ชุดโปรแกรมทดสอบความปลอดภัยระบบคอมพิวเตอร์

COMPUTER SECURITY PENETRATION TEST SUITE

ธีรยุทธ ดำรงตระกูลเจริญ

ปิติพล พลพบู

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2550

ปริญญานิพนธ์ปีการศึกษา 2550

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง ชุดโปรแกรมทดสอบความปลอดภัยระบบคอมพิวเตอร์

Computer Security Penetration Test Suite

ผู้จัดทำ

1. นายธีรยุทธ ดำรงตระกูลเจริญ รหัสนักศึกษา 47010340
2. นายปิติพล พลพบู รหัสนักศึกษา 47010455

_____ อาจารย์ที่ปรึกษา

(อาจารย์ อัครเดช วัชระภูพงษ์)

_____ อาจารย์ที่ปรึกษา

(ผศ. ธนา หงษ์สุวรรณ)

_____ อาจารย์ที่ปรึกษา

(อาจารย์ ธนัญชัย ตรีภาค)

ชุดโปรแกรมทดสอบความปลอดภัยระบบคอมพิวเตอร์

นายธีรยุทธ	ดำรงตระกูลเจริญ	47010340
นายปิติพล	พลพบู	47010455
อาจารย์อัครเดช	วัชระภูพงษ์	อาจารย์ที่ปรึกษา
ผศ.ธนา	หงษ์สุวรรณ	อาจารย์ที่ปรึกษาร่วม
อาจารย์ธนัญชัย	ตรีภาค	อาจารย์ที่ปรึกษาร่วม

ปีการศึกษา 2550

บทคัดย่อ

โครงงานนี้เป็นโครงงานที่มุ่งเน้นการศึกษาแนวทางของการเจาะระบบรักษาความปลอดภัยทางคอมพิวเตอร์ด้วยเครื่องมือเจาะระบบรักษาความปลอดภัยทางคอมพิวเตอร์ ไม่ว่าผ่านเครือข่าย หรือ ณ ตัวเครื่อง เพื่อใช้ในการตรวจหาช่องโหว่ความปลอดภัยก่อนที่ผู้บุกรุกพบและใช้ประโยชน์ แล้วทำการสร้างต้นแบบเครื่องมือทดสอบความปลอดภัยระบบคอมพิวเตอร์ตามหลักธรรมจรรยา (Ethical Hacking) สำหรับทั้งแพลตฟอร์มยูนิกซ์ (GNU Linux) และไมโครซอร์ฟวินโดวส์ (Microsoft Windows)

การพัฒนาชุดทดสอบความปลอดภัยระบบคอมพิวเตอร์นี้ มุ่งเน้นระบบเป้าหมายที่ติดตั้งระบบปฏิบัติการไมโครซอร์ฟวินโดวส์เอ็กซ์พี เซอร์วิสแพ็ค 2 (Microsoft Windows XP Service Pack 2) เนื่องจากปัจจุบันเป็นระบบปฏิบัติการที่นิยมใช้ในเครื่องคอมพิวเตอร์ในองค์กร และผู้ใช้งานทั่วไป นอกจากนี้ชุดทดสอบความปลอดภัยระบบคอมพิวเตอร์สามารถทำงานบนระบบปฏิบัติการยูนิกซ์ (GNU Linux) เพื่อให้ผู้ทำการทดสอบระบบความปลอดภัยคอมพิวเตอร์ (Penetration Tester) ซึ่งมักมีความชำนาญในการใช้ระบบปฏิบัติการยูนิกซ์ สามารถนำชุดทดสอบความปลอดภัยฯนี้ไปประยุกต์ใช้งานและพัฒนาต่อไป

Computer Security Penetration Test Suite

Mr. Teerayuth Dumrongtrakulcharoen 47010340

Mr. Pitiphol Pholpabu 47010455

Mr. Akkradach Watcharapupong Advisor

Asst.Prof. Thanna Hongsuwan Co-Advisor

Mr. Thananchai Treepak Co-Advisor

Academic Year 2007

ABSTRACT

This project focuses on research of computer security hacking with hacking tools to detect security holes before an intruder found and exploit by building a prototype of computer security penetration test tool according to ethical hacking for GNU Linux platform and Microsoft Windows platform.

Our tool concentrates upon target hosts which Microsoft Windows XP Service Pack 2 was installed because it is the most popular operating system for general users at the present time. Furthermore, this tool gets along well with GNU Linux in order to penetration testers who are professional on this operating system can apply to use and develop in the future.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้ได้รับคำแนะนำ และคำปรึกษาเกี่ยวกับการวิจัยและการค้นคว้าจาก อาจารย์อัครเดช วัชระภูพงษ์ อาจารย์ผู้ควบคุมปริญญานิพนธ์ ผศ.ธนา หงษ์สุวรรณ และอาจารย์ ธนัญชัย ตรีภาค ผู้ควบคุมปริญญานิพนธ์ร่วม ผู้วิจัยรู้สึกซาบซึ้งในความอนุเคราะห์จากอาจารย์ทั้ง สามท่านเป็นอย่างสูง

ขอบคุณห้องวิจัย ISAG ภาควิชาคอมพิวเตอร์ที่ได้สนับสนุนในส่วนของอุปกรณ์ เครื่องมือ ตลอดจนหนังสือต่างๆที่มีเอื้อประโยชน์แก่การวิจัยในครั้งนี้ด้วย

ขอกราบขอบพระคุณคณาอาจารย์ รวมถึงผู้ช่วยสอนทุกท่านในภาควิชาวิศวกรรม คอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุก ท่านที่ประสิทธิ์ประสาทวิชาความรู้และประสบการณ์ดีๆให้แก่ข้าพเจ้ามาตลอดระยะเวลา 4 ปีที่ ทำการศึกษา

ขอขอบคุณเพื่อนๆ พี่ๆ และน้องๆ ในภาควิชาวิศวกรรมคอมพิวเตอร์ที่คอยให้กำลังใจ และ คำแนะนำ รวมถึงประสบการณ์ต่างๆที่ได้ทำร่วมกันตลอดมา

สุดท้ายนี้ข้าพเจ้าขอขอบพระคุณบิดา มารดาและครอบครัวของข้าพเจ้าที่เป็นกำลังใจและ เป็นแรงผลักดันให้ข้าพเจ้าสามารถทำปริญญานิพนธ์นี้ด้วย

อย่างไรก็ตามข้าพเจ้าหวังเป็นอย่างยิ่งว่ารายงานของข้าพเจ้าจะเป็นประโยชน์ต่อทุกท่าน และให้คำแนะนำแก่นักศึกษารุ่นต่อไปในอนาคตข้างหน้า

นายธีรยุทธ ดำรงตระกูลเจริญ
นายปิติพล พลพบู

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญรูป

สารบัญรูป(ต่อ)

รูปที่ **หน้า**

สารบัญตาราง

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

การรักษาความปลอดภัยระบบคอมพิวเตอร์นั้นนอกจากแนวที่ไม่มีการใช้ปฏิกิริยาโต้ตอบ (passive) แล้วยังมีแนวที่จะใช้ปฏิกิริยาโต้ตอบเข้าควบคุมสถานการณ์ (proactive) เพื่อตรวจหาช่องโหว่ความปลอดภัยก่อนผู้บุกรุกพบและใช้ประโยชน์ ฉะนั้นจึงมีความจำเป็นต้องใช้เครื่องมือคล้ายของผู้บุกรุกสำหรับทดสอบระดับความปลอดภัย ซึ่งในปัจจุบันยังมีความก้ำกึ่งแง่จรรยาบรรณสำหรับเครื่องมือประเภทนี้ อีกทั้งต้องอาศัยความชำนาญเฉพาะในแต่ละเครื่องมือ ทำให้เสาะหาและใช้งานได้ยาก เช่น Password Cracker, Port Scanner, Security Scanner และ Exploit Code Injection เป็นต้น นอกจากนี้ในปัจจุบันเครื่องมือประเภทนี้พัฒนาเพื่อจุดประสงค์ทางการค้าเป็นส่วนใหญ่ เช่น Nessus, Retina และ GFI LANguard เป็นต้น จึงได้มีการพัฒนาให้อยู่ในรูปของโอเพนซอร์ส (Open Source) เพื่อทำให้ผู้ทำการทดสอบระบบคอมพิวเตอร์ (Penetrate Tester) สามารถให้ข้อแนะนำที่เหมาะสมในการเพิ่มความปลอดภัยให้แก่เครื่องที่ทำการตรวจสอบ

1.2 วัตถุประสงค์ของโครงงาน

1 เพื่อศึกษาพฤติกรรมในการเจาะระบบคอมพิวเตอร์ของผู้บุกรุก
2 เพื่อศึกษาแนวทางการทดสอบความปลอดภัยระบบคอมพิวเตอร์
3 เพื่อศึกษาวิธีการบรรเทาปัญหาช่องโหว่ความปลอดภัยของระบบคอมพิวเตอร์
4 เพื่อสร้างต้นแบบระบบทดสอบความปลอดภัยระบบคอมพิวเตอร์

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1 สามารถช่วยผู้ที่ทำการทดสอบและประเมินระบบความปลอดภัยทำการตรวจสอบความปลอดภัยคอมพิวเตอร์
2 เพื่อใช้เป็นโปรแกรมพื้นฐานในการพัฒนาโปรแกรมที่เกี่ยวกับการทดสอบความปลอดภัย ในรูปแบบของโอเพนซอร์ส
3 เพื่อแนะนำเกี่ยวกับการป้องกันการโจมตีของผู้บุกรุก ที่อาจถูกทำการเอ็กซ์พลอยท์และนำระบบคอมพิวเตอร์เป้าหมายไปใช้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
4 สามารถทำให้ผู้ใช้งานคอมพิวเตอร์ทั่วไปตระหนักถึงปัญหาความปลอดภัยคอมพิวเตอร์

5 สามารถสร้างระบบต้นแบบในการทดสอบความปลอดภัยระบบคอมพิวเตอร์ เพื่อนำไปใช้งานจริง

6 สามารถสร้างชุดโปรแกรมที่ทำการสร้างเอกสาร เพื่อรายงานผลการทดสอบ และแนะนำเกี่ยว กับวิธีการบรรเทาปัญหาช่องโหว่ความปลอดภัยของระบบคอมพิวเตอร์

7 ได้รับความรู้ความเข้าใจเกี่ยวกับทางการทดสอบความปลอดภัยระบบคอมพิวเตอร์

8 ได้รับความรู้ความเข้าใจเกี่ยวกับวิธีการบรรเทาปัญหาช่องโหว่ความปลอดภัยของระบบคอมพิวเตอร์

9 ได้รับความรู้ความเข้าใจเกี่ยวกับการสร้างเอกสาร XML ในการวิเคราะห์ความปลอดภัยของคอมพิวเตอร์ และการสร้างส่วนต่อประสานกราฟิกกับผู้ใช้งาน

1.4 ขอบเขตของโครงงาน

1. ชุดโปรแกรมสามารถทำงานได้บนระบบปฏิบัติการลินุกซ์ (Linux) เท่านั้น
2. การทำงานของชุดโปรแกรมจะมีประสิทธิภาพสูง เมื่อระบบที่นำมาทดสอบทำงานบนระบบปฏิบัติการวินโดวส์เอ็กซ์พี เซอร์วิสแพ็ค 2 (Microsoft Windows XP Service Pack 2)
3. ชุดโปรแกรมสามารถทำการสแกน และเอ็กซ์พลอยท์ (Exploit) ระบบคอมพิวเตอร์ได้ ชุดโปรแกรมสามารถติดต่อผู้ใช้งานผ่านส่วนต่อประสานกราฟิกกับผู้ใช้งาน และคอมมานด์ไลน์
4. ชุดโปรแกรมสามารถสร้างเอกสาร XML ในส่วนของการสรุปผลการทดสอบ
5. ชุดโปรแกรมสามารถสแกนระบบคอมพิวเตอร์ได้อย่างประสิทธิภาพ เมื่อทำสแกนจากเครือข่ายภาย ในระบบคอมพิวเตอร์เป้าหมาย (Local Area Network)

1.5 ขั้นตอนการดำเนินการ

1. ศึกษาความรู้พื้นฐานเกี่ยวกับการทำงานของโพรโตคอลทีซีพี และแนวทาง / รูปแบบของการทดสอบการเจาะระบบ (Penetration Test) รวมถึงศึกษาพฤติกรรมของผู้บุกรุก
2. ศึกษากระบวนการทำงานของชุดโปรแกรมทดสอบระบบคอมพิวเตอร์
3. ศึกษาหลักการการสแกน และเทคนิคการเอ็กซ์พลอยท์ (Exploit) ต่างๆ
4. ทดสอบและพัฒนาโปรแกรมหรือโค้ดที่จะนำมาใช้ในชุดโปรแกรมทดสอบระบบคอมพิวเตอร์
5. ทดลองสร้างชุดโปรแกรมการทดสอบระบบคอมพิวเตอร์
6. ศึกษาการการใช้งาน XML และการนำดึงข้อมูลเข้า / ออก XML

7. ศึกษาการทำงานและช่องโหว่ของแต่ละแอปพลิเคชัน ที่นิยมใช้ในปัจจุบัน
8. ศึกษาวิธีการรักษาความปลอดภัยและช่องโหว่ความปลอดภัยบนระบบปฏิบัติวินโดวส์ เอ็กซ์พี เซอร์วิสแพ็ค 2
9. ศึกษาและเขียนโปรแกรมในส่วนของอินเตอร์เฟสและการติดตั้ง
10. สร้างระบบต้นแบบที่ใช้ในการทดสอบชุดโปรแกรมทดสอบระบบคอมพิวเตอร์
11. ทดลองติดตั้งชุดโปรแกรมทดสอบระบบคอมพิวเตอร์ และทดสอบกับระบบต้นแบบ
12. ทำเอกสารโครงงานและสรุปผล

1.6 เนื้อหาของรายงาน

รายงานฉบับนี้มีทั้งหมด 5 บท ดังนี้

- บทที่ 1 กล่าวถึง วัตถุประสงค์, ประโยชน์, ขอบเขต, และขั้นตอนการดำเนินการของโครงงาน
- บทที่ 2 กล่าวถึง ทฤษฎีที่เกี่ยวข้องที่ใช้ในการพัฒนาโครงงาน
- บทที่ 3 กล่าวถึง หลักการออกแบบพัฒนาโครงงาน ซึ่งอธิบายการขั้นตอนการทำงานของโปรแกรมในส่วนต่างๆ รวมทั้งรายละเอียดทางด้านซอร์ฟแวร์
- บทที่ 4 กล่าวถึง การทดลองและผลการทดลองของโปรแกรมที่นำมาพัฒนา และชุดโปรแกรมทดสอบความปลอดภัยระบบคอมพิวเตอร์
- บทที่ 5 กล่าวถึง บทวิจารณ์, ปัญหาและอุปสรรค, ผลการดำเนินงาน และแผนในการพัฒนาต่อ
- บรรณานุกรม

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

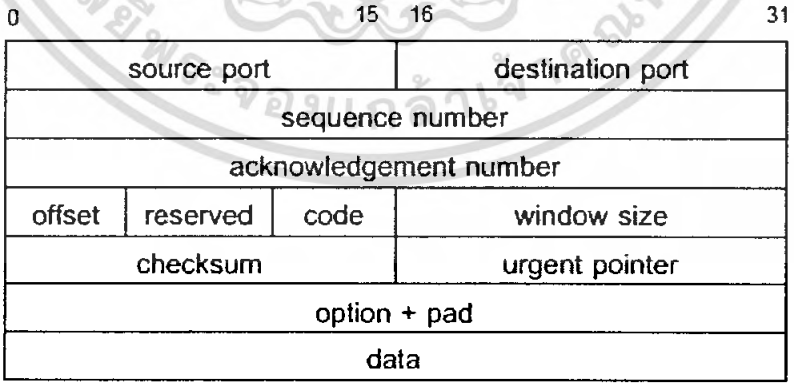
2.1 ทฤษฎีพื้นฐานที่เกี่ยวข้องกับโครงงาน

เทคนิคของการสแกนนั้นมีอยู่หลายอย่าง โดยจะทำงานผ่านโพรโตคอล ได้แก่ โพรโตคอลไอพี(IP) ทีซีพี ยูดีพีไอซีเอ็มพีและเออาร์พี ซึ่งเทคนิคการสแกนส่วนใหญ่ที่มีการใช้งานอยู่นั้นส่วนมากเกิดจากการตั้งค่าแฟล็กต่างๆในเฮดเดอร์ของโพรโตคอลทีซีพี เช่น เทคนิคการสแกน SYN เกิดจากการตั้งค่าแฟล็ก SYN ที่ทำการส่งไปสแกน

2.1.1 โพรโตคอลทีซีพี (TCP)

