นตอนแรกของการทดสอบเจาะระบบนั้น ทางผู้ว่าจ้างจะออกเอกสารรับรองการทดสอบเจาะระบบเพื่อเป็นการรับทราบว่าจะมีการทดสอบเจาะระบบจากผู้ถูกว่าจ้าง อีกทั้งยังมีการกำหนกขอบเขตของเป้าหมายในการทดสอบเจาะระบบด้วย เช่น ว่าจ้างให้ทดสอบเจาะระบบ Web Application ที่ให้บริการที่พอร์ต 80 เท่านั้นเป็นต้น

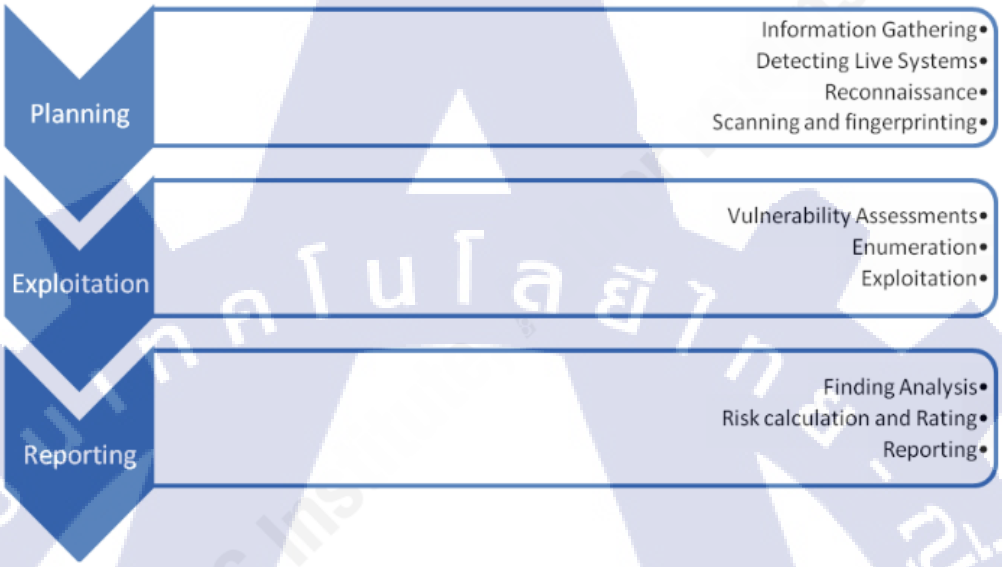
2.1.9.2 ทดสอบเจาะระบบ (Exploitation)

ทดสอบเจาะระบบ (Exploitation) เป็นขั้นตอนการทดสอบเพื่อเลียนแบบการโจมตีของ Hacker นั้นเอง ไม่ว่าจะเป็นการทำ Gaining Access, Maintaining Access เป็นต้น

2.1.9.3 การทำรายงานและสิ่งที่แนะนำให้ทำ (Reporting)

การทำรายงานและสิ่งที่แนะนำให้ทำ (Reporting) คือขั้นตอนการสรุปงานในแต่ละขั้นตอนว่าได้ข้อมูลอะไรบ้าง เช่น ระบบมีช่องโหว่ตรงไหนบ้าง ในแต่ละช่องโหว่มีความร้ายแรงขนาด

ไหน ส่งผลต่อระบบอะไรบ้าง และแต่ละช่องโหว่หรือระบบมีจุดไหนที่ควรแก้ไข และแก้ไขอย่างไรเป็นต้น ซึ่งการทำรายงานเป็นหัวใจหลักของการทดสอบเจาะระบบเลยก็ว่าได้



รูปภาพ 2.2 Method topology การทดสอบเจาะระบบ

2.1.10 PHP Hypertext Preprocessor (PHP)

รูป 2.3 รูปโลโก้ของภาษา **PHP**

PHP คือ ภาษาคอมพิวเตอร์ในลักษณะ เซิฟเวอร์-ไซต์ สคริปต์ โดยลิขสิทธิ์อยู่ในลักษณะโอเพ่นซอร์ส ภาษา PHP ใช้สำหรับจัดทำเว็บไซต์ และแสดงผลออกมาในรูปแบบ HTML โดยมีรากฐานโครงสร้างคำสั่งมาจากภาษาC Java และ Perl ซึ่งภาษา PHP นั้นง่ายต่อการเรียนรู้ ซึ่ง

เป้าหมายหลักของภาษานี้คือ ให้นักพัฒนาเว็บไซต์สามารถเขียนเว็บเพจ ที่มีความตอบโต้ได้อย่างรวดเร็ว PHP รุ่นล่าสุดคือ 5.4.0 ส่วนรุ่นพัฒนาคือ PHP 6.0.0-dev

2.1.10.1 ประวัติความเป็นมาของ PHP

PHP เกิดขึ้นในปี 1994 โดย Rasmus Lerdorf โปรแกรมเมอร์ชาวอเมริกัน ได้คิดค้นสร้างเครื่องมือที่ใช้พัฒนาเว็บส่วนตัวของเขา โดยใช้ข้อดีของภาษา C และ Perl เรียกว่า Personal Home Page และได้สร้างส่วนติดต่อกับฐานข้อมูลที่มีชื่อว่า Form Interpreter (FI) รวมทั้งสองส่วนเรียกว่า "PHP/FI" ซึ่งเป็นจุดเริ่มต้นของ PHP มีคนเข้ามาเยี่ยมชมเว็บไซต์ของเขาแล้วเกิดชอบจึงติดต่อขอโค้ดไปใช้งานบ้าง รวมถึงการนำโค้ดดังกล่าวนั้นไปพัฒนาต่อในลักษณะ Open source ภายหลังมีความนิยมขึ้นเป็นอย่างมาก ภายหลังเพียงระยะเวลาแค่ 3 ปีมีเว็บไซต์ที่มีการใช้ PHP/FI ในการติดต่อฐานข้อมูลและแสดงผลแบบไดนามิกมากกว่า 5000 เว็บไซต์ด้วยกัน

PHP 2 (ในตอนนั้นใช้ชื่อว่า PHP/FI) ในช่วงระหว่าง คริสตศักราช 1995-1997 Rasmus Lerdorf ได้ผู้ที่มาช่วยเขาพัฒนาภาษา PHP/FI เพิ่มอีก 2 คนด้วยกัน ซึ่ง 2 คนนั้นคือ Zeev Suraski และ Andi Gutmans ชาวอิสราเอล ซึ่งปรับปรุงโค้ดของ Lerdorf ใหม่โดยใช้ภาษา C++ ให้มาความสามารถในการจัดการฟอร์มข้อมูลที่ถูกสร้างมาจากภาษา HTML และสนับสนุนการติดต่อกับโปรแกรมจับการฐานข้อมูล MySQL จึงทำให้ PHP เริ่มถูกใช้มากขึ้นอย่างรวดเร็ว และเริ่มมีผู้สนับสนุนการใช้งาน PHP มากขึ้น โดยในปลายปี คริสตศักราช 1996 PHP ถูกนำไปใช้เพิ่มมากขึ้นอีกกว่า 15000 เว็บไซต์ และเพิ่มจำนวนขึ้นเรื่อย ๆ ต่อมาก็มีผู้เข้ามาร่วมช่วยพัฒนาอีก 3 คน คือ Stig Bakken รับผิดชอบความสามารถในการติดต่อ Oracle , Shane Caraveo รับผิดชอบดูแล PHP บทระบบปฏิบัติการ Window 9x/NT และ Jim Winstead รับผิดชอบการตรวจความบกพร่องต่าง ๆ และได้เปลี่ยนชื่อเป็น Professional Home Page ในเวอร์ชั่นที่ 2

PHP 3 ออกมาในช่วงระหว่างเดือน มิถุนายม คริสตศักราช 1997 – 1999 มีคุณสมบัติเด่นคือ สนับสนุนระบบปฏิบัติการทั้ง Window 95/98/ME/NT, Linux และเว็บเซิฟเวอร์ อย่าง IIS,

PWS, Apache, OmniHTTPd รวมถึงสนับสนุนฐานข้อมูลได้หลากหลายรูปแบบเช่น SQL Server, MySQL, Oracle, Informix, ODBC

PHP 4 ตั้งแต่ คริสศักราช 1999 – 2007 มีการเพิ่มความสามารถในการทำงานด้านต่าง ๆ ให้มากขึ้น โดยบริษัท Zend ซึ่งมี Zeev และ Andi Gutmans ได้ร่วมกันก่อตั้งขึ้น ในเวอร์ชั่นนี้จะเป็น compile script ซึ่งก่อนหน้านี้ จะเป็น Embed script interpreter ในปัจจุบันนี้มีคนใช้ PHP ในการพัฒนาเว็บไซต์กว่า 5,100,00 เว็บไซต์ทั่วโลก และ ผู้พัฒนาตั้งชื่อใหม่ของ PHP ใหม่ว่า “PHP : Hypertext Preprocessor” ซึ่งหมายถึงประสิทธิภาพระดับโปรเฟสเซอร์สำหรับไฮเปอร์เท็กสซ์

PHP 5 ตั้งแต่ปี คริสตศักราช 2007 – ปัจจุบัน ได้เพิ่มความสามารถในการทำงานด้านต่าง ๆ

- Object Oriented Model
- การกำหนดสโคป public / private / protected
- Exception handling
- XML and Web service
- MySQLi and SQLite
- Zend Engine 2.0

ตารางที่ 2.1 ตารางแสดงเวอร์ชั่นของภาษา PHP

Ver.	Release date	Support until	Note
1.0	8 June 1995		Officially called "Personal Home Page Tools (PHP Tools)". This is the first use of the name "PHP"
2.0	1 November 1997		Officially called "PHP/FI 2.0". This is the first release that could actually be characterised as PHP, being a standalone

			language with many features that have endured to the present day.
3.0	6 June 1998	20 October 2000	Development moves from one person to multiple developers. Zeev Suraski and Andi Gutmans rewrite the base for this version.
4.0	22 May 2000	23 January 2001	Added more advanced two-stage parse/execute tag-parsing system called the Zend engine.
4.1	10 December 2001	12 March 2002	Introduced 'superglobals' ($_GET, $_POST, $_SESSION, etc.)
4.2	22 April 2002	6 September 2002	Disabled register_globals by default. Data received over the network is not inserted directly into the global namespace anymore, closing possible security holes in applications.
4.3	27 December 2002	31 March 2005	Introduced the command-line interface (CLI), to supplement the CGI.
4.4	11 July 2005	7 August 2008	Fixed a memory corruption bug, which required breaking binary compatibility with extensions compiled against PHP version 4.3.x.
5.0	13 July 2004	5 September 2005	Zend Engine II with a new object model.
5.1	24 November 2005	24 August 2006	Performance improvements with introduction of compiler variables in re-engineered PHP

			Engine.Added PHP Data Objects (PDO) as a consistent interface for accessing databases.
5.2	2 November 2006	6 January 2011	Enabled the filter extension by default. Native JSON support.
5.3	30 June 2009	14 August 2014	Namespace support; late static bindings, jump label (limitedgoto), closures, PHP archives (phar), garbage collection for circular references, improvedWindows support, sqlite3, mysqlnd as a replacement for libmysql as underlying library for the extensions that work withMySQL, fileinfo as a replacement for mime_magic for better MIMEsupport, the Internationalization extension, and deprecation of ereg extension.
5.4	1 March 2012	1 March 2015	Trait support, short array syntax support. Removed items: register_globals, safe_mode, allow_call_time_pass_reference, session_register(), session_unregister() and session_is_registered(). Built-in web server.[52] Several improvements to existing features, performance and reduced memory requirements.
5.5	20 June 2013	20 June 2016	Support for generators, finally blocks for exceptions handling, OpCache (based on Zend Optimizer+) bundled in official distribution.
5.6	28 August 2014	28 August 2017	Constant scalar expressions,variadic functions, argument unpacking, new exponentiation operator, extensions of the usestatement for functions and constants,

			new phpdbg debugger as a SAPI module, and other smaller improvements.

ที่มา : http://en.wikipedia.org/wiki/PHP

2.1.10.2 โครงสร้างของภาษา PHP

การเขียนภาษา PHP นั้นเราสามารถเขียนแทรกไว้ในภาษา HTML หรือจะเขียนเดี่ยว ๆ เลยก็ได้ แต่เมื่อเขียนแล้วเราจะต้องทำการเซฟไฟล์ดังกล่าวเป็นสกุล .php การเขียน php นั้นมีรูปแบบการเขียนอยู่หลายแบบดังนี้

2.1.10.3 ประโยชน์และข้อดีของภาษา PHP

- ไม่เสียค่าใช้จ่าย PHP เป็นภาษาที่ไม่มีลิขสิทธิ์เพราะถือว่าเป็น Open source ตัวหนึ่ง ทำให้สามารถนำมาใช้งาน ได้โดยไม่เสียค่าใช้จ่ายใด ๆ
- ทำงานได้หลากหลายระบบปฏิบัติการ ภาษา PHP สามารถทำงานอยู่บนระบบปฏิบัติการได้หลากหลาย ทำให้ไม่จำเป็นต้องกังวลเรื่องของระบบปฏิบัติการ ทำให้ไม่จำเป็นต้องกังวลในเวลาออกแบบระบบ ช่วยให้การออกแบบระบบนั้นทำได้ง่ายยิ่งขึ้น
- เรียนรู้และใช้งานง่าย ภาษา PHP นั้นพัฒนามาจาก ภาษา C , Java , Perl ซึ่งเป็นภาษาพื้นฐานในการเขียนโปรแกรมอยู่แล้ว โปรแกรมเมอร์จึงสามารถเรียนรู้ภาษา PHP ได้อย่างรวดเร็ว รวมถึงการใช้งานที่เพียงเขียนแทรกเอาไว้ในภาษา HTML ได้ และความสามารถทำงานร่วมกับภาษา HTML นี้เองทำให้ผู้พัฒนาสามารถสร้างเว็บไซต์ที่มีลูกเล่น หรือระบบการใช้งานต่าง ๆ ได้ง่ายดายขึ้น
- การทำงานร่วมกับเซิฟเวอร์ ภาษา PHP เป็นภาษาที่ทำงานอยู่ในฝั่งเซิฟเวอร์ ทำให้การทำงานร่วมกับเซิฟเวอร์ต่าง ๆ จุดแข็งที่สำคัญอย่างหนึ่งของภาษา PHP คือ ความสามารถในการเชื่อมต่อกับฐานข้อมูลได้อย่างง่ายดาย ซึ่งความสามารถในการเชื่อมต่อกับเซิฟเวอร์ดังกล่าวนั้น ทำให้ผู้พัฒนานั้นสามารถทำเว็บไซต์ที่ไม่ใช่เพียงแค่แสดงข้อความเท่านั้น เว็บไซต์จึงกลายเป็นส่วนหนึ่งของระบบ ที่สามารถรับข้อมูลจากผู้ใช้มาเก็บไว้ในฐานข้อมูลที่ต้องการ รวมถึงการประมวล และ แสดงผลบนหน้าเว็บไซต์ ภาษา PHP จึงนิบ

ว่าเป็นภาษาที่มีประสิทธิภาพสูงภาษาหนึ่ง ที่สามารถพัฒนาเว็บแอพลิเคชั่นตั้งแต่ขนาดเล็กไปจนถึงขนาดใหญ่ได้