โพรโตคอลทีซีพีเป็นโพรโตคอลที่ทำงานอยู่บนระดับชั้น Transport ซึ่งเป็นโพรโตคอลที่มีความสามารถในการรับประกันการส่งข้อมูล (Guarantee Delivery) โดยสามารถตรวจสอบความผิดปกติของข้อมูลที่ส่ง และส่งซ้ำเมื่อพบความผิดปกติ สามารถรับรองความครบถ้วนของข้อมูลที่ส่ง เช่น หากส่งข้อมูลเป็นไฟล์ขนาด 10 กิโลไบต์ โพรโตคอลทีซีพีจะแบ่งข้อมูลออกเป็นส่วน ๆ เรียกว่า เซ็กเมนต์ (Segment) เช่น หากกำหนดให้ขนาดของเซ็กเมนต์เป็น 1 กิโลไบต์ ก็จะต้องส่งทั้งหมด 10 ครั้ง ในการส่ง 10 ครั้งนี้ หากมีความผิดพลาดเกิดขึ้นที่เซ็กเมนต์ใด ก็จะส่งเซ็กเมนต์นั้นใหม่ และหากไม่สามารถส่งให้ครบได้ ก็จะแจ้งความผิดพลาด โดยจะไม่มีกรณีที่รับข้อมูลได้ไม่ครบถ้วนอย่างเด็ดขาด ซึ่งโครงงานนี้ได้มีการใช้คุณลักษณะรูปแบบเซ็กเมนต์ของทีซีพีในการหาช่องโหว่ความปลอดภัยเป็นส่วนสำคัญ

รูปแบบเซ็กเมนต์ของทีซีพี แสดงดังรูปที่ 1



รูปที่ 2.1 แสดงรูปแบบเซ็กเมนต์ของทีซีพี

- Source Port มีขนาด 16 บิต เป็นหมายเลขพอร์ตของฝั่งต้นทาง
- Destination Port มีขนาด 16 บิต เป็นหมายเลขพอร์ตของฝั่งปลายทาง

- Sequence Number มีขนาด 32 บิต ใช้ในการบอกลำดับการส่งของเซ็กเมนต์ในการส่งชุดเดียวกัน
- Acknowledgement Number มีขนาด 32 บิต ใช้บอกการตอบรับในการรับชุดเดียวกัน
- Offset มีขนาด 4 บิต บอกตำแหน่งเริ่มต้นของข้อมูล หรือ จุดสิ้นสุดของส่วนเฮดเดอร์ ดังนั้นจึงใช้บอกขนาดของเฮดเดอร์ได้ ค่าของข้อมูลเป็นหน่วยของ 4 ไบต์ เช่น หากมีค่า 5 หมายถึงเฮดเดอร์ยาว 20 ไบต์
- Reserved มีขนาด 4 บิต สำรองสำหรับการใช้ในอนาคต
- Code มีขนาด 8 บิต ประกอบด้วย 6 ฟิลด์ย่อย ดังต่อไปนี้

URG	ACK	PSH	RST	SYN	FIN	N/A	N/A

รูปที่ 2.2 แสดงรูปแบบฟิลด์ Code

  - URGent ใช้บอกว่ามีข้อมูลเร่งด่วน หากบิตนี้มีค่าเป็น 1 หมายถึง ในฟิลด์ Urgent Pointer มีข้อมูลเร่งด่วนบรรจุอยู่
  - ACKnowledgement ใช้บอกการตอบรับการส่งข้อมูล โดยหากเซ็กเมนต์ใดที่มีบิตนี้เป็น 1 หมายความว่าเซ็กเมนต์นั้นบรรจุข้อมูลการตอบรับเอาไว้
  - PuSH ใช้บอกความเร่งด่วน โดยหากเซ็กเมนต์ใดที่บิตนี้เป็น 1 หมายความว่าให้ส่งเซ็กเมนต์นั้นไปยังระดับชั้นแอปพลิเคชันทันที โดยไม่ต้องรอให้บัฟเฟอร์เต็ม บิตนี้จะมีประโยชน์สำหรับแอปพลิเคชันที่ต้องการการตอบสนองที่รวดเร็ว เช่น เทลเน็ต
  - ReSeT ใช้ในการยกเลิกการเชื่อมต่อครั้งนี้ โดยหากบิตนี้เป็น 1 หมายถึงให้ยกเลิกการเชื่อมต่อครั้งนี้ไปก่อน อาจเนื่องจากความผิดพลาด และหากต้องการส่งข้อมูลต่อ ก็จะต้องสร้างการเชื่อมต่อขึ้นใหม่
  - SYNchronize กล่าวถึงรายละเอียดในเรื่องการสร้างการเชื่อมต่อ
  - FINish ใช้ในการจบการเชื่อมต่อ โดยบิตนี้ของเซ็กเมนต์ใดที่มีค่าเป็น 1 หมายถึง ให้สิ้นสุดการเชื่อมต่อ บิตนี้จะต่างจาก Reset ตรงที่บิตนี้จะหมายถึงจบการเชื่อมต่อแบบถาวร ในขณะที่ Reset มักจะใช้ในการจบการเชื่อมต่อชั่วคราว
  - Window Size (16 บิต) ใช้ในการกำหนดขนาดบัฟเฟอร์ที่ใช้ในการเชื่อมต่อแต่ละครั้ง
- Checksum (16 บิต) ใช้ในการตรวจสอบความผิดปกติของเซ็กเมนต์ ซึ่งส่วนของ Checksum ของทีซีพีจะต่างจากไอพี เพราะ Checksum ของทีซีพีเป็นการตรวจสอบทั้งเฮดเดอร์และส่วนข้อมูล

- Urgent Pointer ทำหน้าที่เป็นตัวชี้ตำแหน่งในส่วนข้อมูล ที่เป็นข้อมูลเร่งด่วน เพื่อให้แอปพลิเคชันสามารถนำข้อมูลนั้นไปใช้ทันที
- Options มีขนาดไม่แน่นอน ใช้ในการกำหนดงานเพิ่มเติมให้กับทีซีพี
- Pad มีขนาด 0-3 ไบต์ ใช้เพิ่มส่วนที่เหลือของ Options เพื่อให้เฮดเดอร์ของเฮดเดอร์หารด้วย 4 ลงตัว
- Data เป็นส่วนข้อมูลของทีซีพี

2.1.2 ไมโครซอร์ฟวินโดวส์เอ็กซ์พี เซอร์วิสแพ็ค 2 (Microsoft Windows XP Professional Service Pack 2)

ไมโครซอร์ฟวินโดวส์เอ็กซ์พี เซอร์วิสแพ็ค 2 (Microsoft Windows XP) เป็นระบบปฏิบัติการที่ไมโครซอฟท์ได้ผลิตออกมาในปี ค.ศ. 2002 (พ.ศ. 2545) เป็นระบบปฏิบัติการที่ใช้รากฐานในการพัฒนาจากวินโดวส์เอ็นทีและมีกลุ่มเป้าหมายเป็นผู้ใช้ทั่วไปโดย XP นั้นคือตัวอักษรที่ย่อมาจาก eXPerience ที่หมายถึง ประสบการณ์ และระบบปฏิบัติการไมโครซอร์ฟวินโดวส์เอ็กซ์พี ได้แบ่งออกเป็น 3 เวอร์ชัน ได้แก่ Windows XP Starter Edition, Windows XP Home Edition, Windows XP Professional Edition

ไมโครซอฟต์ได้ทำการปรับปรุงระบบปฏิบัติการไมโครซอร์ฟวินโดวส์เอ็กซ์พี ซึ่งประกอบด้วยการปรับปรุงทางด้านความปลอดภัยและเพิ่มขีดความสามารถทางด้านความปลอดภัยใหม่ๆ นอกจากนี้ได้รวมเอาการแก้ไขและการปรับปรุงปัญหาทางด้านความปลอดภัย ซึ่งก่อนหน้านี้ได้ทยอยออกมาเรื่อยๆ เข้ามาไว้ในเซอร์วิสแพ็ค 2 ทั้งหมด โดยสามารถสรุปการปรับปรุงทางด้านความปลอดภัยใหม่ดังนี้

- *Personal Firewall* เพื่อช่วยป้องกันการโจมตีจากหนอนอินเตอร์เน็ต และซอฟต์แวร์ไม่ประสงค์ดี
- *ยกเลิกการทำงานของ ActiveX และแอ็คทิฟสคริปต์* ใน Local Machine Zone ให้ ซึ่งจะช่วยแก้ปัญหาการโจมตีและช่องโหว่ต่างๆ ของวินโดว์เอ็กซ์พี
- *ปรับปรุงปัญหาทางด้านความปลอดภัยของบราวเซอร์ IE* เช่น การบล็อกหน้าต่างป็อบอัพ และการจัดการรูปแบบไฟล์แนบ MIME type (ป้องกันปัญหา social engineering และ Phishing) นอกจากนี้ได้เสริมความปลอดภัยให้กับ security zone, object caching และช่วยป้องกันปัญหาของสคริปต์โจมตีต่างๆ ได้ (malicious web scripts)
- *ปรับปรุงความปลอดภัยของโปรแกรมอ่านอีเมล์* Outlook Express ได้รับการปรับปรุงให้สามารถอ่านและแต่งอีเมล์แบบ plain text ได้ รวมทั้งสามารถบล็อก HTML เช่น พวก

ข้อผิดพลาดของเว็บได้ การตรวจสอบไฟล์แนบต่างๆ จะกระทำอย่างระมัดระวังเพื่อป้องกันการรันไฟล์แนบที่ไม่ประสงค์ดี

- *จัดตั้งศูนย์กลางการรักษาความปลอดภัย (Security Center)* ศูนย์กลางนี้จะช่วยเป็นแหล่งข้อมูลการปรับแต่งค่าความปลอดภัยต่างๆ การเรียนรู้สิ่งใหม่ๆ เกี่ยวกับเรื่องความปลอดภัย รวมทั้งการตรวจสอบว่าเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ได้ติดตั้งโปรแกรมอุดช่องโหว่ให้ทันสมัยแล้วหรือไม่
- *ปรับปรุง Automatic Updates* ความสามารถในการปรับปรุงระบบโดยอัตโนมัติไมโครซอร์ฟวินโดวส์เอ็กซ์พี ได้รับการปรับปรุงใหม่ US-CERT แนะนำให้เลือกใช้งานฟังก์ชันนี้
- *ป้องกันการทำงานของโค้ดบนเครื่องที่ใช้งาน* Service Pack 2 ได้เสริมกลไกการป้องกันหน่วยความจำเพื่อป้องกันผู้บุกรุกสั่งรันโค้ดในเครื่องของผู้ใช้งาน

ในโครงงานนี้ได้ทำการสร้างระบบต้นแบบที่ใช้ในการทดสอบชุดโปรแกรมทดสอบระบบคอมพิวเตอร์ โดยทำการติดตั้งระบบปฏิบัติการไมโครซอร์ฟวินโดวส์เอ็กซ์พี เซอร์วิสแพ็ค 2 ซึ่งนอกจากระบบปฏิบัติการแล้ว ชุดโปรแกรมสามารถใช้ในการทดสอบระบบคอมพิวเตอร์เป้าหมายที่ทำงานบนระบบปฏิบัติการอื่นๆได้ เพียงแต่ประสิทธิภาพและความแม่นยำในการทำงานของโปรแกรมอาจจะมีประสิทธิภาพที่ต่ำกว่า

2.1.3 ไฟร์วอลล์

ไฟร์วอลล์ เป็นส่วนประกอบที่ทำหน้าที่ในการควบคุมการเข้าถึงระหว่างเครือข่ายภายนอกเครือข่ายที่คิดว่าไม่ปลอดภัย กับเครือข่ายภายในหรือเครือข่ายที่ต้องการเพิ่มความปลอดภัย โดยที่ส่วนประกอบนั้นอาจจะเป็นเราเตอร์ คอมพิวเตอร์ หรือเครือข่าย ประกอบกันก็ได้ ขึ้นอยู่กับวิธีการหรือสถาปัตยกรรมไฟร์วอลล์ที่ใช้ ซึ่งไฟร์วอลล์นั้นสามารถแบ่งตามลักษณะการทำงานได้เป็น 3 ประเภทดังนี้

- **แพ็คเก็ตฟิลเตอริง (Packet Filtering Firewall)**

ไฟร์วอลล์ชนิดนี้ เป็นไฟร์วอลล์ที่มีรูปแบบการทำงานง่ายที่สุด และเป็นไฟร์วอลล์ที่เก่าแก่ที่สุด ปัจจุบันไฟร์วอลล์มักจะเป็นฟังก์ชันหนึ่งของเราเตอร์ โดยเราเตอร์ที่มีความสามารถนี้นอกจากจะสามารถหาเส้นทางได้แล้ว ยังสามารถกรองแพ็คเก็ตได้อีกด้วย กล่าวคือ สามารถจะอนุญาตหรือไม่อนุญาตให้แพ็คเก็ตผ่านเราเตอร์ได้ โดยการกำหนดเป็นกฎขึ้นมา

โดยหลักการทำงานโดยทั่วไปแล้ว ในการควบคุมทราฟฟิกของข้อมูล จะอาศัยการตรวจสอบข้อมูลที่ปรากฏอยู่ในเฮดเดอร์ของแพ็คเก็ต เช่น ที่อยู่ต้นทาง(Source IP) ที่อยู่ปลายทาง (Destination IP) พอร์ต โพรโตคอล เป็นต้น เพื่อใช้ในการกำหนดการกระทำต่างๆตามเงื่อนไขใน

การควบคุมการเข้าออกของข้อมูล โดยการพิจารณาข้อมูลทั้งหมดให้เป็นไปตามกฎที่ได้ระบุเอาไว้ ซึ่งเรียกว่า แอคเซสรูล (Access Rules) หรือ กฎของการควบคุมการผ่านการเข้าออกของแพ็คเก็ต โดยทั่วไปแล้วจะมีรูปแบบของแอคเซสรูลเบื้องต้นดังต่อไปนี้

ตารางที่ 2.1 แสดงรูปแบบของแอคเซสรูลเบื้องต้น

Source Address	Destination Address	Protocol	Service (Dst. Port)	Action

- **สเตทฟูลอินสเป็คชัน (Stateful Inspection Firewall)**

แพ็คเก็ตฟิลเตอริง สามารถกรองแพ็คเก็ตที่ไม่ต้องการออกไป แต่ไฟร์วอลล์ข้างต้นก็ไม่ได้ตรวจสอบว่า การเชื่อมต่อผ่านพอร์ตนั้นเป็นการเชื่อมต่อตามปกติหรือไม่ ทั้งนี้อาจเป็นแพ็คเก็ตโจมตีก็ได้ และสำหรับพอร์ตที่มีหมายเลขมากกว่า 1024 ไฟร์วอลล์ดังกล่าวจะต้องเปิดพอร์ตเหล่านั้นไว้ตลอดเวลา เนื่องจากไฟร์วอลล์ไม่รู้ว่าแอปพลิเคชันใดจะใช้งานพอร์ตหมายเลขใดบ้าง ซึ่งถือเป็นความไม่ปลอดภัย

จากข้อบกพร่องทั้งหมดนี้ ไฟร์วอลล์แบบ สเตทฟูลอินสเป็คชัน สามารถป้องกันได้ โดยในระหว่างการเชื่อมต่อไฟร์วอลล์จะทำการสร้างตารางสถานะ (State Table) ที่จะเก็บสถานะของการเชื่อมต่อในทุกๆ การเชื่อมต่อเอาไว้ และสำหรับกรณีของแพ็คเก็ตที่มีการ Fragmentation มานั้น ไฟร์วอลล์สเตทฟูลจะรอจนครบทั้งตาต้าแกรม แล้วจึงทำการจัดเรียงแพ็คเก็ตใหม่ (Reassemble) แล้วจึงตรวจสอบว่าถูกต้องหรือไม่ และไฟร์วอลล์แบบสเตทฟูลไม่จำเป็นต้องเปิดพอร์ตหมายเลข 1024 ขึ้นไป ทิ้งเอาไว้ เนื่องจากเมื่อไฟร์วอลล์สามารถติดตามสถานะได้แล้ว ก็ย่อมจะรู้ว่าการเชื่อมต่อนั้น ๆ ฝั่งไคลเอนต์มีการใช้งานพอร์ตใด ก็จะเปิดพอร์ตนั้น “เฉพาะ” สำหรับไคลเอนต์นั้น และเมื่อการเชื่อมต่อจบลง ก็จะปิดพอร์ตนั้นไว้เหมือนเดิม ทำให้ระบบมีความปลอดภัยเพิ่มขึ้นมาก

แม้ว่าไฟร์วอลล์แบบสเตทฟูลจะมีความปลอดภัยเพิ่มขึ้นมากแล้วก็ตาม ไฟร์วอลล์ประเภทนี้ยังไม่สามารถป้องกันการโจมตีที่แทรกซึมมากับการเชื่อมต่อตามปกติได้ เช่น โพรโตคอล FTP นั้น แม้ว่าไฟร์วอลล์แบบสเตทฟูลจะมีการติดตามให้มีการเปิดพอร์ต 20 และ 21 อย่างถูกต้อง แต่หากมีการส่งข้อมูลอื่น ๆ ที่ไม่ใช่ข้อมูล FTP แทรกมาในระหว่างการเชื่อมต่อ ไฟร์วอลล์ประเภทนี้ก็จะไม่รู้ ซึ่งสามารถแก้ไขปัญหาด้วยการหาไฟร์วอลล์ที่มีความสามารถในการติดตามการทำงานของชั้นแอปพลิเคชัน และทราบว่าการติดต่อตามรูปแบบโพรโตคอล ถูกต้องหรือไม่ โดยจะเรียกไฟร์วอลล์ชนิดนี้ว่า Application Proxy Firewall

- **แอปพลิเคชันพร็อกซี่ไฟร์วอลล์ (Application Proxy Firewall)**

ไฟร์วอลล์ประเภทนี้จะทำหน้าที่เป็นตัวแทน (Proxy) ในการส่งต่อ การเชื่อมต่อใด ๆ ไปยังเซิร์ฟเวอร์ ดังนั้นข้อดีประการแรกของไฟร์วอลล์ประเภทนี้ คือ บุคคลภายนอกจะไม่รู้หมายเลขไอพี

ของเครือข่ายภายในที่ขอเชื่อมต่อออกมาภายนอก นอกจากนี้แอปพลิเคชันพร็อกซี่จะทำหน้าที่ในการตรวจสอบรูปแบบการติดต่อ ว่ามีรูปแบบที่ถูกต้องตามโพรโตคอลนั้น ๆ หรือไม่ ทำให้มีความปลอดภัยเพิ่มขึ้น นอกจากนั้นไฟร์วอลล์แบบนี้ยังป้องกันการปลอมไอพีได้โดยเด็ดขาด

แต่การติดต่อแบบนี้ก็มีข้อเสียเช่นกัน คือ ไฟร์วอลล์แบบนี้จะทำงานได้ช้ากว่า เพราะมีการตรวจสอบมากกว่า และยังต้องสร้างแพ็คเก็ตใหม่ในทุก ๆ ครั้งด้วย และหากกรณีที่การเชื่อมต่อหนึ่งมีการแบ่งเป็นเซกเมนต์หลาย ๆ เซกเมนต์ด้วยแล้ว ไฟร์วอลล์ประเภทนี้ต้องรอให้ทุกเซกเมนต์ส่งมาจนครบก่อน จึงจะส่งต่อได้ ทำให้เกิดความล่าช้าในการทำงานขึ้น นอกจากนั้นการที่ไฟร์วอลล์ประเภทนี้ทำงานในระดับชั้นแอปพลิเคชัน หมายความว่า มันจะส่งต่อได้เฉพาะโพรโตคอลที่มันรู้จักเท่านั้น

จากข้อดีของไฟร์วอลล์แบบสเตทฟูล ที่มีความรวดเร็วในการทำงาน และข้อดีของไฟร์วอลล์แบบ แอปพลิเคชันพร็อกซี่ ที่มีความปลอดภัยสูง จึงทำให้มีผู้สร้างไฟร์วอลล์ที่ผสมผสานความสามารถของไฟร์วอลล์ทั้งสองขึ้น และเรียกไฟร์วอลล์แบบใหม่นี้ว่า Hybrid Firewall หรือบางผู้ผลิตจะเรียกว่า Adaptive Firewall ซึ่งจะแตกต่างกันไปตามผู้ผลิต บางผลิตภัณฑ์ก็ทำงานในแบบพร็อกซี่ สำหรับโพรโตคอลหลัก ๆ และแบบสเตทฟูลสำหรับโพรโตคอลทั่ว ๆ ไป บางผลิตภัณฑ์ก็ทำงานในแบบพร็อกซี่ ในช่วงแรกของการเชื่อมต่อ เพราะมีความปลอดภัยสูง และต่อมาหากเชื่อว่าการเชื่อมต่อนั้น เป็นการเชื่อมต่อตามปกติ ก็จะขยับลงมาทำงานในแบบสเตทฟูล เพราะมีความรวดเร็วในการทำงานมากกว่า

นอกจากนี้ในส่วนของแนวทางป้องกันการบุกรุกที่เกิดกับภายในระบบนั้นมีได้หลายวิธี เช่น การติดตั้งระบบตรวจจับการบุกรุก (IDS), การติดตั้งโปรแกรมป้องกันไวรัส หรือการติดตั้งโปรแกรมไฟร์วอลล์สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Firewall) เป็นต้น ซึ่งการทำงานของไฟร์วอลล์สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลอาศัยหลักเดียวกับ Firewall gateway ที่มีหน้าที่ในการตรวจสอบว่าแพ็คเก็ต หรือการเชื่อมต่อใดบ้างสามารถผ่านระหว่างเครื่องส่วนบุคคลกับระบบเครือข่ายภายนอก โดยอาศัยการตั้งกฎของการใช้งานไอพีแอดเดรส และพอร์ต ดังนั้นหากมีการขอการเชื่อมต่อจากระบบเครือข่ายที่ผิดปรกติ ไฟร์วอลล์จะปิดกั้นการเชื่อมต่อนั้นทันที

ในปัจจุบันนั้นไฟร์วอลล์สำหรับเครื่องส่วนบุคคลมีการใช้งานอย่างแพร่หลาย และมีผู้ผลิตหลายรายที่ได้ทำการพัฒนา โดยในโครงงานนี้ได้ทำการทดสอบกับระบบทดสอบที่มีการใช้งานไฟร์วอลล์สำหรับเครื่องส่วนบุคคลดังต่อไปนี้

- Windows Firewall
- ZoneAlarm Personal Firewall

2.2 ทฤษฎีที่เกี่ยวกับการทดสอบความปลอดภัยของระบบ

ทฤษฎีที่เกี่ยวกับการทดสอบความปลอดภัยของระบบในส่วนนี้จะเป็นการอธิบายเกี่ยวกับพื้นฐานของการทดสอบความปลอดภัยของระบบ (Penetration Test) โดยสามารถทำการอธิบายได้ดังต่อไปนี้

2.2.1 นิยามและความหมาย

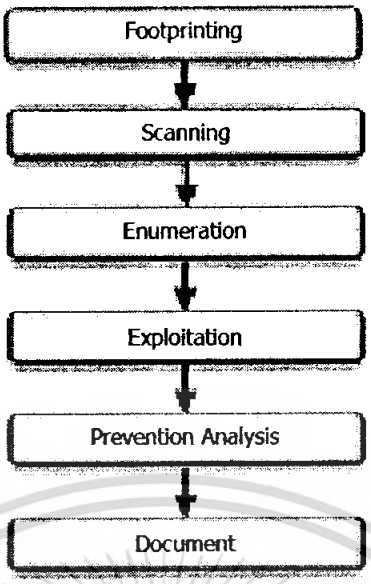
การทดสอบความปลอดภัยของระบบ (Penetration Test) คือ วิธีที่ใช้ในการประเมินความปลอดภัยของระบบคอมพิวเตอร์ หรือระบบเครือข่ายโดยการจำลองการโจมตีของผู้ใช้งานที่ประสงค์ร้าย (Hacker – malicious user) โดยกระบวนการที่ทำการวิเคราะห์ช่องโหว่ความปลอดภัยที่อาจมีอยู่ภายในระบบ (Vulnerabilities) ที่เกิดเนื่องจากหลายสาเหตุ ได้แก่ การปรับแต่งระบบที่ไม่เหมาะสม, ข้อบกพร่องทางด้านฮาร์ดแวร์/ซอร์ฟแวร์ ที่อาจจะทราบหรือไม่ทราบ, หรือความอ่อนแอของขั้นตอนการทำงานในกระบวนการหรือ เทคนิคในการรับมือ ผลของการวิเคราะห์นี้จะเกิดจากการโจมตีต่างๆของผู้บุกรุกที่อาจจะเกิดขึ้นได้ และทำการบุกรุกหาประโยชน์จากช่องโหว่ความปลอดภัย (Exploitation) ซึ่งปัญหาความปลอดภัยต่างๆที่ถูกพบจะถูกแสดงให้แก่เจ้าของระบบที่ทำการตรวจสอบ พร้อมด้วยการประเมินผลกระทบและข้อเสนอแนะเกี่ยวกับวิธีการป้องกันปัญหาที่พบในการทดสอบเหล่านั้น ซึ่งเจตนาของการทดสอบความปลอดภัยของระบบ คือ การหาความเป็นไปได้ของการโจมตี, ผลกระทบทางธุรกิจเมื่อถูกทำเอ็กซ์พลอยท์ (Exploit)สำเร็จ

2.2.2 เป้าหมายของการทดสอบความปลอดภัยของระบบ

1. เพื่อค้นหาช่องโหว่ความปลอดภัย และให้คำแนะนำเกี่ยวกับช่องโหว่ความปลอดภัย
2. เพื่อพัฒนาความปลอดภัยของระบบที่ทำงานทางด้านเทคนิค เช่น ไฟร์วอลล์ เราเตอร์
3. เพื่อทำให้ความปลอดภัยทางด้านไอทีได้รับการรับรองโดยกลุ่มบุคคลที่สามภายนอก
4. เพื่อพัฒนาความปลอดภัยของโครงสร้างพื้นฐานขององค์กรและบุคคล เช่น การทดสอบโดยใช้เทคนิค Social Engineering

2.2.3 ขั้นตอนของการทดสอบความปลอดภัยของระบบ

แนวคิดการทดสอบความปลอดภัยของระบบ (Penetration Test) จะแบ่งออกเป็น 6 ขั้นตอนดังนี้



รูปที่ 2.3 ขั้นตอนการทดสอบความปลอดภัยของระบบ

การแกะรอย (Footprinting) - ก่อนที่ผู้บุกรุกจะทำการบุกรุกระบบนั้น มักจะทำการรวบรวมข้อมูลต่างๆของระบบเป้าหมายจากฐานข้อมูลอินเทอร์เน็ต เพื่อให้ได้มาซึ่งข้อมูลเกี่ยวกับเทคโนโลยีดังต่อไปนี้ : อินเทอร์เน็ต อินทราเน็ต การบริหารการเชื่อมต่อระยะทางไกล และเอ็กซ์ทราเน็ต โดยใช้เครื่องมือ เช่น whois, SamSpade, traceroute / tracert, nslookup ในการหาข้อมูลต่างๆในการกรองให้เหลือขอบเขตเท่าที่สนใจ เช่น ชื่อโดเมน เน็ตเวิร์คบล็อค และหมายเลขไอพีของคอมพิวเตอร์ภายในระบบ โดยการแกะรอยนั้น แบ่งออกเป็น 3 ขั้นตอน คือ การกำหนดขอบเขตของการแกะรอย การรวบรวมรายละเอียดต่างๆของเครือข่ายเป้าหมาย และการหาข้อมูลจาก DNS Server

การสแกน (Scanning) - การสแกนพอร์ตระบบเป้าหมายที่ต้องการทดสอบ เพื่อตรวจสอบว่าเครื่องเป้าหมายใดบ้างที่ทำงาน และมีหมายเลขพอร์ตอะไรที่ทำงานอยู่บ้าง รวมทั้งการค้นหาประเภท และเวอร์ชันของระบบปฏิบัติการ และแอปพลิเคชัน

การรวบรวมรายละเอียด (Enumeration) - ค้นหาและรวบรวมรายละเอียดต่างๆ ได้แก่ การค้นหาเกี่ยวกับบัญชีรายชื่อผู้ใช้งาน และ ทรัพยากรที่ได้ทำการแชร์ไว้ของระบบเป้าหมาย รวมถึงช่องโหว่ของระบบปฏิบัติการและ service จากข้อมูลที่หามาได้

การบุกรุกหาประโยชน์จากช่องโหว่ความปลอดภัย (Exploitation) – การโจมตี เพื่อให้ได้รับประโยชน์ต่างๆ เช่น การยกระดับสิทธิ การทำให้ระบบเป้าหมายหยุดการทำงาน และอื่นๆ

การวิเคราะห์การป้องกัน (Prevention Analysis) - รวบรวมและวิเคราะห์ช่องโหว่ความปลอดภัยต่างๆที่พบในการทดสอบ และให้ข้อเสนอแนะเกี่ยวกับวิธีการป้องกันปัญหาช่องโหว่ความปลอดภัยที่พบ

การทำเอกสาร (Document) – นำผลการทดสอบความปลอดภัยของระบบ จัดให้อยู่ในรูปแบบของเอกสารที่สามารถอ่าน และเข้าใจได้ง่าย

2.2.4 กล่องดำ และกล่องขาว (Black box vs. White box)

ในการทดสอบความปลอดภัยของระบบทำได้หลายแนวทาง ขึ้นกับรายละเอียดของระบบที่ทำการทดสอบที่ผู้ทดสอบทราบ ซึ่งแบ่งการทดสอบออกเป็น 2 ประเภท คือ

- **กล่องดำ (Black Box)** จะเป็นการทดสอบจากการสมมติว่าไม่ทราบข้อมูลอะไรเลยเกี่ยวกับโครงสร้างของระบบที่ทำการทดสอบ ซึ่งสิ่งที่ผู้ทำการทดสอบต้องทำในขั้นตอนแรกของการวิเคราะห์ คือการหาตำแหน่งและขนาดของระบบ โดยทั่วไปแล้วเรียกขั้นตอนนี้ว่า การแกะรอย
- **กล่องขาว (White box)** จะทดสอบโดยสมมติว่า ผู้ทำการทดสอบนั้นทราบรายละเอียดเกี่ยวกับ โครงสร้างพื้นฐานของระบบที่ถูกทดสอบ ซึ่งมักประกอบด้วย โครงสร้างของเครือข่าย, ซอร์สโคด (source code) และรายละเอียดของหมายเลขไอพี

นอกจากทั้ง 2 รูปแบบนี้แล้วยังมีรูปแบบของการทดสอบอีกประเภทคือ กล่องสีเทา (Gray Box) ซึ่งอาจจะมีการเปิดเผยข้อมูลให้แก่ผู้ทดสอบ และทำการซ่อนรายละเอียดบางส่วนเอาไว้

ข้อดีของแต่ละวิธีการทดสอบความปลอดภัยของระบบนั้น จะมีลักษณะต่างๆกัน โดยกล่องดำจะเป็นการจำลองการกระทำของผู้ไม่ประสงค์ดีอย่างแท้จริง แต่ปฏิเสธไม่ได้ว่าในความจริงแล้วเป้าหมายที่ถูกโจมตีนั้นจากรายละเอียดที่ผู้บุกรุกได้ทราบก่อนแล้ว โดยเฉพาะอย่างยิ่งเมื่อผู้บุกรุกเป็นบุคคลภายในองค์กร (Insider) เช่น พนักงานหรืออดีตพนักงานที่ไม่พอใจกับองค์กร เป็นต้น ซึ่งจะใช้รายละเอียดขององค์กรเพื่อทำความเสียหายให้กับองค์กร ซึ่งก่อให้เกิดความเสียหายอย่างมากขึ้น

2.2.5 ระเบียบวิธีของการทดสอบความปลอดภัยของระบบ

Open Source Security Testing Methodology Manual (OSSTMM) เน้นไปที่รายละเอียดทางด้านเทคนิคที่จำเป็นในการทดสอบในแต่ละขั้นตอนว่า อะไรควรทำก่อน / ระหว่าง และภายหลังการทดสอบความปลอดภัย และผลลัพธ์ที่ได้จากการทดสอบเป็นอย่างไร OSSTMM นั้นอาจกล่าวได้ว่าเป็น หลักเกณฑ์สัญญาของทั้งฝ่ายผู้ทดสอบ และทางฝั่งลูกค้า ว่าการทดสอบนั้นเริ่มจากการปฏิเสธการโฆษณาที่เป็นเท็จจากผู้ทดสอบ ไปถึงลูกค้าว่าคาดหวังว่าจะได้รับอะไรบ้าง

Information Systems Security Assessment Framework (ISSAF) โดย Open Information Systems Security Group เป็นระเบียบวิธีใหม่ที่จะพิจารณาดูโครงสร้างการทำงานที่แบ่งการประเมินความปลอดภัยของข้อมูลระบบออกเป็นชั้นๆภายในโดเมนที่หลากหลาย และการประเมิน

รายละเอียดพิเศษ หรือการทดสอบเกณฑ์สำหรับแต่ละโดเมน ซึ่งมุ่งหมายที่จะจัดหาฟิลด์ของขาเข้าบนการประเมินความปลอดภัยที่มีผลต่อชีวิตจริง ISSAF ควรถูกใช้เพื่อให้บรรลุความต้องการในการประเมินความปลอดภัยขององค์กรและอาจจะเพิ่มการใช้การอ้างอิงข้อมูลด้านความปลอดภัยอื่นๆ ISSAF ประกอบด้วยมุมมองที่สำคัญของการดำเนินการด้านความปลอดภัย การประเมิน และการทำเพิ่มการป้องกัน (Hardening) เกี่ยวกับปัญหาช่องโหว่ที่มีอยู่

2.3 ทฤษฎีการสแกนช่องโหว่คอมพิวเตอร์

เมื่อได้เริ่มทำการทดสอบระบบจะมีการรวบรวมข้อมูลต่างๆของระบบเป้าหมายด้วยวิธีการแกะรอย แล้วจะนำหมายเลขไอพีที่เป็นส่วนหนึ่งของผลการแกะรอยมาทำการสแกน ซึ่งถือได้ว่าเป็นขั้นตอนแรกของการโจมตี เพื่อตรวจสอบว่าเครื่องเป้าหมายใดบ้างที่ทำงาน และมีหมายเลขพอร์ต (TCP / UDP) อะไรบ้างที่ทำงานอยู่ โดยการสแกนพอร์ตไปยังหมายเลขไอพีเป้าหมายที่เชื่อมต่ออินเทอร์เน็ต เมื่อได้ผลของการสแกนจึงนำไปทำหาประเภทของระบบปฏิบัติการ และเวอร์ชันของบริการ (service)