- ได้รับความนิยมสูง และ มีการพัฒนาอย่างต่อเนื่อง โดย PHP เป็นภาษาที่มีคนนิยมใช้อย่างมาก ทำให้เกิด โค้ดสำเร็จรูป ที่มีผู้พัฒนาเขียนขึ้นเพื่อนใช้งานในรูปแบบต่าง ๆ อยู่เป็นจำนวนมาก รวมถึง การพัฒนาความสามารถของภาษาที่เป็นไปอย่างรวดเร็ว ทำให้ PHP เติบโตขึ้นอย่างรวดเร็ว และมีความสามารถต่าง ๆ ที่เพิ่มเติม รวมถึงการที่ได้รับความนิยม หากผู้ใช้พบปัญหาอะไรในการทำงานกับภาษา PHP ก็ย่อมสามารถหาทางแก้ไขปัญญาได้อย่างง่ายดาย เพราะมีกลุ่มคนจำนวนมากที่ใช้ภาษา PHP นี้อยู่ รวมถึงคู่มือ และ โค้ดตัวอย่างจำนวนมากที่สามารถหามาศึกษาใช้งานอย่างง่ายดาย รวมถึงชุดโค้ดสำเร็จรูปที่กล่าวไปในข้างต้น ทำให้ผู้พัฒนาไม่จำเป็นต้องเขียนโค้ดทั้งหมด จึงช่วยลดเวลาในการพัฒนาเว็บไซต์ลงได้

2.1.10.4 ข้อเสียของภาษา PHP

เนื่องจากเป็นภาษาที่มีการพัฒนาอย่างรวดเร็ว ทำให้ผู้พัฒนาจำเป็นต้องคอยติดตามข่าวสารของ ภาษา PHP เวอร์ชั่นใหม่ ๆ อยู่สม่ำเสมอ เพราะในเวอร์ชั่นใหม่ อาจมีการนำฟังก์ชั่นของภาษา ออกไป หรือปรับเปลี่ยนรูปแบบการเขียนไป ทำให้โค้ดที่เขียนไว้นั้นใช้งานไม่ได้

2.1.10.5 ได้รับความนิยมสูง และ มีการพัฒนาอย่างต่อเนื่อง

เนื่องจาก PHP เป็นภาษาที่มีคนนิยมใช้อย่างมาก ทำให้เกิด โค้ดสำเร็จรูป ที่มีผู้พัฒนาเขียนขึ้น เพื่อนใช้งานในรูปแบบต่าง ๆ อยู่เป็นจำนวนมาก รวมถึง การพัฒนาความสามารถของภาษาที่ เป็นไปอย่างรวดเร็ว ทำให้ PHP เติบโตขึ้นอย่างรวดเร็ว และมีความสามารถต่าง ๆ ที่เพิ่มเติม รวมถึงการที่ได้รับความนิยม หากผู้ใช้พบปัญหาอะไรในการทำงานกับภาษา PHP ก็ย่อมสามารถหาทางแก้ไขปัญญาได้อย่างง่ายดาย เพราะมีกลุ่มคนจำนวนมากที่ใช้ภาษา PHP นี้อยู่ รวมถึงคู่มือ และ โค้ดตัวอย่างจำนวนมากที่สามารถหามาศึกษาใช้งานอย่างง่ายดาย รวมถึงชุด

โค้ดสำเร็จรูปที่กล่าวไปในข้างต้น ทำให้ผู้พัฒนาไม่จำเป็นต้องเขียนโค้ดทั้งหมด จึงช่วยลดเวลาในการพัฒนาเว็บไซต์ลงได้

2.1.11 Hypertext Markup Language (HTML)

เป็นภาษามาร์กอัปหลักในปัจจุบันที่ใช้ในการสร้างเว็บเพจ หรือข้อมูลอื่นที่เรียกดูผ่านทางเว็บเบราว์เซอร์ ซึ่งตัวโค้ดจะแสดงโครงสร้างของข้อมูล ในการแสดง หัวข้อ ลิงค์ ย่อหน้า รายการ รวมถึงการสร้างแบบฟอร์ม เชื่อมโยงภาพหรือวิดิโอด้วยโครงสร้างของโค้ดเอชทีเอ็มแอลจะอยู่ภายในลักษณ์ภายในวงเล็บสามเหลี่ยม

2.1.11.1 ประวัติความเป็นมาของภาษา HTML

วัตถุประสงค์หลักของ HTML ถูกเสนอโดยนาย ทิม เบอร์เนอร์ส-ลี (Tim Berners-Lee) แห่งศูนย์ปฏิบัติการวิจัยทางอนุภาคฟิสิกส์ของยุโรป (CERN) ซึ่งตั้งอยู่ที่กรุงเจนีวา สวิตเซอร์แลนด์ได้กำหนดไว้ว่า เพื่อสร้างสื่อที่นักวิทยาศาสตร์สามารถจะเผยแพร่ผลงาน และใช้อ้างอิงได้ตลอด 24 ชั่วโมง หรือ เพื่อสร้างภาษาคอมพิวเตอร์ที่รองรับภาษาท้องถิ่น ที่ไม่ขึ้นกับระบบของเครื่องคอมพิวเตอร์ (Platform) หรือระบบเครือข่ายใด ๆ และด้วยวัตถุประสงค์ข้างต้น ภาษา HTML จึงถูกใช้งานอย่างแพร่หลายในสังคมของนักวิทยาศาสตร์และกำหนดให้เครื่องมือที่ใช้เขียน เป็นโปรแกรม Text editor ทั่ว ๆ ไป สำหรับภาษา HTML ในอินเตอร์เน็ตได้รับการพัฒนาอย่างต่อเนื่อง เพื่อให้คนทุก ๆ ชาติบนโลกสามาเข้าถึง เผยแพร่ และอ้างอิงวิทยาการความรู้ได้ ด้วยการเชื่อมโยงไปมาแบบ Hyperlink อาจจะด้วยตัวอักษร หรือรูปภาพ โดยอาจเชื่อมโยงเฉพาะภายในเอกสารนั้น หรือ เชื่อมโยงข้ามไปยังเอกสารอื่น ๆ ได้

ภาษา HTML มีต้นแบบมาจากภาษา SGML (Standard Generalized Markup language) ซึ่งเป็นภาษาที่ใช้ได้เฉพาะกับประเภทของคอมพิวเตอร์ และสิ่งที่ HTML รับมาจาก SGML คือ การประกาศค่า และการกำหนดรูปแบบเอกสาร (Document Type Definition -DTD)

สิ่งที่ทำให้ ภาษา HTML ได้รับความนิยมอย่างมาก และรวดเร็วก็คือ HTML รวมถึงโปรโตคอล HTTP (Hyper Text Transfer Protocol) เป็นภาษาที่ใช้สื่อสารกันได้ทั่วโลก โดยที่ตัวภาษาและโปรโตคอลไม่ขึ้นกับระบบเครือข่าย และประเภทของคอมพิวเตอร์ ซึ่งมีความ

หลากหลาย อันเนื่องมาจากเทคโนโลยี และประเภทการใช้งาน เป็นผลให้เอกสารที่เขียนโดย HTML สามารถถ่ายโอนได้อย่างกว้างขวาง ทั้งในรูปแบบของอักษร ภาพ และเสียง

2.1.11.2 HTML เวอร์ชั่นต่าง ๆ

HTML เวอร์ชั่นแรก ๆ ยังไม่สมบูรณ์ดีนัก จนกระทั่งในปี 1994 HTML 2.0 จึงได้รับการยอมรับเป็นมาตรฐานที่สมบูรณ์ แต่อย่างไรก็ดี Netscape และ Microsoft ต่างก็เพิ่มคำสั่งใหม่ ๆ ลงในโปรแกรมของตนเอง เพื่อให้ผู้ออกแบบเพจสามารถใช้ฟังก์ชั่นอื่นนอกเหนือไปจาก HTML2.0

ต่อมา W3C ได้พัฒนามาตรฐาน HTML 3.0 ขึ้นมา แต่ปรากฏว่ามาตรฐานใหม่นี้ ไม่เป็นที่ยอมรับของ Netscape , Microsoft และบริษัทอื่น ๆ โดยแต่ละบริษัทต่าง ๆ ก็พยายามให้มาตราฐานใหม่มีฟังก์ชั่นที่ตนเองต้องการ จนในที่สุด W3C จึงต้องกลับไปแก้ไขใหม่ และก็คือ HTML 3.2

HTML 3.2 เป็นมาตรฐานในปัจจุบันของ W3C โปรแกรมเบราว์เซอร์ เกือบทั้งหมดได้รับการพัฒนาให้สามารถทำงานตามคำสั่งที่กำหนดในมาตรฐานของ HTML 3.2 ซึ่ง HTML 3.2 เพิ่งจะได้รับการยอมรับเป็นมาตรฐานเมื่อ มกราคม คศ.1997 แต่กระนั้นก็ดียังมีขีดกำจัดบางประการที่นักออกแบบเพจต้องการที่จะให้ HTML 3.2 มีความสามารถเพิ่มมากขึ้น นักออกแบบจำนวนมากนิยมใช้คำสั่งใหม่ ๆ ที่ยังไม่ถือว่าเป็นมาตรฐาน ทั้ง ๆ ที่รู้ว่า การทำเช่นนี้ จะทำให้ต้องเสียเวลาในการเปลี่ยนเบราว์เซอร์ใช้หลาย ๆ ตัว แต่ก็เป็นการท้าทายความสามารถของนักออกแบบ ความต้องการของนักออกแบบที่เพิ่มมากขึ้น ทำให้องค์กร W3C ตกลงใจใช้ HTML 4.0 ฉบับร่างขึ้น เมื่อ 8 กรกฎาคม 1997 ทุก ๆ บริษัทก็พยายามปรับปรุงโปรแกรมเบราว์เซอร์ของตน ให้สามารถใช้คำสั่งใหม่ ๆ ตามมาตรฐาน HTML 4.0 ความสามารถใหม่ที่เพิ่มขึ้นใน HTML 4.0 จะช่วยให้ผู้ออกแบบเพจ สามารถควบคุมรูปแบบเอกสาร และ รูปภาพได้ดีขึ้น แต่ทั้งนี้โปรแกรมเบราว์เซอร์นั้นจะต้องสนับสนุนฟังชั่นของ HTML 4.0 ด้วย

คุณสมบัติบางประการของ HTML 4.0 ได้มีการนำไปใช้ใน Netscape และ Microsoft ก่อนที่จะมีการพัฒนา HTML 4.0 เสียอีก หลังจากนั้นจึงเพิ่มความสามารถนี้ลงในมาตรฐาน

HTML 4.0 แต่ก็มีคุณสมบัติบางประการของ HTML 4.0 ที่ไม่เคยมีอยู่ในเบราว์เซอร์ใด ๆ มาก่อนเลยก็คือ ความสามารถในการจัดการกับ Object Model โดย HTML 4.0 ถูกแบ่งออกเป็น 3 ประเภทได้แก่

- แบบค่อยเป็นค่อยไป (Transitional / Loose HTML4.0) เป็นเอกสารที่สร้างด้วย HTML 4.0 โดยใช้ร่วมกับคำสั่งใน HTML 3.2 เพื่อให้ เอกสารที่สร้างขึ้นมีรูปแบบ และใช้งานได้ตามจริง แม้ว่าจะใช้โปรแกรมเบราว์เซอร์ ระบบเครือข่าย และปรเภท คอมพิวเตอร์ที่หลากหลายก็ตาม
- แบบเฟรมเซต (Freameset HTML 4.0) เป็นเอกสารที่รวมเอาประเภท Transitional เข้ากับ Tag ประเภท เฟรม ได้แก่ frame , frameset , noframes และ iframe ซึ่งเป็น tag ใหม่ในเวอร์ชั่น 4.0 นี้
- แบบเคร่งครัด (Strict HTML 4.0) เป็นเอกสาร Hypertext ที่เขียนด้วยภาษา HTML 4.0 ตามมาตรฐานอย่างเคร่งครัด tag ใดที่คณะกรรมการชุดนี้นิยามว่า ล้ำสมัย (Deprecate) หรือ ให้เลิกใช้ (Obsolete) ก็จะไม่ใช้คำสั่งนั้นในการเขียนเอกสาร ซึ่งในความเป็นจริงขณะนี้ ยังไม่มีโปรแกรมเบราว์เซอร์ใดสนับสนุน HTML4.0 อย่างเคร่งครัด แต่คาดว่าในอนาคตอันใกล้ น่าจะมีความเป็นไปได้

2.1.11.3 โครงสร้างของภาษา HTML

ในการเขียนภาษา HTML นั้น จะมีรูปแบบโครงสร้างการเขียนแบ่งออกเป็น 3 ส่วนคือ

2.1.11.3.1 ส่วนประกาศ

เป็นส่วนที่กำหนดให้เบราว์เซอร์ทราบว่า นี้คือภาษา HTML และจะต้องทำการแปรผลอย่างไรมีคำสั่งคู่เดียวคือ <html> และ </html> ปรากฏที่หัวและท้ายของไฟล์

2.1.11.3.2 ส่วนหัวเรื่อง

เป็นส่วนที่แสดงผลข้อความบนไตเติ้ล (Title) ของเบราว์เซอร์ และอาจมีคำสั่งสำหรับกำหนดรายละเอียดด้านเทคนิคอื่น ๆ แรกอยู่ระหว่างคำสั่ง <head> และ </head>

2.1.11.3.3 ส่วนเนื้อหา

เป็นส่วนที่มีความซับซ้อนมากที่สุด และสามารถใส่เทคนิคลูกเล่นเพื่อดึงความสนใจจากผู้เข้าชมเว็บเพจได้มาก ความแตกต่างระหว่างเว็บไซต์ต่าง ๆ แสดงความมีฝีมือของผู้จัดทำ ศิลปะในการออกแบบจะอยู่ในส่วนนี้ทั้งหมด ซึ่งจะแทรกอยู่ระหว่างคำสั่ง <body> และ </body>

โครงสร้างพื้นฐานของภาษาคอมพิวเตอร์เป็นส่วนที่สำคัญที่สุดของการเขียนภาษาคอมพิวเตอร์โดยทั่วไปแล้ว มันจะต้องถูกเขียนขึ้นทุกครั้ง ภาษา HTML ก็เหมือนกับภาษาคอมพิวเตอร์ทั่ว ๆ ไป ที่มีโครงสร้างพื้นฐานเฉพาะของมัน คำสั่ง HTML ส่วนมากจะถูกกำหนดอยู่ในเครื่องหมาย < และ > ซึ่งถูกเรียกว่า Tag ซึ่ง Tag

2.1.11.4 คำสั่งในโครงสร้างพื้นฐาน

2.1.11.4.1 Title

Title (ชื่อหัวเรื่อง) จะถูกกำหนดอยู่ภายในส่วนของ <head> ข้อมูลที่ถูกเขียนอยู่ภายในจะถูกแสดงออกมาให้เห็นที่บนบาร์ของ เบราว์เซอร์

<head>

<title> ชื่อหัวเรื่อง</title>

</head>

2.1.11.4.2 ข้อมูลที่ต้องการแสดงผล

ข้อมูลที่ต้องการแสดงผล จะเป็นส่วนแสดงให้เราเห็นไม่ว่าจะเป็นตัวอักษร รูปภาพ ตาราง ฯลฯ (คำสั่งที่ต้องการแสดงผล จะอยู่ระหว่าง tag body ทั้งหมด) ซึ่งถูกกำหนดอยู่ระหว่างคำสั่ง

<body> จนถึงคำสั่ง </body>

2.1.11.4.3 Comment Tag

Comment Tag (คำอธิบาย) เป็นคำสั่งที่ใช้ในการอธิบายอยู่ภายใน HTML จะไม่มีการแสดงผลออกมาที่เบราว์เซอร์ จะมีประโยชน์สำหรับผู้จะทำการแก้ไขโปรแกรมในภายหลัง

<!-ใส่ข้อความใด ๆ ก็ได้เพื่อนใช้ในการอธิบาย->

2.1.11.4.4 BR

BR (คำสั่งขึ้นบรรทัดใหม่) เป็นคำสั่งที่ใช้กำหนดให้ข้อความที่เราพิมพ์ลงไปในเอกสาร ขึ้นบรรทัดใหม่ได้ตามที่เราต้องการ เพราะ ถ้าเราไม่ใช้คำสั่ง สั่งให้เอกสารแสดงผลขึ้นบรรทัดใหม่ การแสดงผลของข้อความจะแสดงต่อกันไปเรื่อย ๆ แม้ว่าเราจะพิมพ์ขึ้นบรรทัดใหม่ก็ตาม

ข้อความ.....
 ข้อความ.....