ในการโจมตีระบบคอมพิวเตอร์นั้น ขั้นตอนแรก คือ การสแกน เพื่อตรวจสอบว่าเครื่องเป้าหมายใดบ้างที่ทำงาน และมีหมายเลขพอร์ต (TCP / UDP) อะไรบ้างที่ทำงานอยู่ โดยการสแกนพอร์ตไปยัง IP address เป้าหมายที่เชื่อมต่ออินเทอร์เน็ต เมื่อได้ผลของการสแกน แล้วจึงนำไปทำการหาประเภทของระบบปฏิบัติการ และเวอร์ชันของบริการ หลังจากนั้นจึงนำผลที่ได้ไปวิเคราะห์ว่า มีแอปพลิเคชันอะไรบ้างที่ทำงานอยู่ ซึ่งเครื่องมือในการสแกนมักจะมีคุณสมบัติของการทำ s อยู่ด้วย ได้แก่ Nmap, Netscan tools โดยในการสแกนนี้จะแบ่งประเภทการทำงานออกเป็น 3 รูปแบบดังต่อไปนี้

2.3.1 Network Ping Sweep

Network Ping Sweep เป็นการสแกนด้วยการ ping ไปยังเป้าหมายจำนวนมากพร้อมๆกัน ในลักษณะของการกวาดยิง เพื่อทำการตรวจสอบว่าเครื่องปลายทางใดบ้างที่เปิดทำงานอยู่ โดยโปรแกรมที่ทำงานตามลักษณะนี้ ได้แก่ fping, gping, nmap, Netscan tools, superscan โดยจะทำงานได้เฉพาะกรณีที่ทางเครื่องปลายทางนั้นได้เปิดให้สามารถส่ง ICMP Reply กลับมาได้ ถ้าเครื่องปลายไม่อนุญาตควรที่จะใช้วิธีการสแกนพอร์ต ที่จะใช้เวลาในการทำงานมากกกว่า แต่มีประสิทธิในการสแกนมากกว่า

2.3.2 การสแกนพอร์ต (Scan Port)

การสแกนพอร์ต (Scan Port) เป็นกระบวนการในการติดต่อเข้าไปที่พอร์ตทีซีพี/ยูดีพี ของเครื่องปลายทาง เพื่อค้นหาว่ามีบริการ / พอร์ต อะไรบ้างที่ทำงานในสถานะ LISTENING เพื่อที่จะ

ใช้ในการตรวจสอบประเภทของระบบปฏิบัติการและแอปพลิเคชันที่ใช้งานอยู่ในระบบ เนื่องจากระบบปฏิบัติการหรือบริการที่ทำงานอาจมีข้อบกพร่องเกี่ยวกับความปลอดภัยอยู่ โดยประเภทของการสแกนมีหลายประเภท ดังนี้

- *Address Resolution Protocol (ARP) scans* จะตรวจหาอุปกรณ์ที่ทำงานในเครือข่ายโดยการส่งชุดแพ็คเก็ต ARP broadcasts และเพิ่มค่าของฟิลด์ที่บรรจุหมายเลขไอพีของเหยื่อเป้าหมายในแต่ละแพ็คเก็ต broadcast การสแกนชนิดนี้จะได้รับผลตอบสนองจากอุปกรณ์ที่มีหมายเลขไอพีบนเครือข่ายออกมาในรูปแบบของหมายเลขไอพีของแต่ละอุปกรณ์ การสแกน แบบนี้จึงทำการ map out ได้ทั้งเครือข่ายอย่างมีประสิทธิภาพ แต่มีข้อจำกัดคือสามารถใช้ได้ในเครือข่ายเดียวกันเท่านั้น

- *The Vanilla TCP Connect Scan* เป็นเทคนิคการสแกนพอร์ตขั้นพื้นฐานและง่ายที่สุด คือจะใช้ connect system call ของระบบปฏิบัติการไปบนเครื่องเป้าหมาย ด้วยกลไกมาตรฐานที่เรียกว่า TCP three-way handshake เพื่อเปิดการเชื่อมต่อไปยังทุกๆ พอร์ตที่เปิดอยู่ การสแกนชนิดนี้สามารถจับได้ง่ายมาก โดยล็อก (log) ต่าง ๆ ของเครื่องเป้าหมายจะแสดงการร้องขอการเชื่อมต่อ (connection requests) และข้อความแสดงข้อผิดพลาด (error messages) สำหรับบริการที่ตอบรับการเชื่อมต่อนั้น หรืออาจป้องกันโดยติดตั้งไฟร์วอลล์ แต่การสแกนแบบนี้มักได้รายละเอียดมากกว่าการสแกน TCP SYN

- *The TCP SYN (Half Open) scans* เทคนิคนี้บางครั้งถูกเรียกว่าการสแกนแบบ half open เนื่องจากเป็นการเชื่อมต่อที่ไม่สมบูรณ์เป็นการส่งเฉพาะเซ็กเมนต์ที่ตั้งค่าแฟล็ก SYN ไปยังพอร์ตของเครื่องคอมพิวเตอร์ปลายทาง ซึ่งเครื่องปลายทางจะส่ง SYN/ACK กลับมาหากพอร์ตนั้นเปิดอยู่ ซึ่งก็สรุปได้ว่าพอร์ตดังกล่าวอยู่ในสถานะ listening แต่ถ้าพอร์ตถูกปิดอยู่ เป้าหมายก็จะส่ง RST (Reset) กลับมาแทน เทคนิคการสแกนรูปแบบนี้สามารถสแกนเป้าหมายได้อย่างรวดเร็ว และยากต่อการตรวจจับ แต่หากเชื่อมต่อไปยังหลาย ๆ พอร์ตจากแหล่งเดียวกันก็อาจถูกตรวจจับได้เช่นกัน

- *The TCP FIN Scan* เทคนิคนี้สามารถที่จะทะลุผ่านไฟร์วอลล์ส่วนใหญ่ เนื่องจากระบบที่ทำการสแกนจะส่งเซ็กเมนต์ที่เซ็ตแฟล็ก FIN ไปยังเครื่องเป้าหมาย สำหรับพอร์ตต่าง ๆ ที่ปิดอยู่จะตอบสนองกลับไปด้วย RST ส่วนพอร์ตที่เปิดจะไม่สนใจเซ็กเมนต์เหล่านั้นเลย โดยปกติแล้ว เทคนิคนี้มักใช้ได้กับเครื่องปลายทางที่รันบนยูนิกส์

- *The TCP Xmas Tree Scan* ถูกใช้เพื่อหาพอร์ตบนเครื่องเป้าหมายที่อยู่ในสถานะ listening โดยจะไม่ส่งแพ็คเก็ตทีซีพี ทั้ง 3 ตัวซึ่งเป็นที่สังเกตง่าย คือ SYN-ACK-RST แต่จะส่งเซ็กเมนต์ที่เซ็ตแฟล็ก FIN, URG และ PSH ไปยังพอร์ตเป้าหมาย เพื่อหลบหลีกการตรวจจับให้มากที่สุด ซึ่งหากทีซีพี/ไอพี ของเครื่องคอมพิวเตอร์ปลายทางทำงานตรงตาม RFC 793 อย่างครบถ้วน

ถ้าพอร์ตทีซีพีของเครื่องเป้าหมายปิดอยู่ พอร์ตนั้นก็จะส่งแพ็คเก็ตทีซีพี RST กลับมา แต่ถ้าพอร์ตเปิดอยู่ก็จะไม่สนใจเซ็กเมนต์นั้นเลย

- *The TCP Null Scan* เทคนิคนี้จะส่งเซ็กเมนต์ที่แฟล็กทุกตัวถูกรีเซ็ตเป็น 0 ทั้งหมด ซึ่งมีแต่ sequence number ไปยังเครื่องเป้าหมาย ซึ่งหากทีซีพี/ไอพี ของเครื่องคอมพิวเตอร์ปลายทางทำงานตรงตาม RFC 793 อย่างครบถ้วน เครื่องปลายทางจะส่งแพ็คเก็ตทีซีพี RST ของทุกพอร์ตที่ปิดกลับมาให้ ทำให้เรารู้ว่ามีพอร์ตใดเปิดอยู่บ้าง โดยทั่วไปแล้วเซ็กเมนต์ประเภทนี้มักจะไม่มีผู้สนใจ นอกจากการใช้เซ็กเมนต์เหล่านี้ในการสแกนพอร์ตแล้วยังสามารถนำไปใช้ในการตรวจสอบระบบปฏิบัติการของเครื่องเป้าหมายได้อีกด้วย เนื่องจากระบบปฏิบัติการแต่ละแบบจะมีการตอบสนองที่ไม่เหมือนกัน

- *The TCP ACK Scan* เป็นเทคนิคที่ใช้ค้นหาเว็บไซต์ที่เปิดบริการอยู่ แต่ปฏิเสธการตอบสนองต่อ ICMP ping หรือเพื่อค้นหากฎ (rule) หรือนโยบาย (policy) ต่าง ๆ ที่ตั้งไว้ที่ไฟร์วอลล์เพื่อตรวจสอบดูว่าไฟร์วอลล์นั้นๆ ทำหน้าที่แค่เพียงสามารถกรองแพ็คเก็ตอย่างง่าย ๆ หรือเป็นไฟร์วอลล์ที่มีความฉลาดพอสมควร และใช้เทคนิคการกรองแพ็คเก็ตขั้นสูง โดยเทคนิคการสแกนแบบนี้จะใช้แพ็คเก็ตทีซีพีที่มีแฟล็กเป็น ACK ส่งไปยังพอร์ตเครื่องปลายทาง ถ้าพอร์ตเปิดอยู่เครื่องเป้าหมายจะส่ง RST กลับมา แต่ถ้าปิดอยู่ก็จะไม่สนใจแพ็คเก็ตนั้น

- The TCP Reverse Ident scan เป็นเทคนิคที่สามารถตรวจหาชื่อของเจ้าของแต่ละโพรเซสที่เป็นการเชื่อมต่อด้วยทีซีพี บนเครื่องเหยื่อเป้าหมาย เทคนิคการสแกนชนิดนี้จะทำให้ระบบที่ทำการโจมตีสามารถเชื่อมต่อเข้าไปยังพอร์ตที่เปิดอยู่และใช้โพรโตคอลที่ใช้ระบุตัวตน ในการค้นหาว่าใครเป็นเจ้าของโพรเซสบนเครื่องเป้าหมายได้

- *The TCP Windows Scan* เทคนิคการสแกนนี้จะตรวจสอบพอร์ตที่เปิดอยู่ รวมทั้งตรวจดูว่า พอร์ตใดบ้างที่ถูกกรองเอาไว้ไม่ให้ผ่านเข้าไปถึง และพอร์ตหมายเลขใดได้รับการอนุญาตไว้บ้าง โดยอาศัยช่องโหว่จากความผิดปกติบางอย่างในการแจ้งค่า TCP Windows Size ของโพรโตคอลทีซีพี/ไอพี

- *The TCP RPC Scan* เทคนิคการสแกนนี้ใช้งานได้เฉพาะกับเครื่องปลายทางที่รันบนยูนิกซ์เท่านั้น เพื่อตรวจสอบดูว่ามีเซอร์วิสใดทำงานอยู่บนเซอร์วิส RPC บ้าง รวมทั้งตรวจดูเวอร์ชันของเซอร์วิสนั้น และโปรแกรมอื่นที่เกี่ยวข้อง

- The FTP Bounce Attack จะใช้โพรโตคอล FTP สำหรับสร้างการเชื่อมต่อบริการ FTP ของ ตัวกลาง (proxy) เทคนิคการสแกนแบบนี้ ผู้โจมตีจะสามารถซ่อนตัวอยู่หลัง FTP server และสแกนเป้าหมายอื่น ๆ ได้โดยไม่ถูกตรวจจับ ดังนั้น FTP servers ส่วนใหญ่จะมีการ disable บริการของ FTP เพื่อความปลอดภัยของระบบ

- *The UDP ICMP Port scanning* ใช้โพรโตคอล UDP โดยจะส่งคาต้าแกรม UDP ไปยังพอร์ตเป้าหมาย ถ้าพอร์ตปิดอยู่เครื่องปลายทางจะตอบกลับมาด้วยแพ็คเก็ต ICMP type PORT UNREACHABLE ถ้าพอร์ตนั้นเปิดอยู่เครื่องปลายทางจะไม่ส่งแพ็คเก็ตกลับมา เทคนิคนี้ใช้ในการสแกนหาพอร์ตหมายเลขสูง ๆ โดยเฉพาะในระบบ Solaris แต่จะช้าและไม่น่าเชื่อถือ เนื่องจากโพรโตคอล UDP เป็นลักษณะ Connectionless ที่ไม่รับรองว่า แพ็คเก็ตที่ส่งไปจะถึงเครื่องปลายทางครบถ้วนหรือไม่
- *The ICMP Ping-sweeping Scan* จะใช้ ping เพื่อกวาดดูว่ามีระบบไหนที่เปิดใช้งานอยู่ เครือข่ายส่วนใหญ่จึงมีการกรอง หรือไม่เปิดใช้งานในส่วนนี้

สำหรับในส่วนเครื่องมือที่ใช้ในการสแกนมีจำนวนมาก เช่น Strobe, udp_scan, netcat, nmap, NetScan Tools Pro 2000, SuperScan, NTO Scanner, WinScan, ipEye, WUPS ขึ้นกับความชำนาญของผู้ทำการทดสอบ และความยากง่ายในการใช้งานในแต่ละโปรแกรม

2.3.3 Stack Fingerprinting

Stack Fingerprinting เป็นเทคโนโลยีที่ช่วยทำให้สามารถค้นหาประเภทของระบบปฏิบัติการที่ถูกต้องได้ ซึ่งมีเปอร์เซ็นต์ความน่าเชื่อถือสูง โดยอาศัยหลักการที่ว่าโปรแกรมในส่วนสแต็ค ของทีซีพี/ไอพี ล้วนแต่พัฒนาขึ้นโดยทีมงานต่างกัน ย่อมมีการเขียนโปรแกรมที่ต่างกัน ส่วนที่เหมือนกันคือเป็นไปตามมาตรฐาน RFC 793 แต่ RFC 793 ก็ไม่ได้ระบุถึงการเชื่อมต่อในทุก ๆ รูปแบบไว้ เพียงแต่ระบุการเชื่อมต่อเฉพาะส่วนที่ใช้งานจริง ๆ เท่านั้น ดังนั้นหากส่งแพ็คเก็ตที่มีการตั้งค่าแฟล็กแปลก ๆ ที่ไม่ได้กำหนดไว้ใน RFC 793 แล้ว ส่วนสแต็ค ของทีซีพี/ไอพี ที่พัฒนาขึ้นมาต่างกันก็อาจให้ผลตอบกลับที่ต่างกันได้

โดย Stack Fingerprinting นั้นยังแบ่งลักษณะการทำงาน ออกเป็น 2 ประเภท คือ

1.) Active Stack Fingerprinting การพยายามที่หาประเภทระบบปฏิบัติการโดยการสแกนไปยังเครื่องปลายทางโดยตรง ซึ่งมีเครื่องมือที่ใช้ในการทำงาน เช่น Nmap, Queso
2.) Passive Stack Fingerprinting การพยายามที่หาประเภทระบบปฏิบัติการ โดยการดอยมอนิเตอร์เน็ตเวิร์คทราฟฟิก เพื่อค้นหาประเภทของระบบปฏิบัติการ เช่น siphon

การตรวจสอบด้วย Stack Fingerprinting นี้ สามารถเริ่มด้วยการคาดเดาอย่างมีเหตุผล เพื่อให้มีความน่าเชื่อถือสูงสุด Stack Fingerprinting จำเป็นที่อาศัยกลไกกลของการติดต่อไปยังพอร์ตที่เปิดอยู่อย่างน้อยหนึ่งพอร์ต (Nmap สามารถคาดเดาได้อย่างมีเหตุผล ถึงแม้ว่าไม่ได้มีการติดต่อไปที่พอร์ตใดเลย แต่ผลที่ได้อาจจะไม่น่าเชื่อถือมากนัก) ซึ่งวิธีการ Stack Fingerprinting นี้ไม่ได้มีรูปแบบตายตัวแน่นอน เพราะอาศัยความไม่เหมือนกันของส่วนสแต็ค ของทีซีพี/ไอพี ดังนั้น

หากเราสามารถจัดชุดของแพ็คเก็ตที่ส่งออกไปยังระบบปฏิบัติการต่าง ๆ แล้วให้ผลตอบกลับมาไม่เหมือนกันเลย โดยมีรูปแบบการตรวจสอบของ Active Stack Fingerprinting ที่มีการใช้งานกันอย่างกว้างขวาง มีดังต่อไปนี้

- *FIN Probe* ใช้ส่งแพ็คเก็ตที่ตั้งค่าโดยตั้งค่าแฟล็ก FIN โดยตามมาตรฐาน RFC 793 ระบุไว้ว่า พฤติกรรมที่ถูกต้องจะต้องไม่มีการส่งแพ็คเก็ดอะไรตอบสนองกลับไป แต่ในบางระบบปฏิบัติการจะตอบสนองด้วยแพ็คเก็ตที่ตั้งค่าแฟล็ก FIN และ ACK กลับมา
- *Bogus Flag Probe* ใช้ส่งแพ็คเก็ตที่ตั้งค่าแฟล็ก SYN พร้อมทั้งตั้งค่าบางบิตที่ไม่ได้ใช้งาน ในบางระบบปฏิบัติ เช่น Linux จะตอบสนองด้วยการตั้งค่าบางตัวในแพ็คเกจตอบกลับ
- *Initial Sequence Number (ISN) Sampling* ใช้การตรวจหารูปแบบของเลขลำดับ (Sequence Number) ที่อยู่ในเฮดเดอร์ของแพ็คเกจ ว่ามักจะเป็นค่าอะไร
- *"Don't Fragment Bit" monitoring* ในบางระบบปฏิบัติการจะมีการตั้งค่าบิตนี้ไว้เพื่อเพิ่มความเร็วในการส่งข้อมูล ให้มอนิเตอร์บิตนี้ว่าระบบปฏิบัติการไหน ตั้งค่าบิตนี้บ้าง
- *TCP Initial Window Size* ใช้ตรวจหาขนาดของหน้าต่างของทีซีพี (TCP Window) เนื่องจากบางระบบปฏิบัติการได้ทำการจำกัดขนาดของหน้าต่างของทีซีพี (TCP Window) ว่าเป็นเท่าไร ซึ่งเป็นค่านี้มักเป็นค่าเฉพาะของแต่ละระบบปฏิบัติการ
- *ACK Value* ระบบปฏิบัติการต่าง ๆ มักตั้งค่าในฟิลด์ ACK ไม่เหมือนกัน ในบางระบบปฏิบัติการตั้งค่าให้เท่ากับ SYN บางระบบเป็น SYN+1
- *ICMP Error Message Quenching* ในบางระบบปฏิบัติการอาจทำตามมาตรฐาน RFC 1812 โดยจำกัดอัตราของการส่งรหัสความผิดพลาด (Error Message) ดังนั้นหากส่ง UDP ไปยังพอร์ตหมายเลขสูง ๆ แล้วนับจำนวนแพ็คเก็ตแจ้งความผิดพลาด (ICMP type PORT UNREACHABLE Message) ที่ได้รับมา
- *ICMP Message Quoting* เมื่อพบข้อผิดพลาดเกี่ยวกับโพรโตคอลทีซีพี/ไอพี แต่ละระบบปฏิบัติการจะให้ข้อมูลและสาเหตุ มาในแพ็คเกตของ ICMP ไม่เท่ากัน ซึ่งอาจทำให้คาดเดาได้
- *ICMP error message-echoing integrity* บางระบบปฏิบัติการอาจดัดแปลงเฮดเดอร์แพ็คเก็ต IP เมื่อมีการส่ง ICMP error message ด้วยการตรวจสอบลักษณะการดัดแปลงดังกล่าวสามารถใช้ในการคาดเดาได้
- *Type of Service (TOS)* ใช้ตรวจสอบฟิลด์ Type of Service ที่อยู่ในแพ็คเก็ต ICMP ประเภท port unreachable โดยปกติแล้วหลายๆ ระบบปฏิบัติการจะใช้ค่า 0 แต่บางระบบใช้ค่าอื่น
- *Fragmentation handling* แต่ละระบบปฏิบัติการจะมีการจัดการกับแพ็คเก็ตที่ถูกแฟร็กเมนต์ไม่เหมือนกัน เมื่อมีการประกอบแพ็คเก็ตขึ้นเป็นแพ็คเก็ตที่สมบูรณ์อาจจะเขียนทับแพ็คเก็ตย่อยอันเก่าด้วยแพ็คเก็ตอันใหม่ หรือในบางระบบก็ทำในทางตรงกันข้าม ซึ่งใช้ในการคาดเดาได้

- *TCP Option* ถูกกำหนดไว้ในมาตรฐาน RFC 793, 1323 ซึ่งผู้ผลิตหลายรายได้มีการอิมพลีเม็นต์ตัวเลือกพิเศษไปไว้ในระบบปฏิบัติการของตัวเอง ดังนั้นการทดสอบด้วยการตั้งค่าตัวเลือกต่างๆ เช่น no operation, maximum segment size, timestamps เพื่อให้ในการตั้งสมมติฐานที่เกี่ยวกับระบบปฏิบัติการที่ทำงานอยู่เครื่องเป้าหมาย

โดยทั่วไปแล้วไม่ควรทำสแกนเครื่องของผู้อื่นโดยไม่ได้รับอนุญาต เนื่องจากผิดหลักจรรยาบรรณของการโจมตี (Ethical Hacking) และอาจมีโทษตามหลักกฎหมาย พระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์

2.4 ทฤษฎีที่เกี่ยวข้องกับ Exploitation

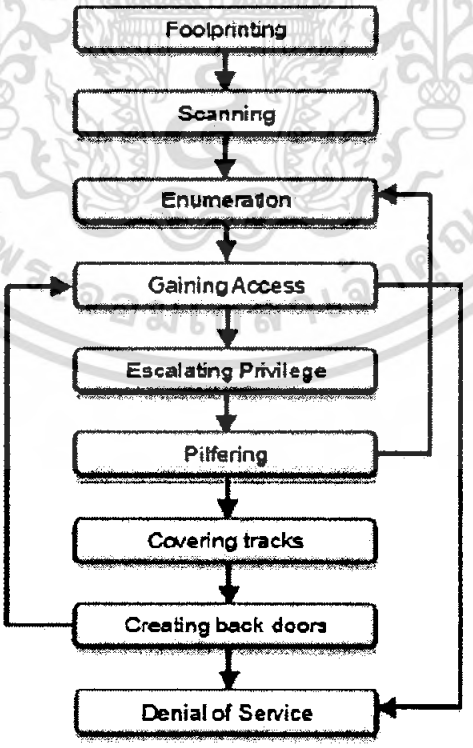
"Exploitation" มี 2 ความหมาย คือ

1. การกระทำเพื่อประโยชน์ใดๆ :: การใช้

2. การกระทำที่ไม่สมควร โหดร้าย หรือเป็นการเห็นแก่ตัว เพื่อให้บุคคลหนึ่งได้รับประโยชน์

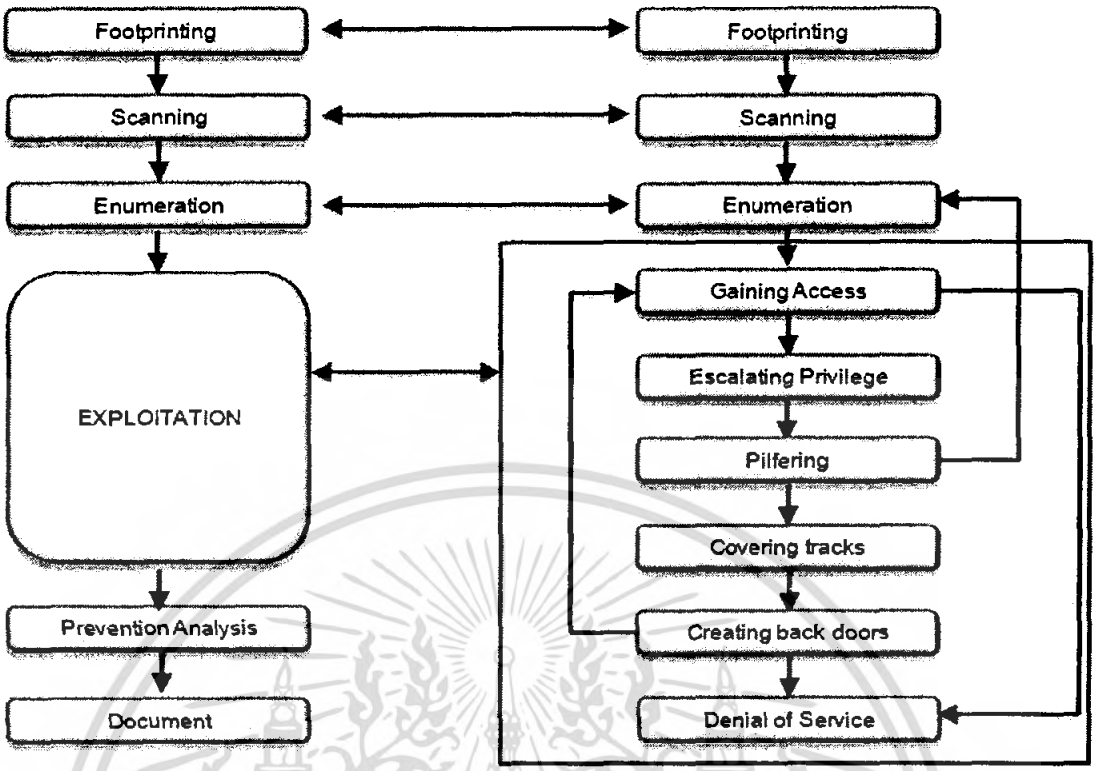
2.4.1 พฤติกรรมของผู้บุกรุก

แบบแผนวิธีการเจาะระบบของผู้บุกรุกนั้นจะมีรูปแบบดังต่อไปนี้



รูปที่ 2.3 แบบแผนวิธีการเจาะระบบของผู้บุกรุก

- *การแกะรอย (Footprinting)* ทำการรวบรวมข้อมูลต่างๆของระบบเป้าหมายจากฐานข้อมูลอินเทอร์เน็ต รวมถึงเครื่องมือต่างๆ เช่น whois, search engine, dig, nslookup, Sam Spade เพื่อกรองให้เหลือขอบเขตเท่าที่สนใจ เช่น ชื่อโดเมน, เน็ตเวิร์คบล็อค และหมายเลข IP address ของคอมพิวเตอร์ภายในระบบ
- *การสแกน (Scanning)* การประเมินสถานการณ์ของเป้าหมาย และการแยกแยะค้นหารายชื่อเซอร์วิสที่ทำงานอยู่ โดยพุ่งความสนใจไปที่ช่องทางในการเข้าโจมตีช่องโหว่ที่มีในเซอร์วิสเหล่านั้น
- *การรวบรวมรายละเอียดต่างๆ (Enumeration)* เป็นการรวบรวมรายละเอียดต่างๆ โดยการค้นหาเกี่ยวกับบัญชีรายชื่อผู้ใช้งาน ,ทรัพยากรที่ได้ทำการแชร์ที่ไม่ได้รับการปกป้องไว้
- *การได้รับสิทธิในการเข้าถึงระบบ (Gaining Access)* เป็นจุดที่พยายามในการเข้าถึงเป้าหมายอย่างรัดกุม โดยอาจใช้เทคนิคของการดักจับรหัสผ่านจากเครือข่าย, การทำ Buffer Overflow, การขโมยไฟล์ที่ทำการเก็บรหัสผ่าน, การคาดเดารหัสผ่านแบบ Brute Force ด้วยเครื่องอย่างเช่น TCPDump, NAT, Legion
- *การยกระดับสิทธิให้เท่าเทียมผู้ดูและระบบ (Escalating Privilege)* เมื่อได้สิทธิของผู้ใช้งานทั่วไปในการเข้าระบบ แล้วผู้บุกรุกจะพยายามเพื่อที่จะยกระดับสิทธิของตนเองให้สามารถควบคุมระบบทั้งหมด โดยการเทคนิค เช่น แคร็กรหัสผ่าน, เอ็กซ์พลอยท์ช่องโหว่ที่มีอยู่ ด้วยเครื่องมือต่างๆ เช่น Enum, Exploit Code
- *การขโมยข้อมูลเพิ่มเติม (Pilfering)* เป็นกระบวนการที่ใช้ในการรวบรวมข้อมูลอีกครั้ง เพื่อหากลไกในการเข้าระบบอื่นๆ ที่ระบบปัจจุบันนั้นได้ให้ความเชื่อถืออยู่
- *การปิดบังอำพรางตัว (Covering tracks)* เป็นขั้นตอนที่มักกระทำทันทีเมื่อสามารถเข้าครอบครองเป้าหมายได้ โดยการลบล็อกไฟล์ หรือการใช้เครื่องมือประเภท Rootkit
- *การสร้างประตูทางลับไว้ (Creating back doors)* เป็นขั้นตอนของการสร้างประตูลับในระบบ เพื่อความสะดวก การเข้าใช้งานในสิทธิของผู้ดูแลระบบในครั้งถัดไปที่ผู้บุกรุกเข้ามา โดยการเทคนิคต่างๆ เช่น การสร้างบัญชีรายชื่อปลอม, การตั้งเวลาให้แบตช์จ๊อบทำงาน, การฝังโปรแกรมไว้กับสตาร์ทอัพเอ็นทรี, การติดตั้งกลไกในการมอร์นิเตอร์, การแทนที่ไฟล์ปกติด้วยโปรแกรมโทรจัน ซึ่งมีเครื่องมือที่ใช้งาน เช่น netcat, VNC, keystroke loggrts
- *การทำให้ระบบเป้าหมายปฏิเสธการให้บริการ (Denial of Service)* ถ้าผู้บุกรุกไม่สามารถทำการโจมตีระบบได้สำเร็จ พวกเขามักเลือกที่จะใช้ความพยายามครั้งสุดท้ายในการโจมตีด้วยโปรแกรม DoS เพื่อทำให้ระบบเป้าหมายหยุดให้บริการ โดยการใช้เทคนิคต่างๆ เช่น SYN flood, DDoS, DoS



รูปที่ 2.4 การเปรียบระหว่าง Penetration Test และพฤติกรรมของผู้บุกรุก

2.4.2 ประเภทของการบุกรุก

การบุกรุกเข้าสู่ระบบแบ่งตามลักษณะการบุกรุกออกเป็น 3 ประเภทหลักๆ ดังนี้

1. การบุกรุกทางกายภาพ (Physical Intrusion) ผู้บุกรุกจะพยายามบุกรุกที่เครื่องคอมพิวเตอร์โดยตรง ซึ่งอาจจะใช้สิทธิพิเศษจากการทำงานที่คอนโซล หรือถอดย้ายอุปกรณ์ เช่น ฮาร์ดดิสก์ ซึ่งอาจนำไปเขียน หรืออ่านภายหลัง หรือบายพาสไบออสได้

2. การบุกรุกทางระบบ (System Intrusion) ผู้บุกรุกมักเป็นผู้ใช้ที่มีสิทธิต่ำ ถ้าระบบไม่ได้ทำการแพตช์ (Patch) ที่สามารถแก้ไขข้อบกพร่องของโปรแกรมแล้ว อาจเป็นช่องโหว่ที่ทำให้ผู้ใช้งานคนนั้นสร้างสิทธิของตัวเองได้มากขึ้น จนเทียบเท่าผู้ดูแลระบบได้ เนื่องจากโปรแกรมที่ใช้งานเกือบทุกโปรแกรมยังมีข้อบกพร่องอยู่

3. การบุกรุกระยะไกล (Remote Intrusion) ผู้บุกรุกติดต่อผ่านทางเครือข่าย ซึ่งมีหลายเทคนิคในการบุกรุกระบบแบบนี้ โดยปัจจุบันนั้นมีโปรแกรมประเภทไฟร์วอลล์ ทำหน้าที่ป้องกันการบุกรุกเป็นด่านแรก ซึ่งแม้แต่การบุกรุกภายในเครือข่ายเดียวกันก็อาจจะถูกป้องกันได้ โดย Personal Firewall ที่มักมีมากับตัวเครื่องของผู้ใช้งานอยู่แล้ว เช่น วินโดว์ไฟร์วอลล์ในระบบปฏิบัติการ ไมโครซอร์ฟวินโดวส์เอ็กซ์พี เซอร์วิสแพ็ค 2

2.4.3 Gaining Access

Gaining Access หมายถึง การได้รับสิทธิในการเข้าถึงระบบ ซึ่งเป็นความพยายามในการเข้าถึงเป้าหมายโดยอาจใช้เทคนิคของ – การดักจับรหัสผ่านจากเครือข่าย (เช่น ARP poisoning) หรือการกระทำใดๆเพื่อให้ได้ในการเข้าไปยังระบบเป้าหมาย

2.4.4 Privilege escalation

Privilege escalation เป็นการใช้ประโยชน์จากช่องโหว่ต่างๆของแอปพลิเคชันเพื่อให้ได้รับสิทธิในการเข้าถึงทรัพยากรต่างๆซึ่งโดยปกติแล้วไม่อนุญาตให้แอปพลิเคชันหรือผู้ใช้งานเข้าถึงได้ ซึ่งมักเกิดจากในขั้นตอน Gain access นั้นไม่ได้เป็นผู้ดูแลระบบ (Administrator) ผู้บุกรุกมักจะพยายามเพื่อยกฐานะ และสิทธิในการควบคุมระบบ โดยอาจจะทำการดึงรหัสผ่านจากภายในเครื่องแล้วมาลองใน Server (Network) แล้ว มักจะมีการใช้เทคนิค Pharming (Hosts file, APR-DNS การดักฟังข้อมูลในอินเตอร์เน็ต CAIN), Buffer overflow เป็นต้น