2.1.11.4.5 P (คำสั่งการย่อหน้าใหม่)

P (คำสั่งการย่อหน้าใหม่) มีลักษณะคล้ายคำสั่ง
 แต่คำสั่งนี้จะมีการเว้นบรรทัดว่างให้บรรทัดหนึ่ง เพราะบางครั้งเราต้องการเว้นบรรทักว่าง หนึ่งบรรทัด แต่โปรแกรมเบราว์เซอร์จะไม่เข้าใจการพิมพ์บรรทัดเปล่า

 ข้อความ ..... หรือ

2.1.11.4.6 HR (เส้นคั่นบรรทัด)

HR (เส้นคั่นบรรทัด) เป็นคำสั่งที่ใช้แบ่งข้อความของจอภาพให้เป็นส่วน ๆ <hr>

2.1.11.5 ประโยชน์ และ ข้อดีของภาษา HTML

2.1.11.5.1 ไม่จำกัดประเภทของคอมพิวเตอร์

กล่าวคือ ไม่ว่าคอมพิวเตอร์จะเป็นระบบปฏิบัติการใด ๆ ก็ตาม ก็สามารถเข้าถึงเอกสาร HTML ได้ ทำให้สามารถเผยแพร่เอกสาร HTML ได้อย่างง่ายดาย เพราะทุกคนทั่วโลกสามารถเข้าถึงเอกสารนี้ได้ ไม่ถูกจำกัดไว้ด้วยระบบปฏิบัติการ รวมถึง ประเภทของโปรแกรมเรียกดูเว็บไซต์หรือ เบราว์เซอร์ (Browser) ไม่เว้นแม้แต่ระบบปฏิบัติการประเภท Unix ที่นิยมใช้งานผ่าน Command line ก็สามารถเข้าถึงเอกสาร HTML ได้เช่นกัน

2.1.11.5.2 สามารถอ่านเข้าใจได้

ภาษา HTML คำสั่งจะมีความหมายที่ตรงตัวกับหน้าที่ของคำสั่งนั้น ๆ อย่างชัดเจน รวมถึงโครงสร้างของภาษาที่ง่าย ทำให้การพัฒนาเว็บไซต์ด้วยภาษา HTML นั้น โปรแกรมเมอร์ผู้อ่านมาอ่านเอกสาร HTML ที่มีอยู่แล้ว ก็สามารถเข้าใจถึงโครงสร้างของเว็บไซต์นั้นได้อย่างรวดเร็ว รวมถึงการที่รูปแบบของไวยากรณ์ที่ตายตัว ทำให้เป็นภาษาที่ง่ายต่อการศึกษา

2.1.11.5.3 ไม่จำกัดเครื่องมือในการพัฒนา

ภาษา HTML นั้นไม่ต้องการการประมวลผลก่อนจึงจะแสดงผลได้ ภาษา HTML จึงไม่ถูกจำกัดเครื่องมือในการพัฒนา ผู้ใช้งานอาจจะใช้โปรแกรมเขียนเอกสารทั่วไปอย่าง NotePad หรือ WordPad หรือแม้กระทั่งโปรแกรมจัดทำเอกสารอย่าง Microsoft word ในการพัฒนาเว็บไซต์ด้วยภาษา HTML แต่ถึงกระนั้น การพัฒนาภาษา HTML ก็เปรียบเสมือนการเขียนโปรแกรมด้วยโปรแกรมอื่น ๆ เช่นกัน การพัฒนาเว็บไซต์ผ่านเครื่องมือ เขียนโปรแกรมต่าง ๆ จึงจะช่วยอำนวยความสะดวกในการเขียนแก่ผู้ใช้งานได้ดีกว่าการใช้โปรแกรมจัดทำเอกสารทั่วไปอย่างแน่นอน

2.1.11.5.4 เป็นภาษามาตรฐานเปิด

หมายถึง ภาษาที่มีผู้เข้าร่วมการพัฒนาอย่างเสรี ทำให้อนาคตภาษา HTML ก็จะมีความสามารถต่าง ๆ เพิ่มขึ้น รวมถึง ไม่เสียค่าบริการในการใช้งานภาษา HTML ในการนำมาพัฒนาเว็บไซต์ต่าง ๆ ดังนั้นกล่าวได้ว่า อนาคตภาษา HTML จะมีลูกเล่นและความสามารถต่าง ๆ อีกมาที่จะให้ผู้พัฒนามาใช้กัน

2.1.11.5.5 Multimedia

ภาษา HTML เวอร์ชั่นล่าสุด (HTML 5) มีความสามารถที่เป็นเอกลักษณ์หลักของเวอร์ชั่นนี้นั้นคือ การทำงานร่วมกับสื่อมัลติมีเดียประเภทต่าง ๆ ได้ ทำสื่อบนเว็บไซต์สามารถเข้าถึงได้ง่ายขึ้นกว่าสมัยก่อนหน้านี้ที่จำเป็นต้องใช้โปรแกรมเสริมในเบราว์เซอร์เพื่อเข้าถึงสื่อมัลติมีเดียนั้น ๆ

2.1.11.6 ข้อเสียของภาษา HTML

เครื่องมือช่วยในการเขียนของภาษา HTML มักจะมีการ สร้างโค้ดที่ไม่จำเป็นออกมาเป็นจำนวนมาก รวมถึงการจัดรูปแบบของภาษาที่ทำให้อ่านยาก ซึ่ง การสร้างโค้ดที่ไม่จำเป็นจำนวนมากนี้ ส่งผลให้ไฟล์ HTML ดังกล่าวมีขนาดใหญ่ และใช้เวลานานในการเรียกใช้งาน การเขียนภาษา HTML ให้มีประสิทธิภาพแก่การใช้งานที่สุด คือ การเขียนโค้ดด้วยตัวเอง อาจใช้เครื่องมือที่สนับสนุนการเขียนโค้ดแต่ไม่ใช่เครื่องมือสร้างโค้ด ดังนั้น ผู้เขียนจึงจำเป็นต้องทำการศึกษาภาษา HTML ให้เข้าใจเสียก่อนจะเริ่มพัฒนาเว็บไซต์ด้วยภาษา HTML เพราะนอกจากเราจะสามารถลดโค้ดที่ไม่จำเป็นออกไปได้แล้ว เรายังเข้าถึงและดึงความสามารถของภาษาออกมาได้อย่างเต็มที่กว่าการใช้โปรแกรมดังกล่าว

2.2 เทคโนโลยีที่ใช้ในการปฏิบัติงาน

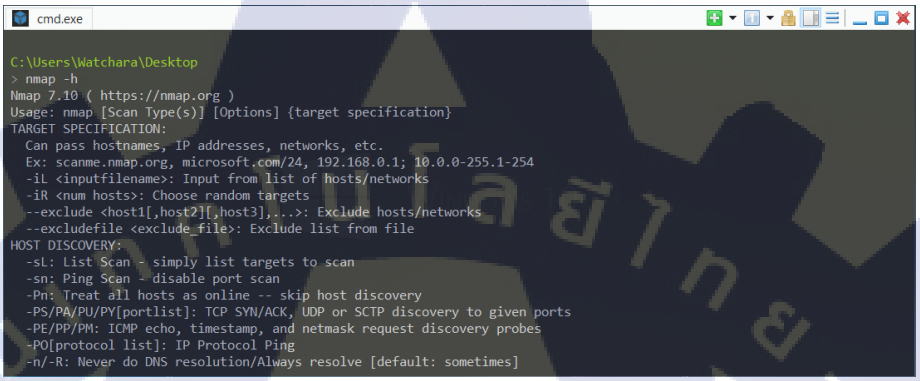
2.2.1 Kali linux

Kali linux เป็นแพลทฟอร์มรันบนระบบปฏิบัติการ Debian Jesse สำหรับใช้เจาะระบบคอมพิวเตอร์เพื่อตรวจหาช่องโหว่โดยเฉพาะ ซึ่งมาพร้อมกับชุดทดสอบเจาะระบบมากกว่า 100 รายการ รวมทั้งมีระบบการวิเคราะห์เชิงสถิติ การแฮ็ค และวิศวกรรมย้อนกลับ (Reverse Engineering) ในเวอร์ชัน 2.0 ล่าสุดนี้ ได้ทำการออกแบบอินเตอร์เฟสใหม่ จัดกลุ่มเครื่องมือ และเมนูแสดงผลต่างๆเพื่อให้ใช้งานได้สะดวก

รูปที่ 2.4 เครื่องมือภายใน Kali Linux

2.2.2 Pentest Box

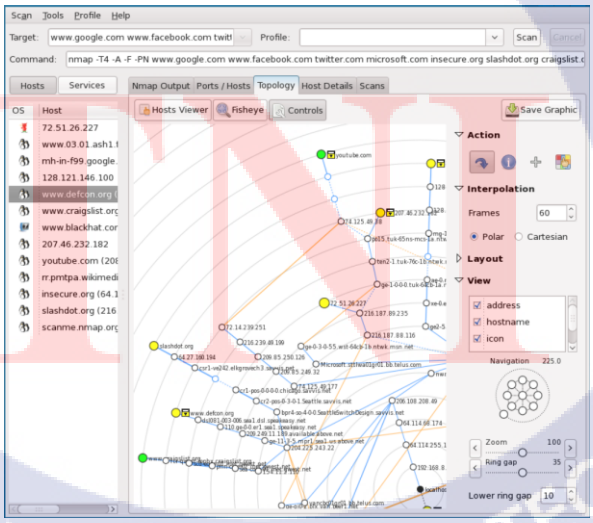
Pentest Box เป็นเครื่องสำหรับใช้ทดสอบเจาะระบบแบบ Portable สำหรับระบบปฏิบัติการ Windows ซึ่งพร้อมใช้งานได้ทันทีโดยไม่จำเป็นต้องลง Driver หรือรันผ่าน Virtual Machine แต่อย่างใด มาพร้อมกับเครื่องมือสำหรับเจาะระบบแบบครบวงจร



รูปที่ 2.5 หน้าตาของโปรแกรม Pentest Box

2.2.3 Nmap (Network Mapper)

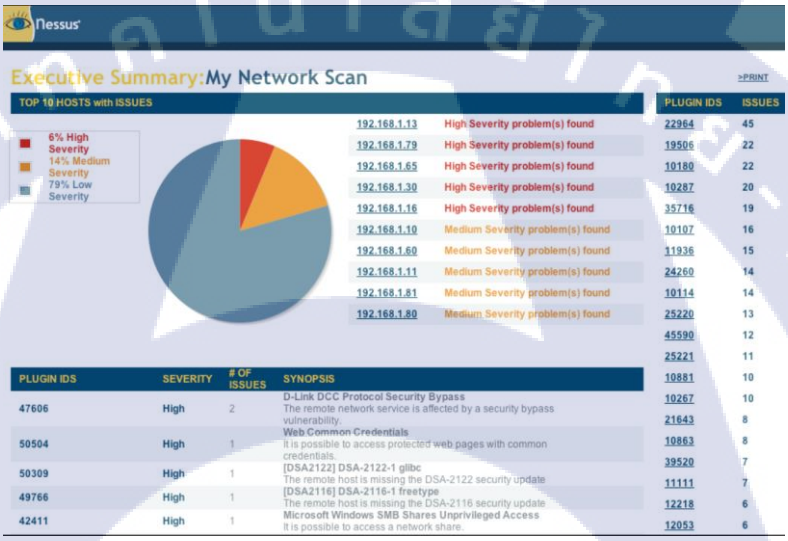
Nmap (Network Mapper) เป็นโปรแกรมที่ใช้ในการสแกนตรวจสอบเครื่อง ต่างจากการใช้ IP Address หรือ ใช้ URLก็ได้ เพื่อที่จะหาข้อมูลเกี่ยวกับเครื่องนั้นๆ เช่น ดูว่าเปิด Port ไหนไว้บ้าง หรือดูว่า ใช้ OS แบบไหน มีการเปิด firewall หรือไม่ เป็นต้น



รูปที่ 2.6 หน้าตาโปรแกรมแบบ GUI ของ Nmap

2.2.4 Nessus

Nessus เป็นโปรแกรม Network Security ที่ไว้สำหรับสแกนเครื่องคอมพิวเตอร์ลูกข่ายผ่านระบบเครือข่าย สำหรับเพื่อช่วยตรวจสอบหาช่องโหว่ของเครื่องคอมพิวเตอร์ลูกข่ายแล้วรายงานให้ผู้ดูแลระบบเครือข่ายทราบ สำหรับโปรแกรม Nessus นี้ดาวน์โหลดได้ฟรีไม่ต้องเสียค่าลิขสิทธิ์ รองรับการทำงานได้ทั้งบนระบบปฏิบัติการ Unix และ Windows และการแสดงผลจะสามารถดูเป็นกราฟิกโหมดได้ โปรแกรมนี้ถือว่าเป็นเครื่องมือดูแล Network Security ที่มีประสิทธิภาพมากโดยมีการอัพเดตฐานข้อมูล อย่างสม่ำเสมอ