2.4.5 Buffer Overflow

การโจมตีด้วยวิธีเอ็กซ์พลอยท์ (Exploit) แบบบัฟเฟอร์โอเวอร์โฟลว์จะมุ่งเน้นไปที่การทำให้โปรแกรมเกิดการล้นของบัฟเฟอร์ เพื่อให้ถูกผู้ถูกโจมตีได้ทำการเรียกโปรแกรมที่ผู้โจมตีต้องการให้ทำงานขึ้นมา โดยส่วนใหญ่แล้ว สิ่งที่ผู้ทำการโจมตีต้องการ คือ สิทธิของการเป็นผู้ดูแลระบบ (Administrator หรือ root) ซึ่งตามทฤษฎีแล้วดูเรียบง่าย คือ โปรแกรมที่ผู้โจมตีส่งเข้ามาจะถูกใส่ไว้ใน บัฟเฟอร์ ซึ่งจะถูกทำให้ล้นมา โดยขั้นตอนแรกการแก้ไขส่วนต่างๆของหน่วยความจำนั้นเอง โดยพื้นฐานจากบัฟเฟอร์โอเวอร์โฟลว์ นั่นคือ สแต็ค โอเวอร์โฟลว์ และฮีปโอเวอร์โฟลว์

- **การจัดการหน่วยความจำ**

โปรเซส คือ ส่วนของโปรแกรมที่กำลังทำงานอยู่ (Running Program) ซึ่งในการที่จะทำให้โปรแกรมทำงานได้นั้น ระบบปฏิบัติการจะต้องทำการโหลดโปรแกรมไปยังหน่วยความจำเสียก่อน โดยที่การจัดสรรหน่วยความจำให้แต่ละโปรเซสนั้น เราสามารถแบ่งออกได้เป็น 5 ส่วนใหญ่ๆ ด้วยกัน คือ

1. ส่วนของข้อความ (Text Segment)

ส่วนของข้อความ หรือส่วนของโค้ด จะประกอบด้วย คำสั่งต่างๆ และโค้ดของโปรแกรม โดยในยูนิกซ์ และลินุกซ์ จะใช้ส่วนนี้ร่วมกันในแต่ละโปรเซสที่มาจากโปรแกรมเดียวกัน จึงทำให้มีส่วนของคำสั่งเพียงหนึ่งเดียวสำหรับโปรแกรมเดียวกันจะอยู่บนหน่วยความจำในขณะใดขณะหนึ่งเท่านั้น

2. ส่วนของข้อมูล (Data Segment)

ในส่วนนี้จะเก็บตัวแปรสากล (Global Variable) และตัวแปรคงที่ (Static Variable) ที่มีค่าเริ่มต้นแล้ว ซึ่งเรียกว่า ส่วนของข้อมูลที่ให้ค่า (Initialized Data) โดยแต่ละโปรเซสก็จะมีส่วนนี้เป็นของตัวเอง

3. ส่วนของ BSS (BSS Segment)

ตัวแปรสากล และตัวแปรคงที่ ที่มีค่าคงที่เป็นศูนย์โดยอัตโนมัติจะถูกเก็บในส่วนนี้ โดยสามารถเรียกส่วนนี้ได้อีกว่า ส่วนของตัวแปรที่มีค่าเป็นศูนย์ โดยแต่ละโปรเซสจะมีส่วนนี้แยกกัน

4. ส่วนของฮีป (Heap Segment)

เป็นส่วนของการเก็บตัวแปรแบบไดนามิค (เกิดจากคำสั่ง moc()) โดยฮีปจะขยายไปทางด้านบน นั่นคือ เมื่อเราใส่ค่าลงไปในฮีฟค่านั้นจะถูกบรรจุลงในตำแหน่งที่มีค่าสูงกว่าค่าที่ใส่ก่อนหน้า

5. ส่วนของสแต็ค (Stack Segment)

ในส่วนนี้จะเก็บตัวแปรเฉพาะที่ (Local Variable) ตัวอย่างของตัวแปรเฉพาะที่ คือ ตัวแปรที่อยู่ในฟังก์ชันย่อย โดยไม่ได้ประกาศให้เป็นตัวแปรคงที่ ซึ่งสแต็คจะขยายตัวลงไปทางด้านล่าง คือ เมื่อเราใส่คงลงไปในสแต็ค แล้วค่านั้นจะอยู่ในตำแหน่งที่มีค่าน้อยกว่าที่ใส่ก่อนหน้านั้น ซึ่งจะสวนทางกับส่วนของฮีป

2.4.6 การทำให้เครื่องเป้าหมายปฏิเสธการให้บริการ (Denial of Service Attack)

Denial of Service Attack หมายถึง การกระทำใดๆ ที่ทำให้ระบบเป้าหมายไม่สามารถให้บริการบางอย่างได้ หรือไม่สามารถให้บริการได้อีก โดยทั่วไปโจมตีที่พอร์ตของทีซีพี/ไอพี ซึ่งเชื่อมต่อกับบริการ (Services) ที่รองรับพอร์ตนั้นๆ ดังนั้นการโจมตีพอร์ตจึงเท่ากับการโจมตีบริการของระบบนั่นเอง และอาจมีผลทำให้ระบบนั้นไม่สามารถให้บริการบางอย่างได้ หรือไม่สามารถให้บริการใดๆ ได้เลย การโจมตีเพื่อปิดบริการแบ่งการโจมตีออกเป็น 2 แบบ คือ การโจมตีในระดับชั้นทีซีพี และ การโจมตีในระดับชั้นไอพี

การโจมตีในระดับชั้นทีซีพี ยังสามารถแบ่งได้เป็น 2 แบบย่อย คือ การโจมตีด้วยแพ็กเกจปริมาณมาก การโจมตีแบบนี้เป็นการส่งแพ็คเก็ตปริมาณมากเข้าไปยังระบบเป้าหมาย อาจทำให้ระบบเป้าหมายไม่สามารถให้บริการบางอย่าง หรือไม่สามารถทำงานต่อไปได้ ซึ่งแพ็คเก็ตที่ส่งออก

ไปนี้สามารถแบ่งออกได้เป็น การโจมตีด้วยแพ็คเก็ตข้อมูล การโจมตีวิธีนี้ทำได้โดยการส่งแพ็คเก็ตข้อมูลปริมาณมาก เมื่อข้อมูลเข้ามาสู่เครื่องเป้าหมายก็เก็บไว้ในบัฟเฟอร์ก่อนนำมาประมวลผลอีกครั้ง ดังนั้นหากส่งแพ็คเก็ตเข้ามาเป็นปริมาณมาก อาจทำให้บัฟเฟอร์ของเครื่องเป้าหมายไม่เพียงพอที่จะสามารถรองรับแพ็คเก็ตเหล่านั้นได้ทั้งหมด ซึ่งอาจทำให้เครื่องเป้าหมายให้บริการได้ช้าลง หรือต้องหยุดการให้บริการไปเลย

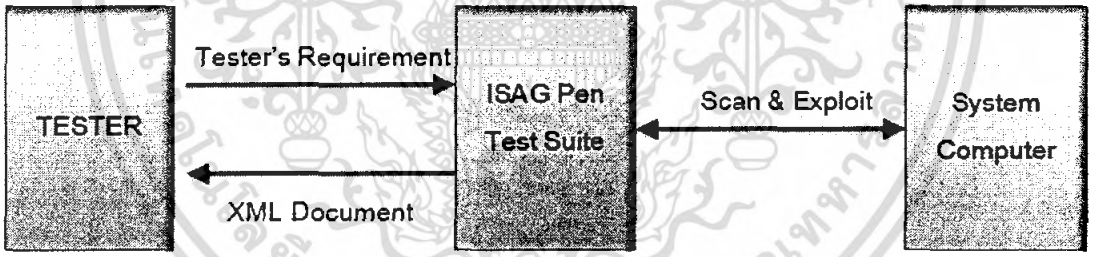
การโจมตีอีกรูปแบบหนึ่ง คือ การโจมตีด้วยแพ็คเก็ตควบคุม (Control Packets) ตัวอย่างของการโจมตีแบบนี้ ได้แก่ การทำ SYN Flooding การโจมตีลักษณะเป็นการทำ TCP 3-way handshake ไม่สมบูรณ์ กล่าวคือ เครื่องที่ขอบริการส่งสัญญาณ SYN ไป แต่เมื่อได้รับสัญญาณ SYN/ACK จากเครื่องที่ให้บริการแล้ว ไม่ส่งสัญญาณ ACK ตอบกลับไป ทำให้เครื่องที่ให้บริการต้องเปิดการเชื่อมต่อรอการตอบกลับ ดังรูปที่ 1 ซึ่งการเปิดการเชื่อมต่อรอเอาไว้นี้ต้องใช้ทรัพยากรของระบบส่วนหนึ่ง โดยเฉพาะทรัพยากรประเภทหน่วยความจำ ซึ่งจะเรียกการเชื่อมต่อที่เปิดค้างไว้นี้ว่า Backlog Queue และหากมีการส่งสัญญาณในลักษณะนี้มากๆ และจำนวนของ Backlog Queue มีมากเข้า ทรัพยากรของระบบอาจไม่เพียงพอ อาจทำให้ระบบไม่สามารถให้บริการอย่างอื่น หรือให้บริการกับผู้ร้องขอรายอื่นได้

บทที่ 3
การออกแบบและพัฒนา

ในส่วนของการออกแบบและการพัฒนานั้นจะต้องมีการพิจารณาถึงขั้นตอนการทำงานต่างๆ ที่จะนำมารวมและสร้างเป็นเครื่องมือขึ้นมาก เพื่อให้การทำงานได้ตามเป้าหมายที่วางไว้ โดยในขั้นตอนการทำงานต่างๆ นั้นได้มีการพิจารณาอย่างเหมาะสม

3.1 โครงสร้างพื้นฐานของโครงงาน

ชุดโปรแกรมทดสอบความปลอดภัยระบบคอมพิวเตอร์ (Computer Security Penetration Test Suite) ทำหน้าที่ในการทดสอบความปลอดภัยระบบคอมพิวเตอร์ที่ได้รับการอนุญาตจากเจ้าของระบบคอมพิวเตอร์นั้น เพื่อทำการค้นหาช่องโหว่ความปลอดภัยต่างๆในระบบคอมพิวเตอร์ และให้คำแนะนำในการป้องกันปัญหาช่องโหว่ความปลอดภัยที่พบในการทดสอบ ให้ในรูปแบบของเอกสารให้แก่ ผู้ทำการทดสอบระบบคอมพิวเตอร์ เพื่อเป็นคำแนะนำในการเพิ่มความปลอดภัยให้แก่ระบบที่ทำการทดสอบ ส่วนของขั้นตอนการทำงานนั้นจะอยู่ในลักษณะมุมมองของผู้บุกรุก แต่จะไม่มีการทำให้ระบบคอมพิวเตอร์ที่ทำการทดสอบได้รับความเสียหาย



รูปที่ 3.1 ลักษณะการทำงานโดยรวมของชุดโปรแกรม

จากรูปที่ 3.1 จะเห็นได้ว่า ผู้ที่ทำการทดสอบระบบคอมพิวเตอร์ที่ใช้ชุดโปรแกรมทดสอบความปลอดภัยระบบคอมพิวเตอร์สามารถทำการทดสอบระบบคอมพิวเตอร์ โดยที่ผู้ทำการทดสอบอาจอยู่ภายในเครือข่าย (ในลักษณะผู้บุกรุกที่อยู่ภายในองค์กร) และเครือข่ายภายนอก (ในลักษณะผู้บุกรุกทั่วไปที่โจมตีผ่านทางอินเทอร์เน็ต)

ปัจจัยที่มีผลต่อการทำงานของชุดโปรแกรมและผลลัพธ์ที่ต้องการจากชุดโปรแกรม มีดังต่อไปนี้

1. ข้อมูลขาเข้าของชุดโปรแกรม คือ ความต้องการใช้งานชุดโปรแกรมของผู้ใช้งาน (Tester's Requirement) ซึ่งในส่วนนี้แล้วชุดโปรแกรมจะมีส่วนต่อประสานกราฟิกกับผู้ใช้งาน เพื่ออำนวยความสะดวกให้แก่ผู้ใช้งานโปรแกรม ประกอบไปด้วย

- *ไอพีแอดเดรส* - ผู้ใช้งานต้องทำการรวบรวมข้อมูลที่เกี่ยวกับระบบคอมพิวเตอร์ที่ทำการตรวจสอบ ว่ามีการใช้งานช่วงไอพีแอดเดรสอะไรบ้างที่ต้องทำการทดสอบ และช่วงไอพีแอดเดรสอะไรบ้างที่ไม่ต้องการทดสอบ หรืออาจจะระบุเพียงไอพีแอดเดรสเครื่องที่ต้องการทดสอบ
- *ลักษณะการใช้งานโปรแกรมที่เกี่ยวกับการสแกน และการเอ็กซ์พลอยท์* - ผู้ใช้งานต้องการสแกน หรือ เอ็กซ์พลอยท์ (Exploit) ระบบคอมพิวเตอร์ในลักษณะรูปแบบที่ทางโปรแกรมจัดเตรียมให้ หรือต้องการปรับแต่งการสแกน หรือ เอ็กซ์พลอยท์ (Exploit)ในลักษณะที่ผู้ใช้งานต้องการ

2. ผลลัพธ์การทำงานของชุดโปรแกรม ซึ่งทางชุดโปรแกรมนี้ได้มีการจัดรูปแบบผลการทดสอบให้อยู่ในของเอกสาร XML (XML Document) และแสดงผลด้วย XSL ออกทางเบราว์เซอร์

3.2 รายละเอียดโปรแกรมที่พัฒนา (Software Specification)

3.2.1 รายละเอียดส่วนนำเข้า

- ผู้ใช้งานเลือกโหมดของชุดโปรแกรมในการทดสอบระบบคอมพิวเตอร์
- ผู้ใช้งานเลือกระบบคอมพิวเตอร์เป้าหมายที่ต้องการทดสอบ
- ผู้ใช้งานใช้งานผ่านส่วนต่อประสานกราฟิกกับผู้ใช้งาน (GUI) และคอมมานไลน์ (Command Line) ได้

3.2.2 รายละเอียดส่วนนำออก

- แสดงปัญหาช่องโหว่ความปลอดภัยที่อาจโดนบุกรุกจากการทดสอบด้วยวิธีการเอ็กซ์พลอยท์ (Exploit)
- แสดงเซอร์วิส พอร์ต และระบบปฏิบัติการของระบบคอมพิวเตอร์ที่ทำการทดสอบ
- แสดงคำแนะนำในการป้องกันปัญหาช่องโหว่ความปลอดภัยที่พบในการทดสอบ
- ผู้ใช้งานรับรายงานผลการทดสอบในรูปแบบของเอกสาร XML

3.2.3 รายละเอียดฟังก์ชัน

- ชุดโปรแกรมสามารถสแกนหา เซอร์วิส พอร์ต และระบบปฏิบัติการ ที่ทำงานได้
- ชุดโปรแกรมสามารถเอ็กซ์พลอยท์ (Exploit) ระบบคอมพิวเตอร์เป้าหมายได้
- ชุดโปรแกรมสามารถวิเคราะห์การป้องกันปัญหาช่องโหว่คอมพิวเตอร์ที่พบได้
- ชุดโปรแกรมสามารถแสดงและสร้างรายงานของผลการทดสอบระบบ และวิเคราะห์การป้องกันในรูปแบบของเอกสาร XML ได้

3.2.4 โครงสร้างของซอฟต์แวร์ (Design)

แบ่งการทำงานเป็น 3 ส่วน คือ การสแกน (Scanner), การแสวงหาประโยชน์ (Exploitation) และการวิเคราะห์การป้องกัน (Prevention)

- การสแกนพัฒนาจาก Nmap เพื่อที่จะทำพอร์ตสแกน, Service & OS Detection
- การแสวงหาประโยชน์ เป็นส่วนในการหาช่องโหว่ความปลอดภัยของระบบเป้าหมาย
- การวิเคราะห์การป้องกัน เป็นส่วนของการวิเคราะห์วิธีการป้องกันปัญหาช่องโหว่ความปลอดภัยที่พบในการทดสอบ และสร้างเอกสาร XML

3.2.5 ขอบเขตและข้อจำกัดของโครงสร้าง

- โปรแกรมทำงานบนระบบปฏิบัติการลินุกซ์ และวินโดส์เท่านั้น
- การทำงานของชุดโปรแกรมจะมีประสิทธิภาพสูง เมื่อระบบที่นำมาทดสอบทำงานบนระบบปฏิบัติการไมโครซอร์ฟวินโดวส์เอ็กซ์พี เซอร์วิสแพ็ค 2 เท่านั้น
- ชุดโปรแกรมสามารถติดต่อผู้ใช้งานผ่านส่วนต่อประสานกราฟิกกับผู้ใช้งาน และคอมมานไลน์
- ชุดโปรแกรมสามารถทำการสแกน และเอ็กซ์พลอยท์ระบบคอมพิวเตอร์ได้
- ชุดโปรแกรมสามารถสร้างเอกสาร XML ในส่วนของการสรุปผลการทดสอบ
- Personal Firewall ที่ใช้ในการทดสอบ คือ Windows Firewall, ZoneAlarm Security