รูปที่ 2.7 หน้าตาการใช้งานของโปรแกรม Nessus

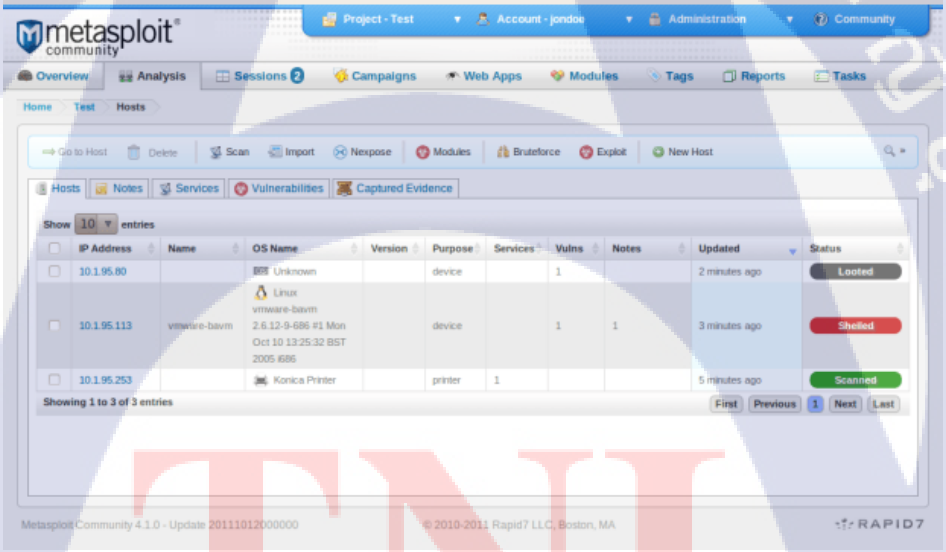
2.2.5 Netcat

Netcat เป็นโปรแกรม Network Security ที่ได้ชื่อว่าเป็น “Swiss Army Knife” (การรวมชุดเครื่องมืออเนกประสงค์มีดพับของสวิสสำหรับนักเดินป่าที่จะหยิบใช้ก็ง่าย) โดย Netcat ใช้ดักจับแพ็กเกตในเครือข่ายคอมพิวเตอร์และสร้างแพ็กเกตเพื่อส่งเข้าไปในเครือข่ายคอมพิวเตอร์ โปรแกรม Netcat รองรับการใช้งานบนระบบปฏิบัติการตระลยูนิกซ์ และระบบปฏิบัติการวินโดวส์ เป็นโปรแกรมฟรีอีกตัวที่น่าใช้

รูปที่ 2.8 โลโก้ NETCAT

2.2.6 Metasploit

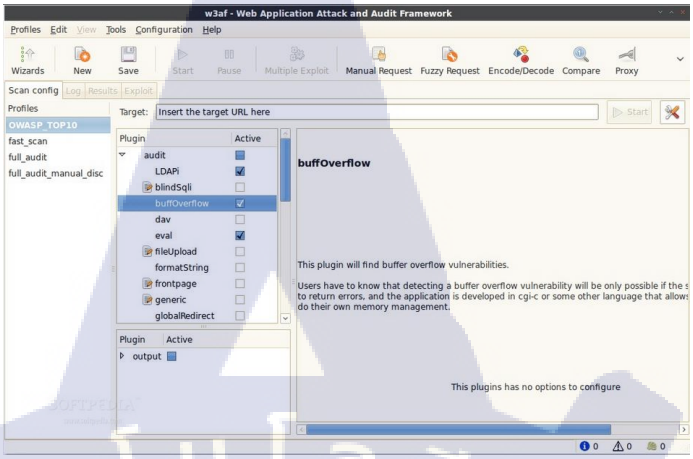
Metasploit คือ Project Open Source เกี่ยวกับ Computer Securityใช้ในการทำทดสอบการเจาะระบบ(Penetration Testing)โดย Project นี้ถูกริเริ่มโดย HD Moore ในปี 2003



รูปที่ 2.9 หน้าตาของโปรแกรม **Metasploit**

2.2.7 W3af

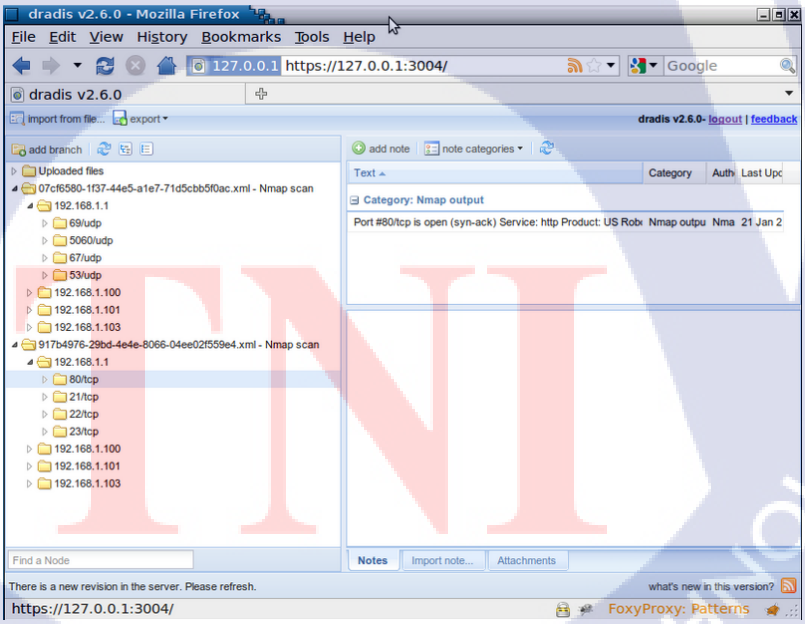
W3af เป็น ตัวสแกนและเจาะช่องโหว่เว็บแอพพลิเคชันแบบ Open-source ซึ่งจะให้ข้อมูลเกี่ยวกับช่องโหว่ที่ตรวจพบเจอและวิธีการอุดช่องโหว่เบื้อง ต้น โปรแกรมนี้ถูกพัฒนาโดยภาษา Python และใช้งานได้ผ่านทั้ง GUI และ Command Line



รูปที่ 2.10 หน้าตาโปรแกรม W3af

2.2.8 Dradis

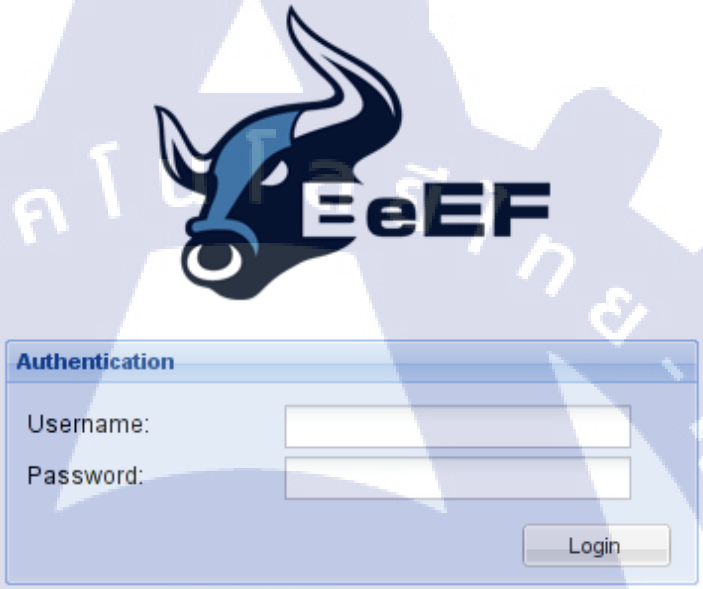
Dradis คือ เครื่องมือสำหรับแชร์ข้อมูลระหว่างทำ Pentest ในกรณีที่มีผู้ทดสอบระบบหลายคนทำงานโปรเจ็คท์เดียวกันพร้อมๆกัน Tool ตัวนี้จะทำหน้าที่เก็บและแชร์ข้อมูลทั้งหมดแบบรวมศูนย์เพื่อป้องกันการทดสอบ ระบบหรือรายงานผลซ้ำซ้อนกัน รองรับการติดตั้งบน BackTrack, Ubuntu, FreeBSD, Mac OS X, Apache และ Metasploit's Cygwin



รูปที่ 2.11 หน้าตาโปรแกรม dradis

2.2.9 BeEF

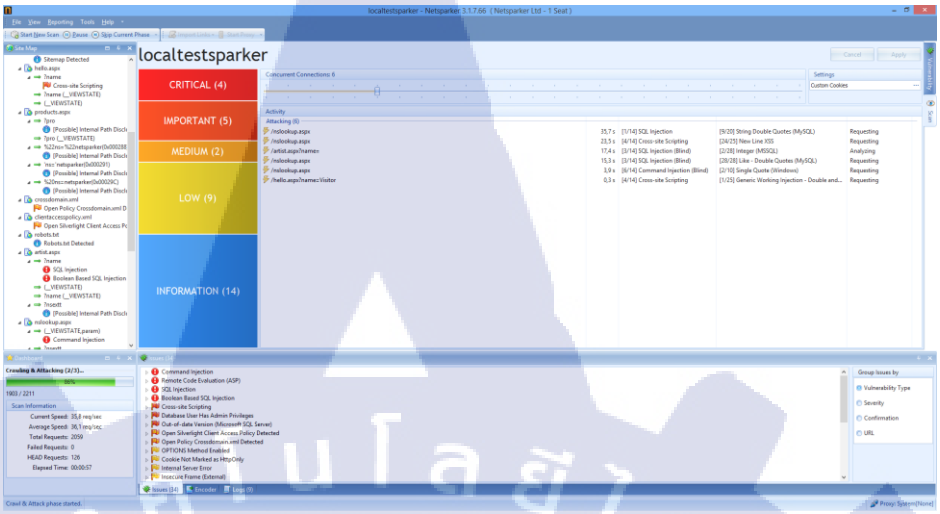
BeEF หรือ Browser Exploitation Framework เป็น Tool สำหรับทดลองเจาะระบบซึ่งโฟกัสที่เว็บเบราเซอร์โดยเฉพาะ BeEF จะทำการดูข้อมูลการทำ Hardenring และ Client ในระบบ แล้วเจาะช่องโหว่ผ่านทางบริบทของเว็บเบราเซอร์



รูปที่ 2.12 หน้าตาอินเตอร์เฟส BeEF

2.2.10 Netsparker

Netsparker คือ เครื่องมือสแกนเว็บแอพพลิเคชันแบบ False-Positive-Free ที่ช่วยค้นหาช่องโหว่หรือข้อผิดพลาดทั้งหมดบนเว็บแอพพลิเคชัน ไม่ว่าจะเป็น SQL Injection หรือ XSS รวมทั้งสามารถทำรายงานสรุปผลพร้อมระบุรายละเอียดและวิธีอุดช่องโหว่ที่เข้า ใจได้ง่าย



รูปที่ 2.13 หน้าตาการใช้งาน Netsparker

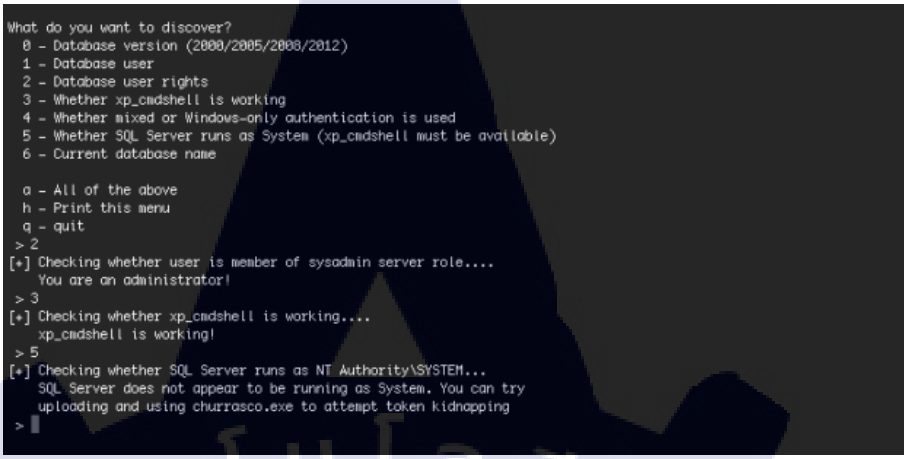
2.2.11 Social-Engineer Toolkit

Social-Engineer Toolkit เป็นเครื่องมือสำหรับเจาะช่องโหว่แบบ Open-source โดยเน้นที่การทำ Social-Engineering ซึ่งพัฒนาโดยใช้ภาษา Python

รูปที่ 2.14 หน้าตาการใช้งาน Social-Engineer Toolkit

2.2.12 SQLNINJA

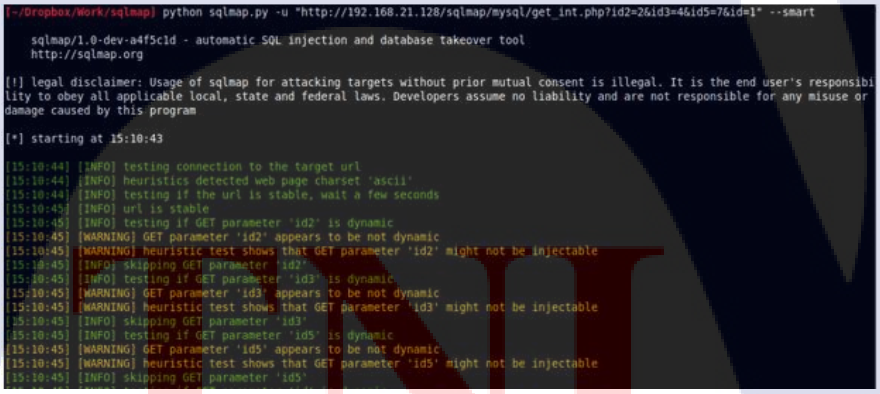
SQLNINJA คือ เครื่องมือเจาะระบบเว็บแอพพลิเคชันที่ใช้งานร่วมกับระบบฐานข้อมูล MsSQL โดยเน้นที่การโจมตีแบบ SQL Injection ถูกพัฒนาโดยใช้ภาษา Perl และรองรับการทำงานบนระบบปฏิบัติการ UNIX-based เช่น Linux, FreeBSD, Mac OS X และ iOS



รูปที่ 2.15 หน้าตาการใช้งาน SQLNINJA

2.2.13 Sqlmap

Sqlmap คือ เครื่องมือสำหรับทดสอบการเจาะระบบแบบ Open-source ซึ่งโฟกัสที่การค้นหาช่องโหว่และโจมตี Database Server โดยใช้ SQL Injection เป็นหลัก ซึ่งรองรับระบบฐานข้อมูลแบบ MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase และ SAP MaxDB



รูปที่ 2.16 หน้าตาการใช้งาน Sqlmap

2.2.14 Mozilla Firefox

Mozilla Firefox คือ โปรแกรมเว็บเบราเซอร์ (Web Browser) ที่ใช้สำหรับเปิดเว็บไซต์โดยมีทีม Mozilla เป็นผู้พัฒนา และยังเป็น (Open source browser) ที่สามารถให้โปรแกรมเมอร์ทั่วโลกพัฒนา

โปรแกรมเสริมเพื่อใช้ร่วมกับ Mozilla Firefox ได้อีกด้วย ปัจจุบันเป็นที่นิยมของผู้ใช้งาน Internet เป็นอย่างมาก

2.2.15 Burp Suite

Burp Suite เป็นโปรแกรม สำหรับการทดสอบของเว็บแอปพลิเคชัน โดยคุณลักษณะ หลักของโปรแกรมนี้คือส่วนของProxy web นันคือสามารถดักจับการส่ง Request จาก Clientและ Response ข้อมูลตอบกลับไปยัง Client โดยสามารถเลือกกระทำการใดๆกับข้อมูลนั้นได้