3.2.6 เครื่องมือที่ใช้การพัฒนา

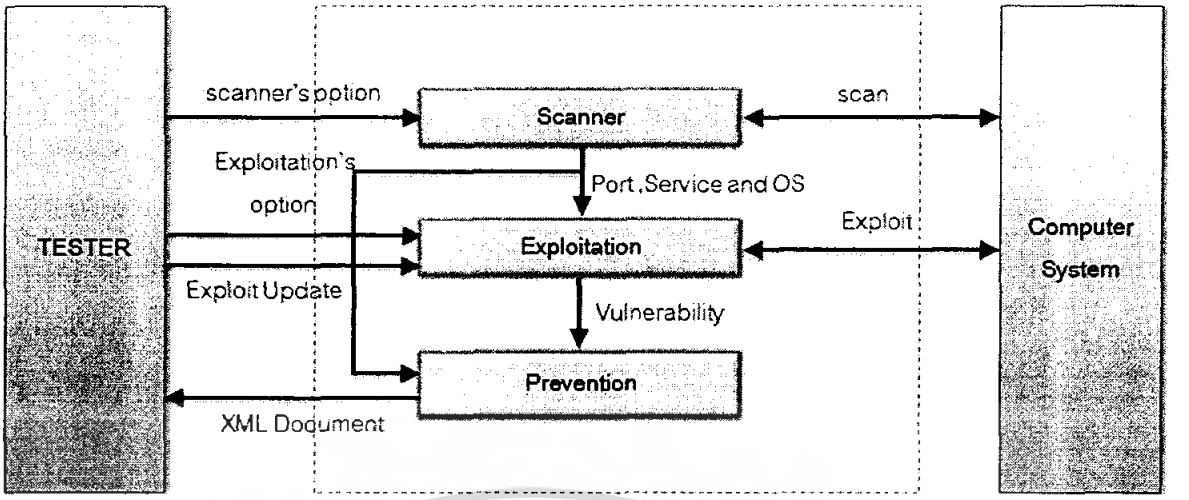
- Linux Kernel - ชุดโปรแกรมนี้สามารถติดตั้งและได้ทดสอบทำงานบนระบบปฏิบัติการ Debian 4.0 Kernel 2.6

- Microsoft Windows XP Service Pack 2 -โครงงานนี้ได้ใช้ระบบต้นแบบเป็น Microsoft Windows XP Service Pack 2 เนื่องจากเป็นระบบปฏิบัติการที่มีการใช้งานและโดนบุกรุกมากที่สุดในปัจจุบัน นอกจากนี้แล้วชุดโปรแกรมนี้ยังสามารถติดตั้งและทดสอบการทำงานได้
- C / C++ Editor (Kwrite) - เนื่องจากการพัฒนาชุดโปรแกรมนั้น ส่วนใหญ่แล้วโปรแกรมที่นำมาพัฒนาในโครงงานนี้มักเขียนด้วยภาษา C / C++ ที่เป็นภาษาพื้นฐานในการพัฒนาโปรแกรม
- Kdevelop – ใช้ในการเขียน GUI
- QT – ไลบรารี (library) สำหรับการเขียน GUI
- g++ / gcc – ตัวแปลภาษา C++ / C (C++ / C Compiler)
- XML - ใช้ในการพัฒนาในการทำรายงานเอกสารของชุดโปรแกรม
- Personal Firewall - ZoneAlarm Security และ Windows Firewall เป็นส่วนที่ใช้ในระบบรักษาความปลอดภัยของระบบต้นแบบที่ทำการทดสอบ
- Nmap - ใช้เป็นต้นแบบในการพัฒนา เพื่อให้ชุดโปรแกรมสามารถทำการสแกนพอร์ต ค้นหาเซอร์วิส และค้นหาประเภทของระบบปฏิบัติการ
- Exploit Code - ใช้เพื่อให้ชุดโปรแกรมสามารถทำเอ็กซ์พลอยท์ (Exploit)ระบบเป้าหมายในรูปแบบต่างๆ ทั้ง buffer overflow, DoS และอื่นๆ โดยที่โค้ดเหล่านี้มาจากเว็บไซต์ต่างๆ

3.3 การออกแบบและพัฒนาซอฟแวร์

ชุดโปรแกรมทดสอบความปลอดภัยระบบคอมพิวเตอร์ (Computer Security Penetration Test Suite) จะทำงานบนระบบปฏิบัติการลินุกซ์ โดยทำงานเมื่อผู้ใช้งานได้ทำการใส่ค่าตัวเลือกต่างๆ และหมายเลขไอพีของระบบคอมพิวเตอร์เป้าหมาย ซึ่งผู้ใช้งานสามารถกำหนดได้ว่าจะสแกนแบบไหน หรือเอ็กซ์พลอยท์ (Exploit) ด้วยเทคนิคใดบ้าง เมื่อโปรแกรมได้ทำการทดสอบระบบเสร็จแล้ว ชุดโปรแกรมจะทำการสร้างเอกสาร XML

ในการทำงานของชุดโปรแกรมทดสอบความปลอดภัยระบบคอมพิวเตอร์นั้น มีขั้นตอนการทำงานคล้ายกับขั้นตอนในการทดสอบความปลอดภัยระบบ (Penetration Test) ซึ่งชุดโปรแกรมนี้ได้ทำการออกแบบขั้นตอนการทำงานของชุดโปรแกรม ในรูปแบบขั้นตอนดังต่อไปนี้



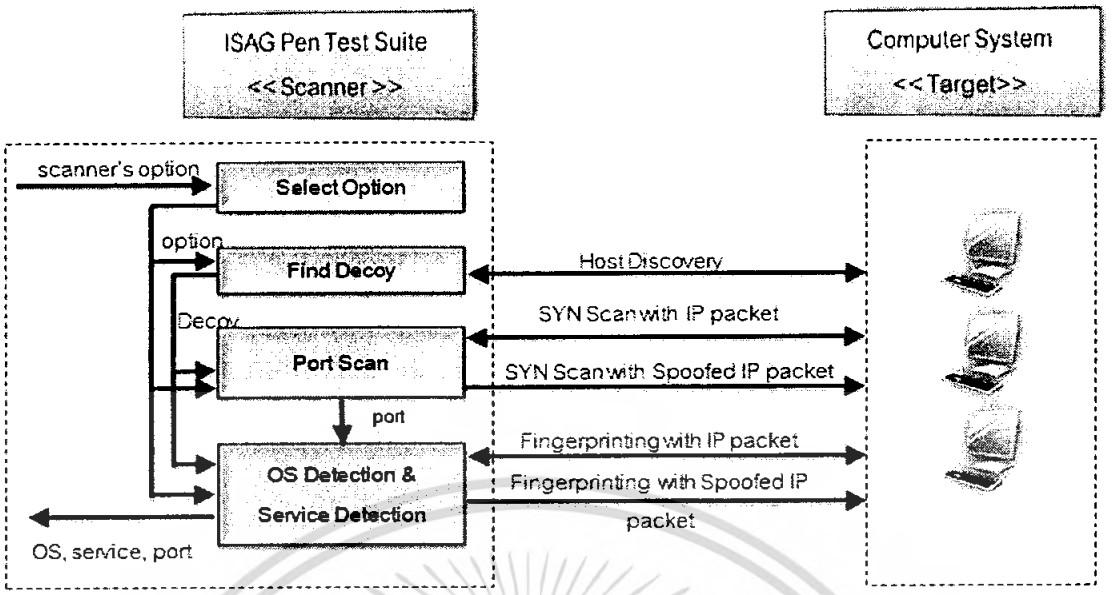
รูปที่ 3.2 ลักษณะขั้นตอนการทำงานของชุดโปรแกรม

จากรูป 3.2 จะเห็นได้ว่าการทำงานของชุดโปรแกรมทดสอบความปลอดภัยระบบคอมพิวเตอร์จะมีขั้นตอนในการทำงานที่สำคัญอยู่ 3 ส่วนหลักๆ ดังนี้

3.3.1 การสแกน (Scanner)

การสแกน เป็นขั้นตอนเริ่มต้นของการทดสอบระบบ โดยจะเป็นขั้นตอนของการรวบรวมข้อมูลต่างๆ ได้แก่ พอร์ตที่เปิดทำงาน ชื่อ/เวอร์ชันของเซอร์วิส ชื่อ/ประเภทของระบบปฏิบัติการของระบบคอมพิวเตอร์ และแอปพลิเคชันที่ทำงานอยู่ เพื่อนำผลที่ได้เหล่านั้นไปวิเคราะห์ว่า มีความเป็นไปได้วิธีการใดบ้างในการเอ็กซ์พลอยท์ ระบบคอมพิวเตอร์ที่ทำการทดสอบ

ในโครงงานนี้ในขั้นตอนของการสแกนจะมีการนำโค้ดของ Nmap มาเป็นต้นแบบในการพัฒนา ซึ่ง Nmap นั้นมีความสามารถในการสแกนได้หลายประเภท, สามารถทำการแกะรอยได้ และยังสามารถที่จะทำการสร้างเอกสาร XML ได้อีกด้วย ซึ่งในโครงงานจะมีการแก้ไขโค้ด Nmap เพื่อให้มีประสิทธิภาพในการ สแกนมากขึ้น, จัดรูปแบบการสแกน และการพัฒนาในสร้างของโค้ดที่เกี่ยวกับการสร้าง XML เนื่องจากในโปรแกรมจะมีการอ่านและเขียนไฟล์ XML โดยขั้นตอนการทำงานทั้งหมดในส่วนของการสแกนมีลักษณะดังต่อไปนี้



รูปที่ 3.3 แสดงขั้นตอนการทำงานในส่วนการสแกน

จากรูปที่ 3.3 จะเห็นได้ว่าในขั้นตอนของการสแกนนั้นจะอาศัยเทคนิคที่สำคัญในการหาผลทดสอบด้วยเทคนิคดังต่อไปนี้

1 เทคนิคการสแกนพอร์ต (Port scan)

สแกนพอร์ตเป็นเทคนิคที่อาศัยการทำงานของระบบคอมพิวเตอร์ที่มีการติดต่อสื่อสารผ่านโพรโตคอลต่างๆ เช่น ทีซีพี ยูดีพี ไอซีเอ็มพี เอเอาร์พี เอฟทีพี โดยอาจทำการเปลี่ยนแปลงเฮดเดอร์ของแพ็คเก็ตก่อนส่งไปยังปลายทาง เช่น การตั้งค่าแฟลกซ์ SYN ในทีซีพีซึ่งเป็นวิธีที่นิยมเนื่องจากความเร็วในการสแกน และยากต่อการตรวจจับ

2 Fingerprint

ใช้ในการสืบหาชื่อและเวอร์ชันของเซอร์วิส (Service Detection) และสืบหาชื่อและประเภทของระบบปฏิบัติ (OS Detection) การหาช่องโหว่ความปลอดภัยจากระบบปฏิบัติการและเซอร์วิสเหล่านั้น โดยอาศัยการส่งแพ็คเก็ตชนิดต่างๆเพื่อไปทำการทดสอบ และรอผลการตอบกลับที่มีลักษณะเฉพาะของระบบปฏิบัติการ

3 Spoofed IP packet

ใช้ในการปลอมไอพีแพ็คเก็ต เพื่อซ่อนการสแกน ไม่ให้ผู้ดูแลระบบที่ถูกสแกนนั้นทราบได้ว่า มีการสแกนมาจากหมายเลขใด ซึ่งหมายเลขไอพีที่ทำการปลอมนั้นจะมักจะถูกเรียกว่า นกต่อ โดยสามารถหานกต่อได้โดยการการใช้ Ping Sweep (TCP SYN Scan หรืออะไรก็ตาม) แต่การใช้

นกต่อนี้ไม่สามารถใช้ร่วมกับการค้นหาเวอร์ชันของเซอร์วิส และ TCP connect scan ซึ่งในการสแกน ถ้ากำหนดไอพีที่ใช้ในการสแกนนั้นต่อท้ายนกต่อในตำแหน่งที่มากกว่า 5 แล้วเครื่องตรวจจับการสแกนพอร์ตทั่วไป (เช่น Solar Designer's excellent scanlogd) ไม่น่าที่จะแสดงหมายเลขไอพีของเครื่องที่ทำการสแกนออกมา

การใช้นกต่อนี้ ถ้าใช้จำนวนมากเกินไปอาจจะทำให้การสแกนช้า และอาจจะทำให้ความถูกต้องของการสแกนน้อยลง ซึ่งในบาง ISPs จะทำการกรองการปลอมแพ็คเก็ตออก แต่อาจจะไม่ทำการห้ามการปลอมไอพีแพ็คเก็ต

ในชุดโปรแกรมทดสอบความปลอดภัยระบบคอมพิวเตอร์นี้ได้ทำการจัดเตรียมตัวเลือกในการ สแกนออกเป็น 4 รูปแบบ โดยในแต่ละตัวเลือกจะขึ้นกับปัจจัย 2 อย่างคือ เวลาในการสแกน และความแม่นยำของการสแกน ซึ่งรายละเอียดของแต่ละตัวเลือกของการสแกนมีดังต่อไปนี้

1 **Complete** เป็นการสแกนที่พยายามที่จะไม่ให้ผู้ดูแลระบบคอมพิวเตอร์ที่ถูกสแกนนั้นรู้ว่ามีการสแกนมาจากที่ใด และยังสามารถที่ผ่านไฟร์วอลส่วนบุคคลที่มีการปรับแต่งค่าไม่ดีได้ แต่การสแกนลักษณะจะใช้เวลาในการสแกนค่อนข้างที่จะนานกว่าตัวเลือกอื่นๆ เหมาะสำหรับการหาช่องโหว่ความปลอดภัยของเครื่องจำนวนไม่มาก โดยใช้เทคนิคของ SYN Scan, UDP Scan, Decoy, Retransmission, Fingerprint ซึ่งในส่วนของ SYN Scan และ UDP Scan ที่ใช้งานมีลักษณะดังนี้

- TCPScan "-sS -sV -O -P0 -r -R --system-dns --version-all --max-retries 10 --max-os-tries 10 --osscan-guess -T4 -oX TCPResult.xml --host-timeout 5m "
- UDPScan "-sU -sV -P0 -r -R --system-dns -T4 --version-all --max-retries 10 -oX UDPResult.xml --host-timeout 3m "

2 **Aggressive** เป็นการสแกนที่ต้องการทั้งในส่วนของความเร็วในการสแกน, ความพยายามที่จะไม่ให้ผู้ดูแลระบบคอมพิวเตอร์ที่ถูกสแกนนั้นรู้ว่ามีการสแกนมาจากที่ใด และผ่านไฟร์วอลส่วนบุคคลที่มีการปรับแต่งค่าไม่ดีได้ โดยใช้เทคนิคของ SYN Scan, UDP Scan, Decoy, Retransmission, Fingerprint ซึ่งในส่วนของ SYN Scan และ UDP Scan ที่ใช้งานมีลักษณะดังนี้

- TCPScan << "-sS -sV -O -P0 -r -R --system-dns --version-all --max-retries 10 --max-os-tries 10 --osscan-guess -T4 -oX TCPResult.xml --host-timeout 3m "
- UDPScan << "-sU -sV -P0 -r -R --system-dns -T4 --version-all --max-retries 10 -oX UDPResult.xml --host-timeout 3m "

3 Fast (default) เป็นการสแกนที่ต้องการความเร็วสูง, ระบบคอมพิวเตอร์เป้าหมายไม่มีการใช้งานไฟร์วอลส่วนบุคคล หรือมีการปรับแต่งค่าไฟร์วอลส่วนบุคคลไว้ในระดับที่ต่ำมาก เหมาะสำหรับการ สแกนเครื่องจำนวนมาก โดยใช้เทคนิคของ SYN Scan, UDP Scan, Decoy, Retransmission, Fingerprint ซึ่งในส่วนของ SYN Scan และ UDP Scan ที่ใช้งานมีลักษณะดังนี้

- TCPScan << "-sS -sV -O -P0 -F -r -R --system-dns -T4 --host-timeout 2m --version-all --max-retries 5 --max-os-tries 2 --osscan-guess -oX TCPResult.xml
- UDPScan << "-sU -sV -P0 -F -r -R --system-dns -T4 --host-timeout 2m --version-all --max-retries 5 -oX UDPResult.xml