2.2.16 VMware

VMware เป็นโปรแกรมซึ่งใช้ในการสร้าง Virtual Machine (VM) หรือเครื่องคอมพิวเตอร์เสมือน คือ เป็นการสร้างเครื่องคอมพิวเตอร์ขึ้นมาอีกเครื่อง ภายในเครื่องcomputer ดังนั้นจึงทำให้สามารถทดลองใช้งาน OS หรือโปรแกรมอื่นๆที่สนใจโดยไม่ต้องทำการ format เครื่องหรือใช้ PC อีกเครื่องหนึ่งมาเพื่อทดสอบระบบที่เราสนใจ

บทที่ 3 แผนงานการปฏิบัติงานและขั้นตอนการดำเนินงาน

3.1 แผนการปฏิบัติงาน

จากการที่นักศึกษาได้เข้าปฏิบัติสหกิจศึกษาที่บริษัท ไซเบอร์ตรอน จำกัด นักศึกษาได้รับมอบหมายให้จัดทำการ ทดสอบเจาะระบบ Cyberrange หรือ ระบบจำลองยุทธ์ทางด้านไซเบอร์ และได้ทำการออกแบบโจทย์ที่ใช้กับการฝึกจำลองยุทธ์ทางด้านไซเบอร์ของ Cyberrange เป็นหลัก รวมทั้งได้รับมอบหมายเพิ่มเติม ตัวอย่างเช่น การจัดเตรียมโจทย์งานแข่งขันทางด้านไซเบอร์ Army Cyber Contest 2016, NAVY Cyber Contest 2016, Cyber Operations Contest 2016, Cyber Defence Exercise CDX 2016 เป็นต้น และยังได้ร่วมเป็นผู้ช่วยในการสอนที่ บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด

ตารางที่ 3.1 ตารางงานการปฏิบัติงานสหกิจศึกษา

หัวข้องาน	**สัปดาห์ที่**															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ศึกษาระบบงาน																
วางแผนการทำงาน																
วางแผนการทำโครงงาน																
ทำงานทั่วไป																
วางแผนการทดสอบระบบ																
ทดสอบเจาะระบบ																
จัดงานแข่ง Cyber Operations																
ทำ report การทดสอบระบบ																
จัดงานแข่ง Army Cyber																
ทำเอกสารโครงงาน																
จัดงานแข่ง Navy Cyber																
นำเสนองานกับบริษัท ฯ																
นำเสนองานกับคณะ ฯ																

3.2 รายละเอียดงานที่ได้รับมอบหมาย

3.2.1 งานที่ได้รับหมอบหมายในการจัดเตรียมสถานที่แข่งขัน

จัดเตรียมระบบในการแข่งขันด้าน security ที่ผู้เล่นจะต้องทำการเจาะระบบอีกฝ่าย หรือ ทำการป้องกันระบบของตัวเอง และทำการวาง server ติดตั้งตัวระบบที่ใช้ในการแข่งขัน โดยตลอดระยะเวลาในการศึกษาสหกิจได้ทำการจัดแข่งขันทั้งหมดสี่สถานที่ ได้แก่ งาน Army Cyber Contest 2016, NAVY Cyber Contest 2016, Cyber Operations Contest 2016 และ Cyber Defense Exercise CDX 2016

3.2.2 งานที่ได้รับหมอบหมายในส่วนของการทำการทดสอบเจาะรบบจำลองยุทธ

ทำการศึกษาการใช้งานระบบ Cyberrange มีการใช้งานอย่างไร ตั้งค่าระบบอย่างไร ศึกษาช่องโหว่ต่างๆ ทั้งในส่วนของ OWAPS(Open Web Application Security Project) Top ten ช่องโหว่ 10 ประเภทที่เกี่ยวกับเว็บที่ได้รับความนิยมมากที่สุด และสุดท้ายทำการทดสอบระบบจำลองยุทธ หรือระบบ Cyberrnge ว่ามีช่องโหว่อะไรเกิดขึ้นบ้างและทำการแก้ไขช่องโหว่นั้นๆไม่ให้เกิดขึ้นต่อตัวระบบหรือผู้ใช้งานเป็นต้น

3.2.3 งานที่ได้รับหมอบหมายอื่นๆ

3.2.1.1 จัดเตรียมโจทย์ที่ใช้ในการแข่งขัน

จัดเตรียมโจทย์ที่ใช้กับระบบ Cyberrange หรือระบบจำลองยุทธ์ทางด้านไซเบอร์ โดยในการเตรียมโจทย์จะใช้เวลาประมาณ 2 เดือน ตัวโจทย์จะเป็นการฝึกการเจาะระบบและการป้องกัน ของระบบ Cyberrange หรือระบบจำลองยุทธ์ทางด้านไซเบอร์ โจทย์ที่นักศึกษาได้ทำขึ้นได้แก่ การเดาพาสเวิดหรือ การ Bruteforce Password การใช้งาน searchsploit ในการค้นหาช่องโหว่ การใช้ msfconsole ในการเจาะระบบหรือการยิง exploits และการใช้ tools ในการ scan หา service ของเครื่องเป้าหมาย เป็นต้น โดยตัวโจทย์สามารถนำมาจัดแข่งขันของของกองทัพได้

3.3 ขั้นตอนการดำเนินงาน

3.3.1 การศึกษาเกี่ยวกับช่องโหว่

ในการทดสอบระบบหรือการทำ Pentest จะต้องทราบรายละเอียด ของแต่ละช่องโหว่เป็นอย่างไร มีลักษณะอย่างไร โดยที่ได้ศึกษามีดังนี้

3.3.1.1 Injection

Injection คือ ข้อผิดพลาดที่ถูกเจาะได้ ตัวอย่างเช่น SQL OS และ LDAP การเจาะจะเกิดขึ้นเมื่อข้อมูลที่ไม่น่าเชื่อถือได้ถูกส่งเข้าไปประมวลผล ข้อมูลของผู้โจมตีที่ไม่เป็นมิตรสามารถทำให้การประมวลผลข้อมูลที่ไม่ได้อ้างถึง หรือเข้าถึงข้อมูลที่ต้องได้รับสิทธิก่อน

3.3.1.2 Broken Authentication and Session Management

Broken Authentication and Session Management ฟังก์ชันแอปพลิเคชันเกี่ยวข้องกับการตรวจสอบสิทธิและการจัดการ session ที่พัฒนามาอย่างไม่ถูกต้อง จะทำให้ผู้โจมตีสามารถยึดรหัสผ่าน คีย์ หรือ session tokens หรือหลอกระบบมีข้อมูลส่วนตัวของผู้ใช้คนอื่น

3.3.1.3 Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) เกิดขึ้นเมื่อแอปพลิเคชันได้รับข้อมูลที่ไม่น่าเชื่อถือและส่งข้อมูลนั้นโดยความถูกต้องอย่างถูกต้อง XSS ทำให้ผู้โจมตีสามารถให้สคริปทำงานใน Browser ของเหยื่อซึ่งถูกยึด session ผู้ใช้โดยเปลี่ยนแปลงหน้าเว็บเพจ หรือส่งผู้ใช้งานไปที่เว็บไซต์หลอกลวง

3.3.1.4 Insecure Direct Object References

Insecure Direct Object References หมายถึงเมื่อผู้พัฒนาเปิดเผยแหล่งอ้างอิงไปถึงวัตถุที่อยู่ภายใน เช่น ไฟล์ นามสังเคราะห์ หรือฐานข้อมูล โดยไม่ได้มีการตรวจสอบสิทธิการเข้าถึงหรือการป้องกัน

3.3.1.5 Security Misconfiguration

Security Misconfiguration คือ ความปลอดภัยที่ดีนั้นต้องมีการตั้งค่าที่ปลอดภัยในทุก ๆ ส่วนของเว็บเซิร์ฟเวอร์

3.3.1.6 Sensitive Data Expose

Sensitive Data Expose คือ เว็บแอปพลิเคชันไม่มีการป้องกันข้อมูลที่ควรปกป้องเช่น เลขบัตรเครดิต รหัสประจำตัวผู้เสียภาษี และใบรับรองการมีสิทธิ ผู้โจมตีสามารถขโมยหรือเปลี่ยนแปลงข้อมูลที่ไม่ได้ป้องกันอย่างเพียงพอเพื่อการโกงบัตรเครดิต การขโมยความเป็นตัวตน หรืออาชญากรรมอื่น ๆ

3.3.1.7 Missing Function Level Access Control

Missing Function Level Access Control คือ เว็บแอปพลิเคชันส่วนใหญ่ตรวจสอบความถูกต้องในการจัดลำดับระดับของฟังก์ชันก่อนที่จะทำให้สามารถใช้งานได้ในส่วนติดต่อผู้ใช้ ถึงแม้ว่าแอปพลิเคชันต้องดำเนินการในการเข้าถึงเซิร์ฟเวอร์ในแต่ละฟังก์ชันแตกต่างระดับกัน ทำให้ผู้โจมตีสามารถร้องขอการใช้ฟังก์ชันที่ไม่ได้อยู่ในระดับที่ได้รับสิทธิแล้ว

3.3.1.8 Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF) คือ การโจมตีที่ Browser ที่กำลังเข้าสู่ระบบด้วยการส่งการร้องขอ HTTP ปลอมไปที่ Browser ของเหยื่อเพื่อให้ได้ข้อมูลเกี่ยวกับคุกกี้ และข้อมูลการมีสิทธิเข้าใช้อื่น ๆ ทำให้ผู้โจมตีสามารถสร้างการเข้าสู่ระบบในเว็บแอปพลิเคชันได้

3.3.1.9 Using Components with Known Vulnerabilities

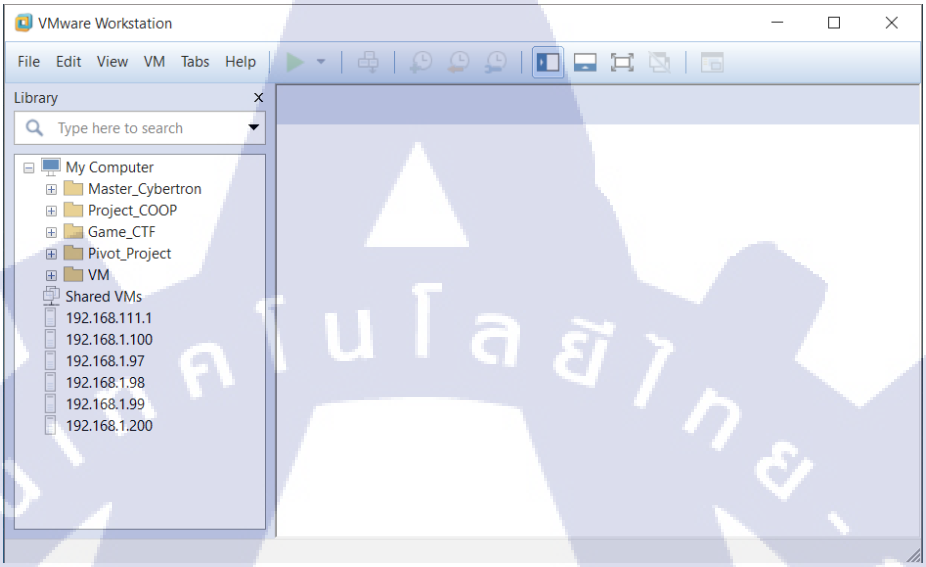
Using Components with Known Vulnerabilities องค์ประกอบเช่น Libraries, Framework และโมดูลซอร์ฟแวร์อื่น ๆ ที่ดำเนินการอยู่บนเอกสิทธิ์เต็ม ถ้าองค์ประกอบนั้นมีช่องโหว่จะทำให้ผู้โจมตีสามารถยึดเซิร์ฟเวอร์นั้นได้

3.3.1.10 Unvalidated Redirects and Forwards

Unvalidated Redirects and Forwards คือ เว็บแอปพลิเคชันจะ redirect ผู้ใช้งานไปสู่หน้าอื่นหรือเว็บไซต์อื่นด้วยข้อมูลที่ไม่น่าเชื่อถือเพื่อตัดสินใจไปสู่เพจปลายทาง โดยไม่ได้ตรวจสอบ ซึ่งจะทำให้ผู้โจมตีสามารถ redirect เหยื่อไปที่หน้าเว็บไซต์ปลอม หรือไปเพจที่ไม่มีสิทธิใช้

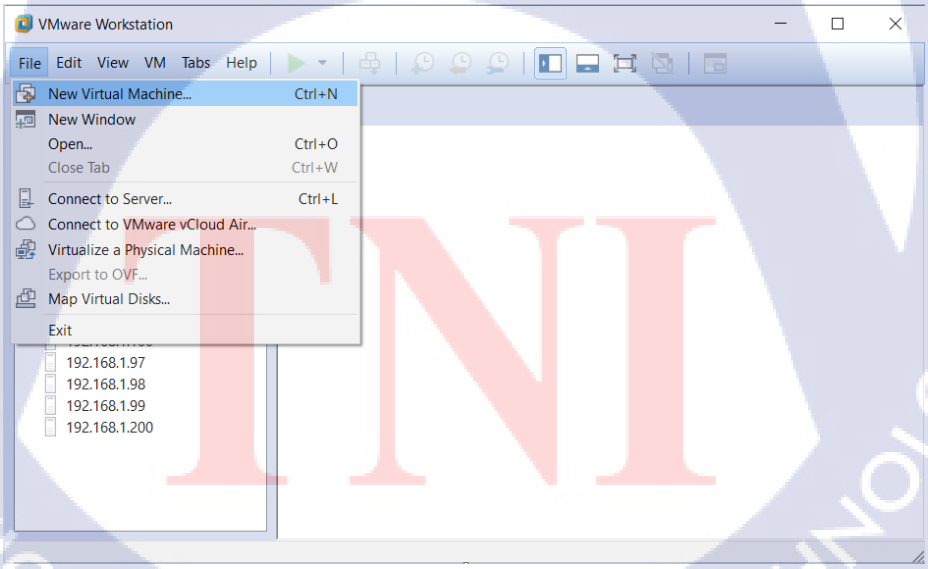
3.3.2 การติดตั้ง Kali linux ลงใน VMware Workstation

3.3.2.1 เปิดโปรแกรม VMWare Workstation



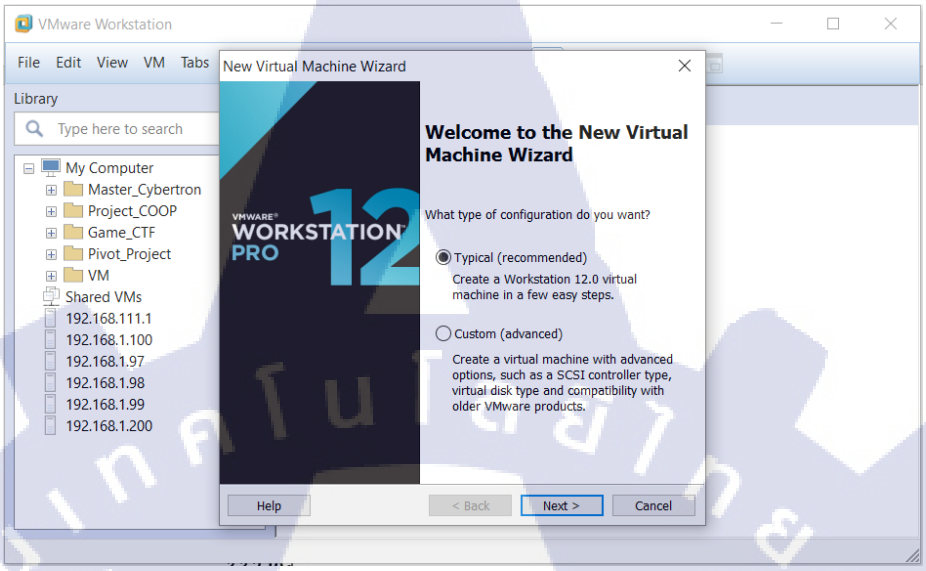
รูปที่ 3.1 หน้าตาโปรแกรม VMWare Workstation

3.3.2.2 คลิ๊กเลือก File > New Virtual Machine



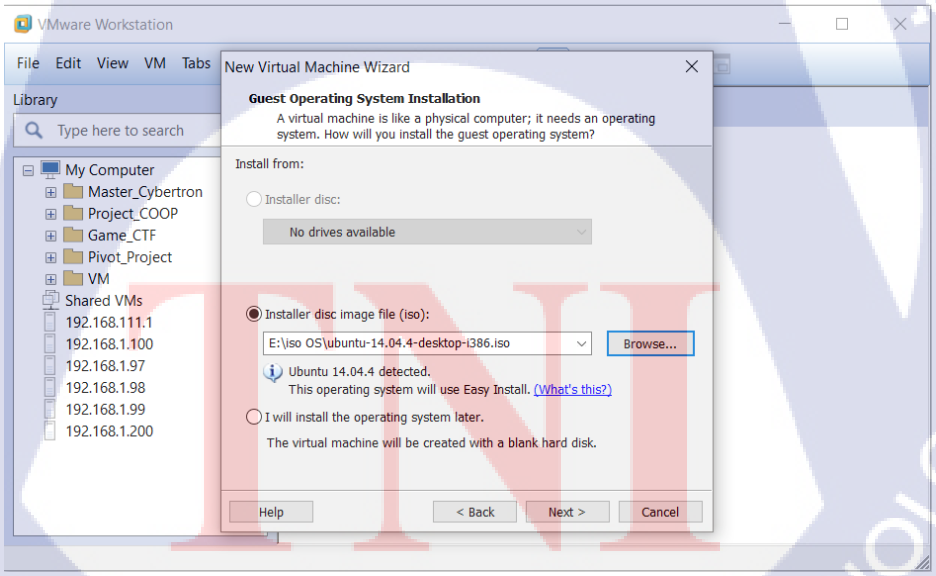
รูปที่ 3.2 การเพิ่มเครื่องลงใน VMWare Workstation

3.3.2.3 เลือก Typical และคลิ๊ก Next



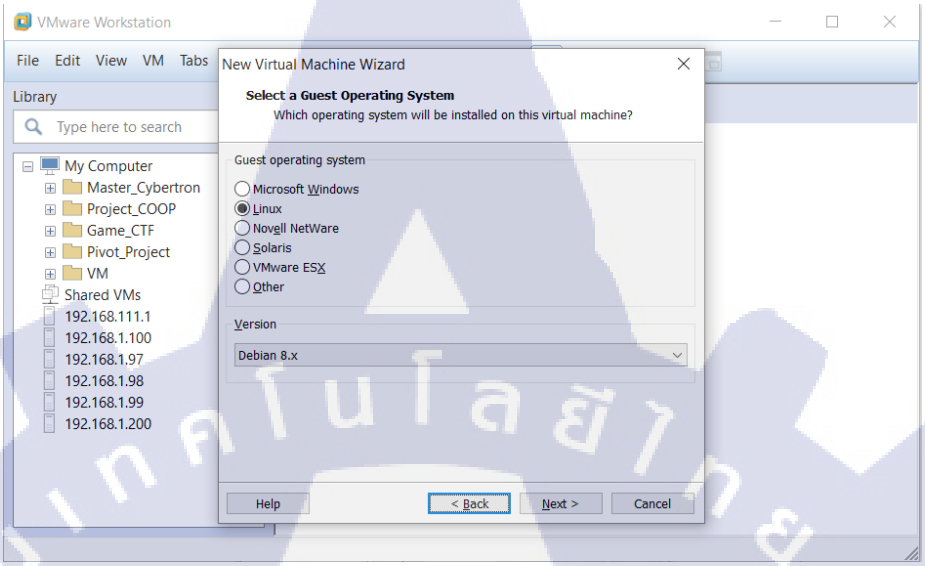
รูปที่ 3.3 เลือกประเภทการติดตั้งใน VMWare Workstation

3.3.2.4 เลือก Installer disc image file (iso) และ Browse ไฟล์ image ของ Kali Linux



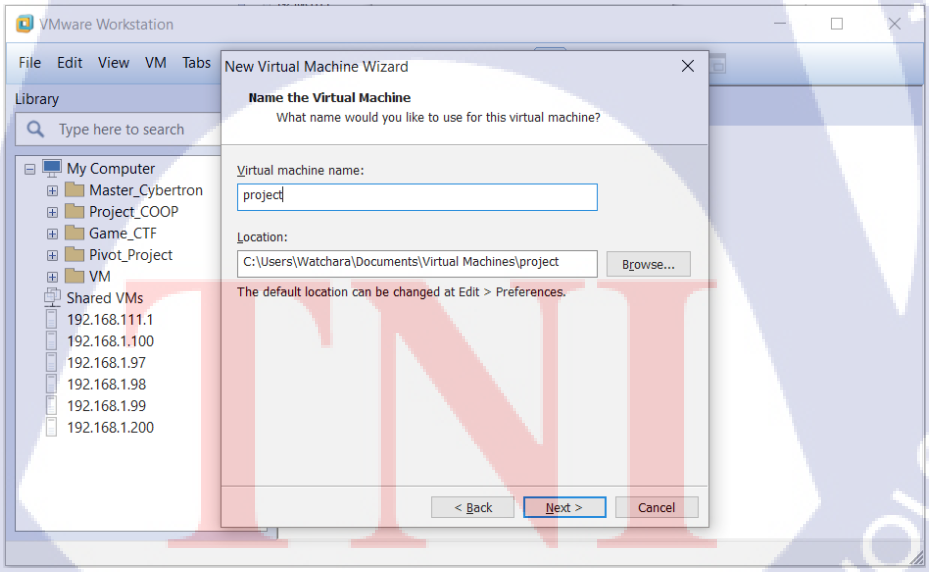
รูปที่ 3.4 เลือกไฟล์ ISO ที่จะติดตั้ง

3.3.2.5 เลือก Linux และ Version Debian



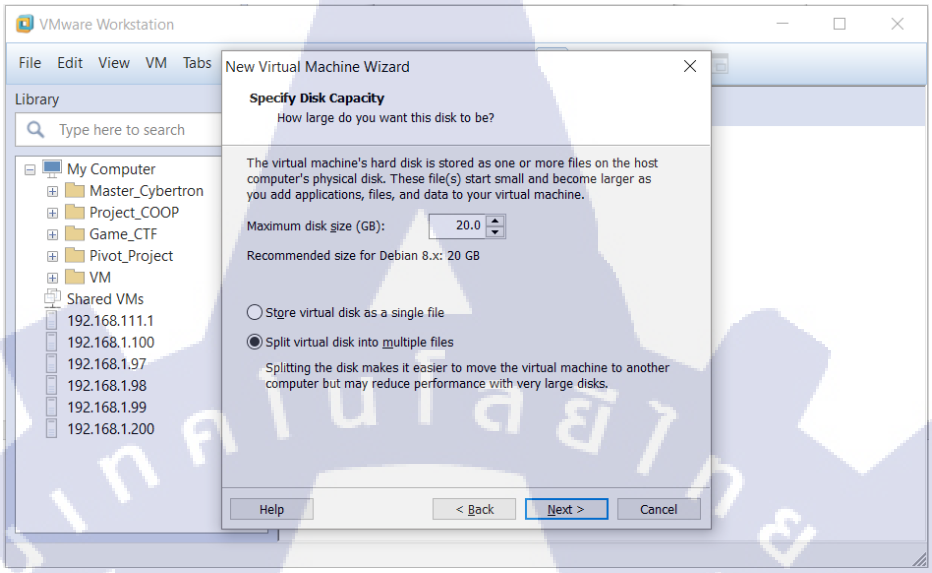
รูปที่ 3.5 เลือกประเภทของ operating

3.3.2.6 ใส่ชื่อที่ต้องการ กด Next



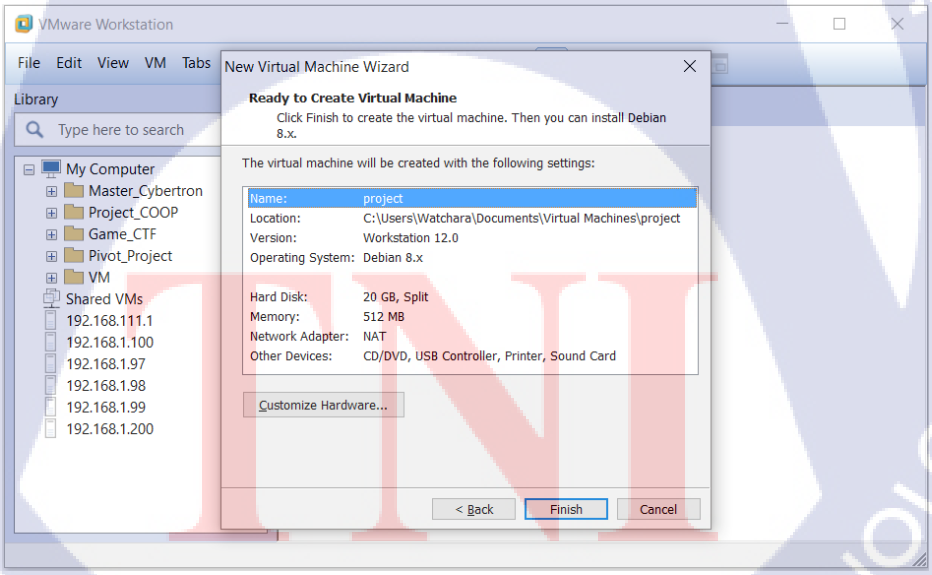
รูปที่ 3.6 ใส่ชื่อที่ต้องการ

3.3.2.7 กำหนดขนาด Disk กด Next



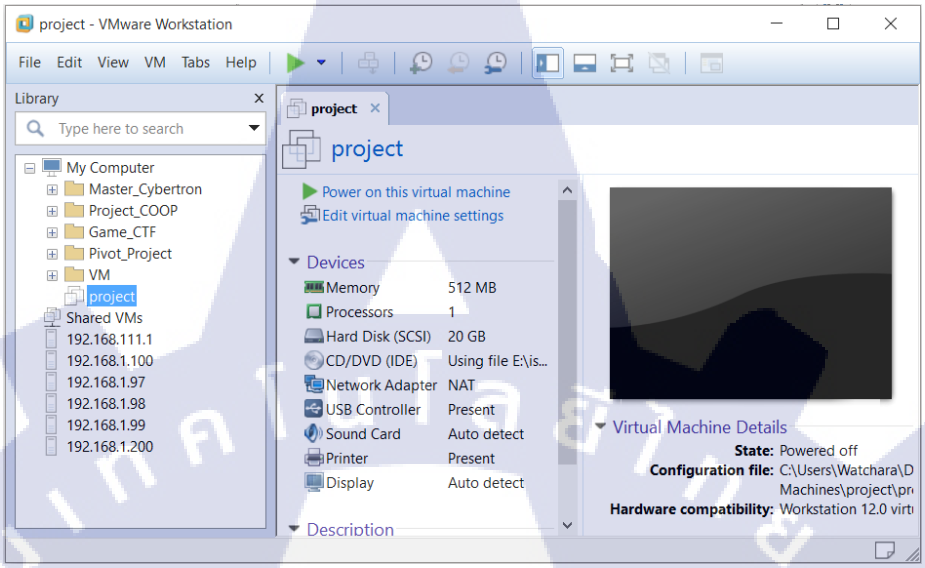
รูปที่ 3.7 กำหนดขนาดของพื้นที่ที่ต้องการ

3.3.2.8 กด Finish



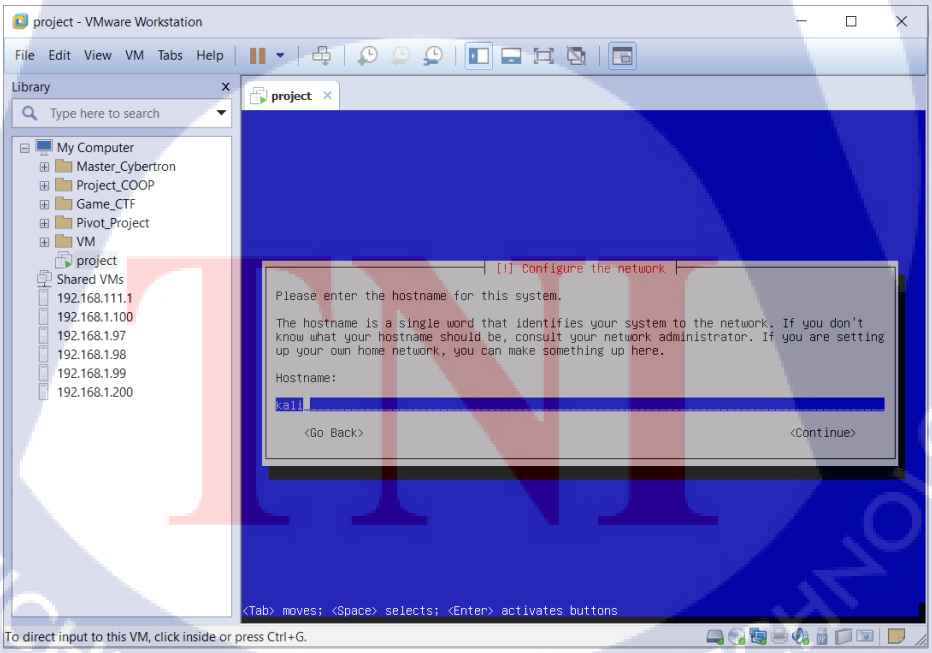
รูปที่ 3.8 การติดตั้งเสร็จสมบูรณ์

3.3.2.9 กด Power On



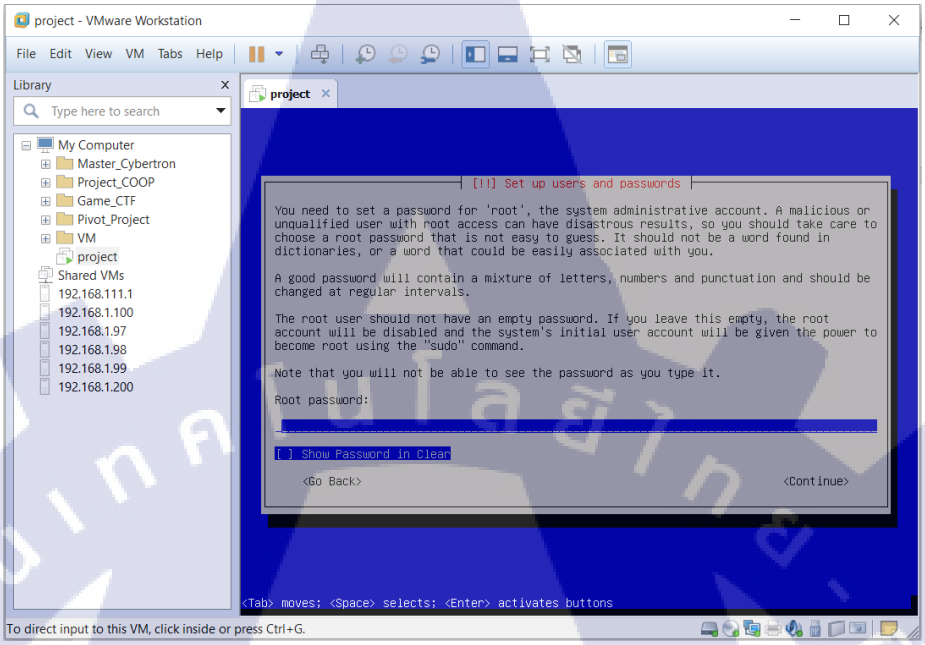
รูปที่ 3.9 หน้าตาที่ติดตั้งเสร็จแล้ว

3.3.2.10 ใส่ชื่อที่ต้องลงไป แล้วกด Continue

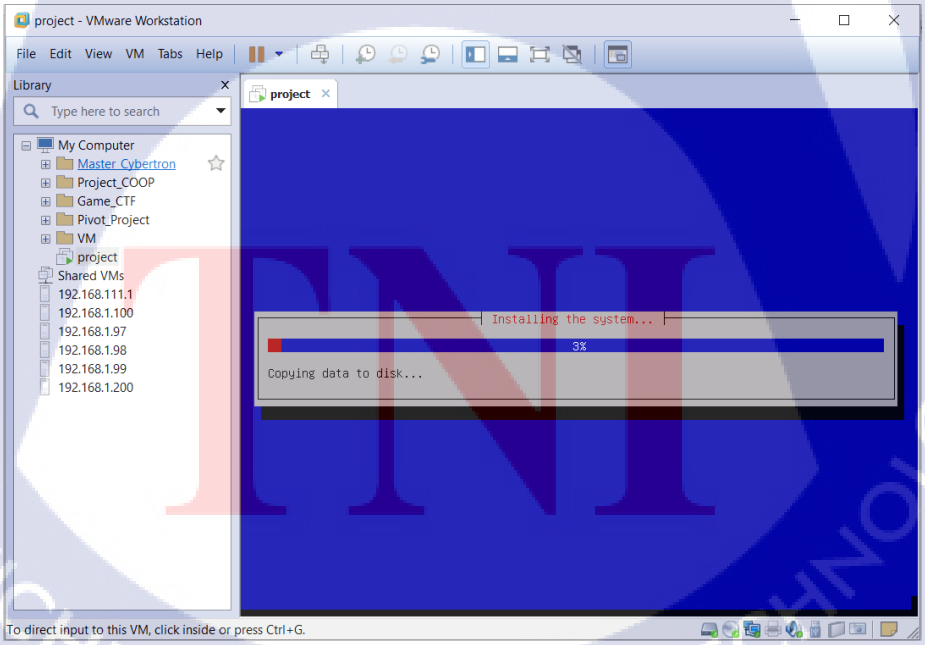


รูปที่ 3.10 ใส่ชื่อในการติดตั้ง kali

3.3.2.11 กำหนด Pass และกด Continue



รูปที่ 3.11 ใส่ password ในการติดตั้ง kali



รูปที่ 3.12 หน้าตารอโหลดติดตั้ง kali

3.3.2.12 ทดสอบการใช้งาน ใส่ User Pass

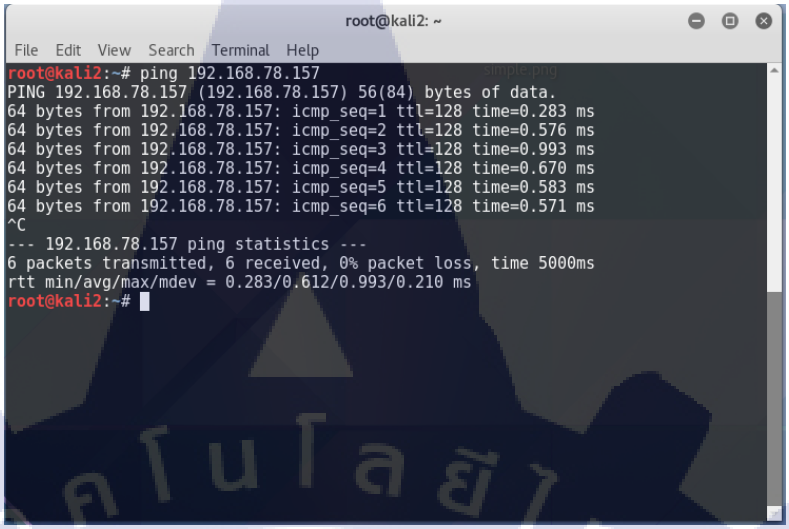
รูปที่ 3.13 หน้าตาการเข้าสู่ระบบเมื่อติดตั้ง kali เสร็จเรียบร้อยแล้ว

3.3.3 ขั้นตอนการดำเนินงานที่ปฏิบัติ

ขั้นตอนของการทำโปรเจ็คที่นักศึกษาได้รับหมอบหมายจากทางผู้ดูแลได้แบ่งออกเป็น 3 กระบวนการดังนี้ โดยนักศึกษาจะแสดงตัวอย่างการทำ penetration test หรือ การทดสอบเจาะระบบว่ามีการทำแต่ละขั้นตอนอย่างไรบ้างตั้งแต่การวางแผน จนถึงการทำรายงานออกมา แต่เนื่องจากข้อมูลของการทำ penetration test หรือการเจาะระบบ ที่บริษัท Cyber Range เป็นข้อมูลที่ไม่สามารถเอาออกมา นึกศึกษาจึงทำการทดลองเพื่อเป็นตัวอย่างออกมาโดยมีกระบวนการตามที่ได้กล่าวไว้

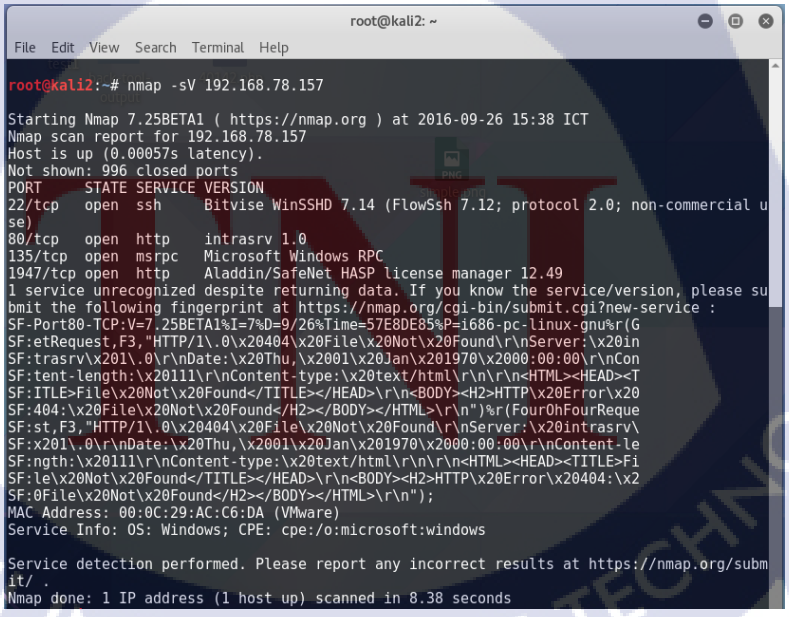
3.3.3.1 Planning (วางแผน)

โดย Scope ของงานมี 1 หมายเลข ip ที่ให้เราทำการทดสอบนั้นคือ 192.168.78.157 และทำการ check ว่าเครื่องนั้นมีอยู่หรือไม่ โดยการใช้คำสั่ง ping 192.168.78.157



รูปที่ 3.14 การใช้ ping ในการตรวจสอบเป้าหมาย

ต่อมาทำการ scan service เพื่อตรวจสอบว่าเครื่องเป้าหมายนั้นใช้ service อะไรบ้างและตรวจสอบช่องโหว่ของ service นั้นๆ ว่าสามารถทำอะไรได้บ้างในขั้นตอนต่อไป โดยในการตรวจสอบ service เบื้องต้นนั้นจะใช้เครื่องมือที่เรียกว่า nmap โดยใช้คำสั่งในการ scan ดังนี้ nmap -sV 192.168.78.157 จะเห็นได้ว่ามี port 22 80 135 1947 เปิดอยู่ โดยแต่ละ port ก็จะมีเวอร์ชั่น ของโปรแกรมนั้นอยู่ ซึ่งจะนำมาใช้ในขั้นตอนต่อไป

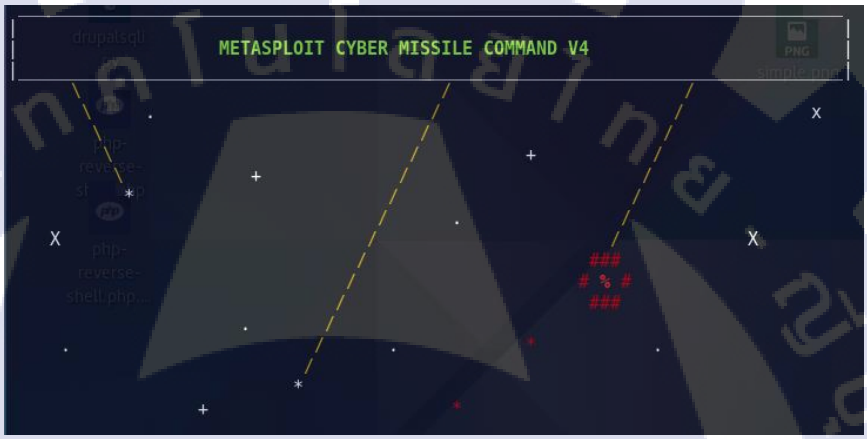


รูปที่ 3.15 การใช้ nmap ในการตรวจสอบ service

3.3.3.2 Exploit (เจาะระบบ)

ในขั้นตอนนี้คือการทดสอบเพื่อเลียนแบบการโจมตีของ Hacker โดยจะใช้ tools metasploit ในการโจมตีเครื่องเป้าหมาย ขั้นตอนนี้จะต้องนำข้อมูลที่ได้จากขั้รตอนแรกมาใช้ โดยจะเอา version service ของเครื่องเป้าหมายมาค้นหาว่ามีช่องโหว่อะไรบ้างในการโจมตีเข้าไป ในการจำลองการโจมตีมีขั้นตอนดังต่อไปนี้

1. เปิดโปรแกรม metasploit ขึ้นมาโดยใช้คำสั่ง msfconsole



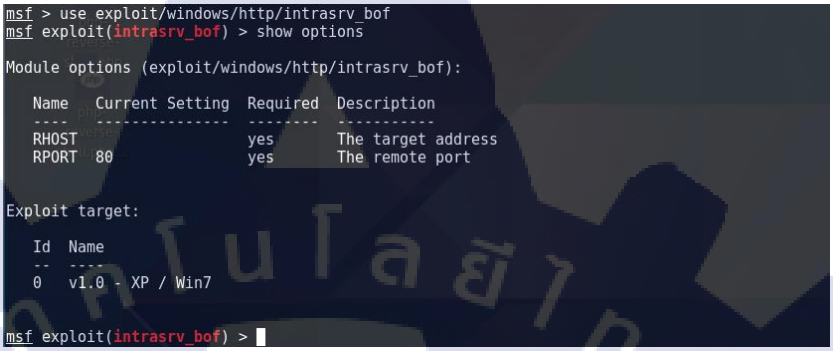
รูปที่ 3.16 การใช้ metasploit

2. ทำการค้นหา exploit หรือช่องโหว่ที่จะใช้เจาะใน metasploit โดยใช้คำสั่ง search ในตัวอย่างจะใช้ service intrasrv port 80 ที่เปิดอยู่ โดยจะค้นหา exploits ดั่งคำสั่งต่อไปนี้ msf > search intrasrv เมื่อทำการ search เสร็จสิ่งที่ได้จะมีชื่อของ exploits ปรากฏอยู่นั้น คือ exploit/windows/http/intrasrv_bof

```
msf > search intrasrv
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                              Disclosure Date  Rank    Description
   ----                              ---------------  ----    -----------
   exploit/windows/http/intrasrv_bof  2013-05-30      manual  Intrasrv 1.0 Buffer Overflow


msf >
```

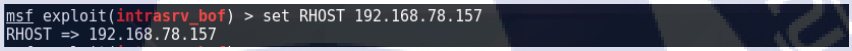
รูปที่ 3.17 การค้นหา exploits ใน metasploit

3. หลังจากได้ exploit มาแล้วจะทำการใช้ exploit หรือการเลือกช่องโหว่โดยมีคำสั่งดังนี้ msf > use exploit/windows/http/intrasrv_bof แล้วให้ทำการ show options เพื่อตรวจสอบความต้องการของตัวช่องโหว่นี้ โดยใช้คำสั่ง show options



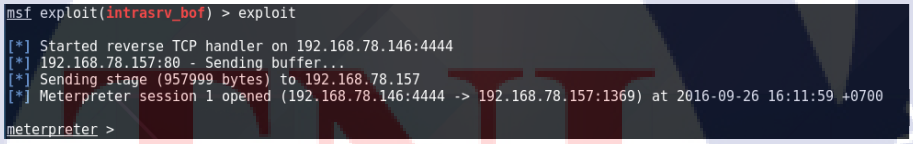
รูปที่ 3.18 การ use exploit ใน metasploit

4. ในขั้นตอนนี้จะทำการ set ip เครื่องเป้าหมายโดยใช้คำสั่ง set RHOST 192.168.78.157



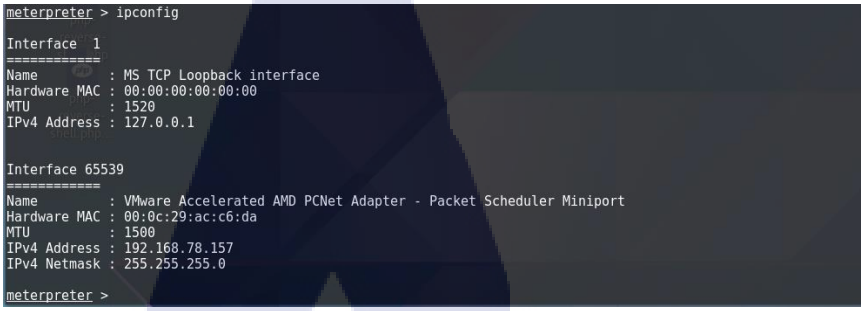
รูปที่ 3.19 การ set ip ใน metasploit

5. ขั้นตอนสุดท้ายจะทำการโจมตีเป้าหมาย โดยใช้คำสั่ง exploit เมื่อทำการโจมตีไปแล้วถ้าสำเร็จ command prom จะเปลี่ยนเป็น meterpreter แสดงว่าสามารถยึดขึ้นเป้าหมายได้สำเร็จ



รูปที่ 3.20 การใช้คำสั่ง exploit ใน metasploit

6. ทำการตรวจสอบหมายเลข ip ว่าตรงกับที่ได้มา โดยใช้คำสั่ง ipconfig เมื่อหมายเลขไอพีตรงกับที่ได้รับหมอบหมายมาถือว่า service นี้มีผลกระทบต่อ ระบบอย่างรุนแรงเพราะสามารถที่จะโดนโจมตี และ โดนยึดเป็นเครื่องของ hacker ได้



รูปที่ 3.21 การใช้คำสั่ง ตรวจสอบเครื่องเป้าหมาย

3.3.3.3 Report (รายงาน)

การทำรายงานและสิ่งที่แนะนำให้ทำ (Reporting) คือขั้นตอนการสรุปงานในแต่ละขั้นตอนว่าได้ข้อมูลอะไรบ้าง เช่น ระบบมีช่องโหว่ตรงไหนบ้าง ในแต่ละช่องโหว่มีความร้ายแรงขนาดไหน ส่งผลต่อระบบอะไรบ้าง และแต่ละช่องโหว่หรือระบบมีจุดไหนที่ควรแก้ไข และแก้ไขอย่างไรเป็นต้น ซึ่งการทำรายงานเป็นหัวใจหลักของการทดสอบเจาะระบบเลยก็ว่าได้

ในการทำรายงานแบ่งออกเป็น 4 ส่วนได้แก่

- Executive Summary คือ ภาพรวมของการทำการทดสอบเจาะระบบเช่น ขอบเขตของงานมีอะไรบ้าง มีเครื่องอะไรบ้างในการทดสอบเจาะระบบนั้นเอง
- Method topology คือ ขั้นตอนของการทดสอบเจาะระบบนั้นเอง แต่ละช่องโหว่มีกระบวนการอย่างไรบ้าง มีขั้นตอนการทำอย่างไรบ้าง โดยจะแสดงเป็นขั้นตอน
- Detail findings คือ รายละเอียดของช่องโหว่ที่พบว่ามีช่องโหว่อะไรบ้าง ช่องโหว่ที่พบมีระดับความปลอดภัยอยู่ที่เท่าไหร่ เป็นต้น
- Reference คือ แหล่งอ้างอิงที่ได้นำมาใช้กับ การทดสอบเจาะระบบนั้นเอง

บทที่ 4 สรุปผลการดำเนินงาน การวิเคราะห์และสรุปผลต่าง ๆ

4.1 ผลการดำเนินงาน

จากการที่ได้ปฏิบัติงานสหกิจศึกษาที่บริษัท ไซเบอร์ตรอน จำกัดในครั้งนี้ได้มีโอกาสเข้าร่วมเป็นส่วนหนึ่งในการจัดเตรียมการแข่งขันการป้องกันทางด้านไซเบอร์ทั้ง 4 งานของบริษัท และได้ร่วมออกแบบโจทย์ที่ใช้กับระบบ Cyber Range หรือระบบจำลองยุทธ์ทางด้านไซเบอร์เพื่อใช้ในการฝึกฝนป้องกัน และเจาะระบบ

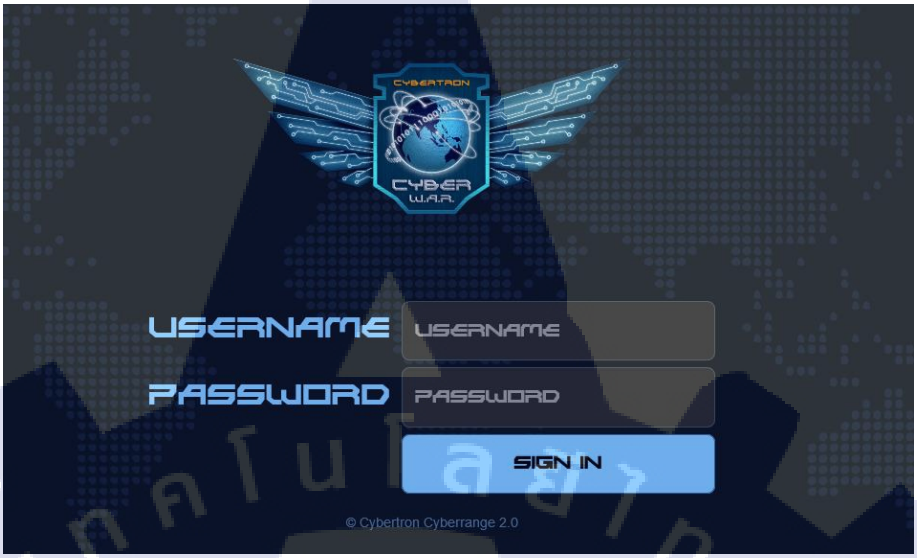
ได้รับประสบการณ์ในการปฏิบัติงานจริงในบริษัท ซึ่งในระหว่างปฏิบัติงานได้มีโอกาสร่วมกับพนักงานภายในบริษัท และมีโอกาสได้เข้ารับฟังคอร์สการฝึกอบรมจากอาจารย์ผู้มากประสบการณ์ทางด้าน Information Security ทำให้ได้รับความรู้ที่กว้างขวางเกี่ยวกับด้านความปลอดภัยทางสารสนเทศ ล้วนแล้วแต่มีประโยชน์ในการปฏิบัติงานในอนาคต

4.1.1 ผลการดำเนินการทดสอบเจาะระบบ

ในช่วงแรกจะทำความเข้าใจเกี่ยวกับตัวระบบก่อน ว่าระบบเป็นอย่างไรมีการใช้งานอย่างไร วิธีใช้เป็นอย่างไร ต่อมาเมื่อได้ข้อมูลเบื้องต้นได้ทำการทดสอบเจาะระบบ และทำการออกรายงานในลำดับต่อมาทั้งสามกระบวนการนี้ทำให้ทราบว่ามีช่องโหว่ตรงไหนบ้าง

และการทดสอบระบบเจาะระบบ Cyber Range นี้ทำให้ผู้ออกแบบระบบทราบถึงปัญหาที่เกิดขึ้นโดยตรงกับระบบ Cyber Rang เช่นตัวอย่างช่องโหว่ที่ได้พบคือ SQL Injection, Cross-site Scripting เป็นต้น

โดยจากปัญหาข้างต้นทำให้สามารถทำรายงานหรือ report เพื่อที่จะส่งต่อนำเอาปัญหาที่ได้พบไปยังทีม Dev เพื่อแก้ไขเว็บไซต์ให้มีความปลอดภัยได้ทันท่วงทีโดยในการแกไขจะจะทำการนำเอาข้อมูลที่ได้รับอินพุตเข้ามา ทำการกรองข้อมูลก่อนเพื่อป้องกันการเกิด SQL Injection โดยในการแก้ไขถือว่าเป็นไปได้ด้วยดีในการดำเนินการทดสอบเจาะระบบ Cyberrange ถือว่าประสบผลสำเร็จเป็นอย่างมาก



รูปที่ 4.1 หน้าตา เข้าสู่ระบบของระบบ Cyber Range

รูปที่ 4.2 หน้าตาผู้เล่นในระบบ Cyber Range

4.2 ผลการวิเคราะห์ข้อมูล

จากการปฏิบัติงานตั้งแต่เดือนมิถุนายน ถึงเดือนตุลาคม เป็นระยะเวลา 4 เดือน หรือ 18 สัปดาห์ ประสบความสำเร็จในระดับที่ดี เนื่องจากได้รับประสบการณ์ในการทำงานจริง และความรู้ต่างๆ ทั้งด้านการทำงาน ด้านการทดสอบและเจาะระบบทำให้รู้กระบวนการต่างๆ ซึ่งสามารถเอาไปใช้งานได้จริง การทำงานร่วมกับผู้อื่น การเรียนรู้การทำงานด้วยตนเอง และการแก้ไขปัญหาต่างๆ

4.3 วิเคราะห์และวิจารณ์ข้อมูลโดยเปรียบเทียบกับวัตถุประสงค์ และจุดมุ่งหมายในการปฏิบัติงาน

ตาราง 4.1 ตารางเปรียบเทียบผลที่ได้รับกับวัตถุประสงค์ในการปฏิบัติงาน

วัตถุประสงค์	ผลที่ได้รับ
เพื่อศึกษาและพัฒนาความรู้การทำงานจากสถานปฏิบัติงานจริง	ได้รับประสบการณ์จากการทำงานในสถานประกอบการจริง สามารถทำไปใช้ในการทำงานจริงต่อไปในภายภาคหน้าได้
ออกแบบโจทย์ที่ใช้งานกับระบบ Cyber Range	ได้รับความรู้ใหม่เพิ่มขึ้น ที่สามารถนำไปทดสอบเจาะระบบได้จริง
การทดสอบเจาะระบบ Cyber Range	ทำให้ทราบถึงผลกระทบที่จะเกิดขึ้นกับตัวระบบ Cyber Range
การออกแบบโจทย์ให้ทำงาน Automatic	ทำให้โจทย์ทำงานได้อย่าง automatic เมื่อทำการติดตั้งโจทย์ลงในระบบ Cyber Range
Deploy ระบบ Cyber Range	ทำการติดตั้งระบบ Cyber Range ที่ไซต์ของลูกค้าได้ โดยติดตั้งลงในระบบ ESXi

จากวัตถุประสงค์ข้างต้น โครงงานการทดสอบเจาะระบบของ Cyber Range สามารถป้องกันและแก้ไขได้โดยไม่ส่งผลกระทบต่อระบบต่อไป

บทที่ 5 บทสรุปและข้อเสนอแนะ

5.1 สรุปผลการดำเนินงาน

จากการที่ได้ปฏิบัติงานสหกิจศึกษาตั้งแต่เดือน มิถุนายน ถึงเดือนตุลาคม เป็นระยะเวลา 4 เดือน หรือ 18 สัปดาห์ที่บริษัท ไซเบอร์ตรอน จำกัด ผู้ปฏิบัติงานได้รับหมอบหมายให้จัดทำการ penetration test ระบบ cyber range หรือระบบจำลองยุทธ์ทางด้านไซเบอร์ เพื่อหาช่องโหว่ที่จะเกิดขึ้นกับระบบ ซึ่งผลกี่ดำเนินงานนั้นเป็นไปได้ด้วยดีและประสบความสำเร็จ ทำให้ได้ทราบวิธีการหรือ กระบวนการของการทำ penetration test อาทิเช่น ในการหาข้อมูลหรือ information ของระบบตั้งแต่ วิธีการสแกน service ที่อยู่ในระบบเอง และได้ทำการทดสอบเจาะเข้าไปจริงๆ ทำให้ได้ทราบความรู้ใหม่ๆ ที่ใช้จริงกับการทดสอบเจาะระบบ ต่อมาได้รับประสบการณ์ในการทำงานเป็นทีมมากขึ้น การปรับตัวในการทำงานกับผู้อื่น การวางแผนการทำงานอย่างเป็นระบบและสามารถแก้ไขปัญหาเฉพาะหน้าได้ อีกทั้งยังได้รับหน้าที่ในการร่วม ออกโจทย์ที่ใช้ในการดำเนินงานแข่งขัน ทั้ง 4 งานที่ได้จัดขึ้นทำให้ได้ใช้ประโยชน์จากความรู้ที่ได้ศึกษามาตลอดระยะเวลา

5.2 แนวทางการแก้ไขปัญหา

ในการทำโครงงาน penetration test ของระบบ cyber range นั้นได้พบปัญหาในการทำหลายรูปแบบไม่ว่าจะเป็นขั้นตอนของการทำ penetration test การเลือกเครื่องมือที่ใช้ในการทดสอบ ร่วมทั้งแหล่งที่ใช้อ้างอิงในการทำรายงาน โดยรุ่นพี่หรือพี่เลี้ยงได้ช่วยสอนหรือช่วยแนะนำตลอดการทำสหกิจศึกษาตลอดมา หลังจากได้รับการช่วยเหลือทำให้นำสิ่งนั้นๆไปศึกษาค้นคว้าด้วยตนเองต่อได้ เมื่อไม่เข้าใจตรงไหนก็สามารถไปขอคำแนะนำจากพนักงานที่ปรึกษาได้

5.3 ข้อเสนอแนะจากการดำเนินงาน

- การทำงานกับภาษาหรือโปรแกรมใหม่ๆที่ที่ไม่เคยศึกษามาก่อนเป็นการเรียนรู้ที่ดีจึงควรที่จะมีการเรียนการสอนเกี่ยวกับภาษาหรือโปรแกรมที่ใช้ให้มีพื้นฐานที่เพียงพอ ก่อนจะเริ่มดำเนินงาน

- หลังจากที่ได้ทำงานจริง การทำงานนั้นต้องมีการวางแผนอย่างเป็นระบบเป็นขั้นเป็นตอน เพื่อให้การทำงานนั้นไม่ยุ่งยากและเข้าใจง่าย เมื่อเกิดการผิดพลาดเราก็จะสามารถแก้ไขปัญหาได้ง่ายและตรงจุด

5.4 ผลที่ได้รับจากการปฏิบัติงาน

- ได้เรียนรู้ระบบการทำงานภายในองค์กร
- ได้ฝึกฝนตนเองให้มีการทำงานเป็นขั้นตอน
- ได้นำความรู้ที่เรียนมาใช้ในการทดสอบระบบ หรือการทำ penetration test
- ได้ศึกษาความรู้ใหม่ๆ เพิ่มเติมเพื่อนำมาใช้กับการทำงาน
- ได้รับประสบการณ์ในการทำงานจริง และเรียนรู้การทำงานร่วมกับผู้อื่น

เอกสารอ้างอิง

1) Anonymous,**HTML** [Online].Available:http://en.wikipedia.org/wiki/HTML[2014,July 22].
2) Anonymous,**Cascading** Style Sheets [Online].Available:http://en.wikipedia.org/wiki/Cascading_Style_Sheets[2014,July 22].
3) Anonymous,**JavaScript** [Online].Available:http://en.wikipedia.org/wiki/JavaScript[2014,July 23].
4) Anonymous,**PHP** [Online].Available:http://en.wikipedia.org/wiki/PHP[2014,July 24].
5) Anonymous,**SQL** [Online].Available.http://en.wikipedia.org/wiki/SQL[2014,July 24].
6) Anonymous,Relational database management system [Online].Available:http://en.wikipedia.org/wiki/Relational_database_management_system[2014,July 22].
7) Anonymous,**Web Application** [Online].Available:http://en.wikipedia.org/wiki/Web_application[2014,July 21].
8) OWASP,**Top 10 2013-Top 10** [Online].Available:https://www.owasp.org/index.php/Top_10_2013-Top_10[2014,July 24].

ประวัติผู้จัดทำโครงงาน

ชื่อ – สกุล วัชระ จึงมงคลสวัสดิ์

วัน เดือน ปีเกิด 07 เมษายน 2535

ประวัติการศึกษา

ระดับประถมศึกษา โรงเรียนอโศกวิทย์ อ่อนนุช

ระดับมัธยมศึกษา โรงเรียนเทพศิรินทร์ร่มเกล้า

ระดับอุดมศึกษา คณะเทคโนโลยีสารสนเทศ สาขาเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีไทย-ญี่ปุ่น กรุงเทพมหานคร

ทุนการศึกษา - ไม่มี -

ประวัติการฝึกอบรม

1. Basic Network Installation and Troubleshooting 2015
2. Penetration Testing & Ethical Hacking Workshop 2013

ผลงานที่ได้รับการตีพิมพ์

1. Design of Framework for Load Control Based on Internet by Using Android Mobile Application ICBIR 2016