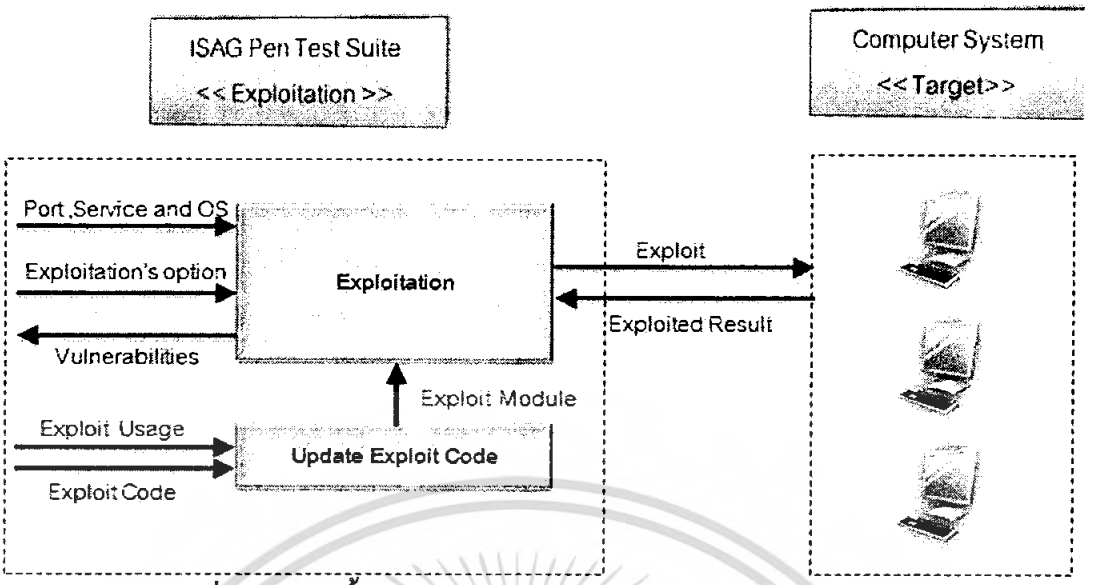
4 Custom_เป็นตัวเลือกสำหรับการสแกนที่เหมาะสมสำหรับผู้ที่มีความรู้ในการสแกน และต้องการปรับแต่งค่าในการสแกนด้วยตนเอง โดยผู้ใช้งานควรทำการเรียนรู้เกี่ยวกับการใช้งานโปรแกรม IPT custom scanner เสียก่อน หรืออาจจะเป็นผู้ที่ทักษะการใช้งานจาก Nmap เนื่องจากชุดโปรแกรมได้ทำการพัฒนาส่วนของการสแกนมาจาก Nmap

ตารางที่ 3.1 แสดงผลการทดสอบในแต่ละตัวเลือกของการสแกน

Scan's Mode	Speed	Accuracy	Security	Average Time / Host
Fast	High	Low	None	80-180 sec.
Aggressive	Medium	Medium	Low	100-330 sec.
Complete	Low	High	Medium	120-400 sec.
Custom	-	-	-	-

3.3.2 การแสวงหาประโยชน์ (Exploitation)

การแสวงหาประโยชน์ เป็นขั้นตอนของการบุกรุกระบบด้วยเทคนิคต่างๆ เพื่อที่จะได้รับประโยชน์จากการบุกรุก เช่น สิทธิการควบคุมระบบ หรือ การทำให้ระบบอยู่ในสภาพปฏิเสธการให้บริการ ซึ่งในส่วนนี้จะมีขั้นตอนการทำงานอยู่ 2 กระบวนการ คือ



รูปที่ 3.4 แสดงขั้นตอนการทำงานในส่วนการแสวงหาประโยชน์

1 การแสวงหาประโยชน์ (Exploitation)

เมื่อผู้บุกรุกไม่สามารถทำการคาดเดารหัสผ่าน หรือยกระดับสิทธิได้ ผู้บุกรุกมักจะเหลือทางเลือกอยู่ไม่มาก โดยทางเลือกแรก คือ การหาข้อบกพร่องที่อาจจะมีในระบบปฏิบัติการหรือในเซอร์วิส / แอปพลิเคชัน ที่แอบแฝงอยู่ และเอ็กซ์พลอยท์ ทางเลือกที่สองที่มักเป็นทางเลือกสุดท้าย คือ Denial of Service: DoS

- **เอ็กซ์พลอยท์ (Exploit)**

  ในชุดโปรแกรมนี้จะทำการเอ็กซ์พลอยท์ โดยการนำโค้ดที่มีในเว็บต่างๆ ที่น่าเชื่อถือมาเป็นต้นแบบในการเอ็กซ์พลอยท์ โดยเน้นไปที่ไมโครซอร์ฟวินโดวส์เอ็กซ์พี เซอร์วิสแพ็ค 2 ซึ่งในการเอ็กซ์พลอยท์ นั้น ชุดโปรแกรมนี้จะใช้หลักการต่อไปนี้

  - Remote Buffer Overflows
  - Escalating Privilege

- **การทำให้เครื่องเป้าหมายปฏิเสธการให้บริการ (Denial of Service)**

  ในชุดโปรแกรมนี้จะทำ Denial of Service โดยการนำโค้ดที่มีในเว็บต่างๆ ที่น่าเชื่อถือมาเป็นต้นแบบในการ Denial of Service โดยเน้นไปที่ระบบปฏิบัติการไมโครซอร์ฟวินโดวส์เอ็กซ์พี เซอร์วิสแพ็ค 2

2 การเพิ่มโค้ดที่ใช้ในการทดสอบระบบคอมพิวเตอร์ (Update Exploit Code)

ในส่วนนี้ใช้สำหรับการเพิ่มโค้ดที่ใช้ในการทดสอบระบบคอมพิวเตอร์ลงในโปรแกรม โดยมีการกำหนดรูปแบบของการเพิ่มโค้ดในรูปแบบที่ สามารถเข้าใจ และใช้งานได้ง่าย

ส่วนขั้นตอนในการเพิ่มโค้ดที่ใช้ในการทดสอบระบบคอมพิวเตอร์ลงในโปรแกรม มีดังนี้

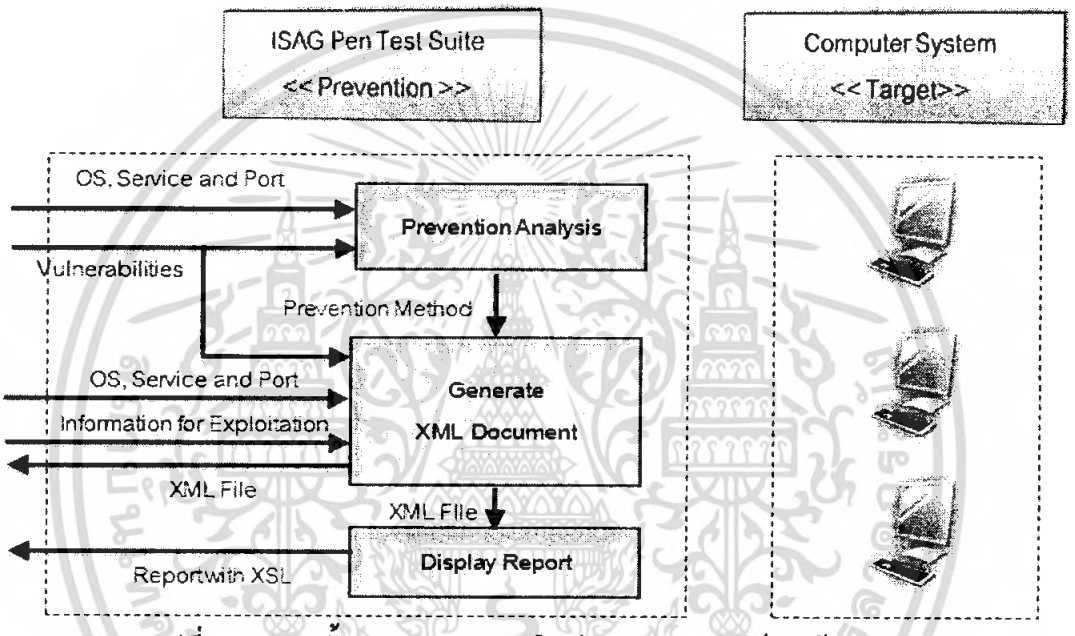
1 ทำการคอมไฟล์โค้ดที่นำมาใช้ในการทดสอบระบบคอมพิวเตอร์ เป็นนามสกุลไฟล์ eipt

2 ใส่ตัวเลือกในการใช้งาน และรูปแบบผลการทำงานที่แสดงว่า โค้ด นั้นทำงานได้สำเร็จ ลงในไฟล์นามสกุล ein

3 ใส่ชื่อ คำอธิบายการทำงาน ความเสี่ยงที่น่าจะเกิดปัญหา และวิธีป้องกันของโค้ดนั้น ในไฟล์นามสกุล epv

4 เพิ่มชื่อของโค้ดลงในไฟล์ชื่อ list.ein

3.3.3 การวิเคราะห์การป้องกัน (Prevention)



รูปที่ 3.5 แสดงขั้นตอนการทำงานในส่วนการวิเคราะห์การป้องกัน

ในขั้นตอนการวิเคราะห์การป้องกัน (Prevention) นั้นเป็นการวิเคราะห์ผลที่เพื่อหาช่องโหว่ความปลอดภัย ให้คำแนะนำเกี่ยวกับวิธีการป้องกันปัญหาช่องโหว่ความปลอดภัยที่พบในการทดสอบ ในรูปแบบของเอกสาร XML และการแสดงผลรายงาน XML ในรูปแบบของ XSL ซึ่งในส่วนนี้จะมีลักษณะการทำงานแบ่งออกเป็น 3 ส่วน คือ

1. การวิเคราะห์การป้องกัน (Prevention Analysis)

ขั้นตอนนี้ชุดโปรแกรมจะทำการรวบรวมช่องโหว่ความปลอดภัยที่ได้จากส่วนการสแกน (Scanner) และส่วนการแสวงหาประโยชน์ (Exploitation) หลังจากนั้น จึงทำการวิเคราะห์หาวิธีป้องกันปัญหาช่องโหว่ความปลอดภัยที่พบในการทดสอบ แล้วนำผลการวิเคราะห์ไปทำการสร้างเอกสาร XML

ในส่วนของฐานข้อมูลที่ใช้ในการวิเคราะห์ความเสี่ยงของผลที่ได้จาก 2 ส่วนก่อนหน้านี้ ผู้พัฒนาได้ทำการค้นหาข้อมูลเกี่ยวกับความเสี่ยงต่างๆที่น่าจะเป็นไปได้ในระบบคอมพิวเตอร์ทั่วไป จากอินเทอร์เน็ต และเก็บข้อมูลไว้ในลักษณะของไฟล์ เพื่อใช้ในการวิเคราะห์หาความเสี่ยง และวิธีการบรรเทาปัญหาความปลอดภัยระบบคอมพิวเตอร์เป้าหมาย โดยใช้เทคนิคของการเปรียบเทียบรูปแบบ (Pattern Matching)

2. การสร้างรายงานเอกสาร XML (Generate XML Document)

การสร้างรายงานเอกสาร XML เป็นขั้นตอนในการนำช่องโหว่ความปลอดภัยที่พบใน การแสวงหาประโยชน์ (Exploitation) ผลลัพธ์ที่ได้จากการสแกน และวิธีการป้องกันปัญหาช่องโหว่ความปลอดภัยที่พบในการทดสอบ นำมาจัดให้อยู่ในรูปแบบเอกสาร XML เพื่อที่จะใช้เป็นฐานข้อมูล หรือใช้ในการแสดงให้แก่เจ้าของระบบคอมพิวเตอร์ที่ทำการทดสอบได้ทราบ

โดยที่เราออกแบบให้มีการจัดเอกสารในรูปแบบของ XML เนื่องจากจุดเด่นของภาษา XML นั้นมีมากมาย ดังนี้

• ภาษา XML มีความยืดหยุ่นสูง (extensible) ซึ่งสามารถนิยามความหมายของข้อมูลและสามารถสร้างแท็กขึ้นมาเองได้ มีการจัดโครงสร้างข้อมูลเป็นหมวดหมู่และส่วนประกอบย่อย

• ภาษา XML ทำให้การแลกเปลี่ยนข้อมูลระหว่างแอพลิเคชันหรือระบบต่าง ๆ ง่ายขึ้นลดเวลาการทำงานของผู้พัฒนาระบบที่ใช้ในการพัฒนาให้ระบบสามารถแลกเปลี่ยนข้อมูลระหว่างกันได้ โดยที่ไม่ส่งผลกระทบต่อรูปแบบของข้อมูลภายในตัวแอพลิเคชันหรือระบบเลย

• ภาษา XML ทำให้การสื่อสารระหว่างธุรกิจและ/หรือองค์กร หรือที่เรียกว่า B2B (Business-to-Business communication) ง่ายขึ้น และมีการแลกเปลี่ยนข้อมูลระหว่างกัน เช่น ข้อมูลทางด้านการเงิน ซึ่งควรเป็นมาตรฐานเดียวกันทั้งโลก

• XML สามารถทำงาน โดยไม่ขึ้นกับแพลตฟอร์มของใด ๆ ทำให้สามารถทำงานข้ามแพลตฟอร์ม และทำงานร่วมกับภาษาอื่น ๆ ได้

• XML ทำให้สามารถเข้าถึงข้อมูลได้ง่าย ยูสเซอร์และแอพลิเคชันต่าง ๆ จะสามารถเข้าถึงไฟล์ xml ได้เสมือนว่าเป็นแหล่งข้อมูลหรือระบบฐานข้อมูล ดังนั้นเอเจ็นท์ (agent) ต่าง ๆ จะสามารถเข้าถึงข้อมูลได้ง่ายขึ้นเช่นกัน

• XML ทำให้ข้อมูลมีความถูกต้องสูง

3. การแสดงผลรายงาน (Display Report)

ในส่วนนี้จะเป็นการแสดงผลรายงานเอกสารXML ในรูปแบบของ XSL ผ่านทางเบราว์เซอร์ (browser) โดยรูปแบบของการแสดงผลแบ่งออกเป็น 4 ส่วน

3.1. Penetration Test Suite Report เป็นการแสดงภาพรวมทั้งหมดของการใช้งานโปรแกรม โดยระบุเกี่ยวกับข้อมูล ดังนี้ เวลาที่ทำการเริ่ม, เวลาที่สิ้นสุด, เวลาทั้งหมดของการทดสอบ, ตัวเลือกที่ใช้ในการทดสอบ, ลิงค์ของเครื่องต่างๆที่ทำงานอยู่, และลิงค์ของการเชื่อมโยงแต่ละส่วนของ Report

ISAG Penetration Test [IPT] Suite Report

Start Time ::	Thu Feb 7 04:32:32 2008
Finish Time ::	Thu Feb 7 04:38:12 2008
Total Scan ::	340 second
IPT's Option ::	ipt -complete -exploit --all-plugin 161.246.5.20
Scan info ::	[illegible] |
Report ::	Overview Scanning | Port | Exploitation | Scan Info | About IPT

รูปที่ 3.6 ตัวอย่างรายงานส่วนที่ 1

3.2. Overview Scanning เป็นการแสดงเกี่ยวกับภาพรวมของการสแกน และ Exploit โดยระบุเกี่ยวกับข้อมูล ดังนี้ จำนวนเครื่องที่ทำงานอยู่บนเครือข่าย, ประเภทของระบบปฏิบัติการ, Port Detection และ Exploitation

Overview Scanning

Overview Scanning

IPT scan 1 host(s) ::	Online 1 hosts(s) | Offline 0 hosts(s)
Microsoft Windows ::	161.246.5.20 |

Port Detection

Port		Service	Host (ip address)
1025	udp	blackjack	161.246.5.20 |
123	udp	ntp	161.246.5.20 |
135	tcp	msrpc	161.246.5.20 |
137	udp	netbios-ns	161.246.5.20 |
138	udp	netbios-dgm	161.246.5.20 |
139	tcp	netbios-ssn	161.246.5.20 |
1900	udp	UPnP	161.246.5.20 |
3306	tcp	mysql	161.246.5.20 |
445	udp	microsoft-ds	161.246.5.20 |
4500	udp	sae-urn	161.246.5.20 |
500	udp	isakmp	161.246.5.20 |
80	tcp	http	161.246.5.20 |

Exploitation

Exploit ID	Exploit Name	Host (ip address)
ipt_dos04	Microsoft Windows SMB PIPE Remote Denial of Service Vulnerability	161.246.5.20 |

รูปที่ 3.7 ตัวอย่างรายงานส่วนที่ 2

3.3. รายละเอียดของแต่ละเครื่อง เป็นการแสดงรายละเอียดของแต่ละเครื่องเกี่ยวกับข้อมูล IP Address, MAC Address, Port Detection, Exploitation และคำแนะนำการบรรเทาปัญหาช่องโหว่ความปลอดภัยที่พบ

161.246.5.20 / isag20.ce.kmitl.ac.th(online)

General

-- **Address** : 161.246.5.20 (ipv4) | 00:15:F2:A5:4D:A5 (mac) |

-- **Hostnames** : isag20.ce.kmitl.ac.th (PTR)

Port Detection

-- The 3173 ports scanned but not shown below are in state: **closed**

Port		State	Service	Product	Version	Extra Info
80	tcp	open	http	Apache httpd		(Win32) PHP/5.2.1
135	tcp	open	msrpc	Microsoft Windows RPC		
139	tcp	open	netbios-ssn			
3306	tcp	open	mysql	MySQL		unauthorized
123	udp	open	ntp	NTP		
137	udp	open	netbios-ns	Microsoft Windows NT netbios-ssn		workgroup: WORKGROUP
138	udp	open|filtered	netbios-dgm			
445	udp	open|filtered	microsoft-ds			
500	udp	open|filtered	isakmp			
1025	udp	open|filtered	blackjack			
1900	udp	open|filtered	UPnP			
4500	udp	open|filtered	sae-urn			

Remote Operating System Guess

-- **IPT Suite used port** : 80/tcp]

-- OS Match ::

Microsoft Windows 2000 Server SP4 [Accuracy: 96%]

Microsoft Windows XP SP2 [Accuracy: 96%]

Microsoft Windows 2000 SP4 [Accuracy: 95%]

Microsoft Windows 2003 Server SP1 [Accuracy: 94%]

Microsoft Windows Server 2003 Enterprise Edition 64-Bit SP1 [Accuracy: 93%]

Microsoft Windows 2000 SP3 [Accuracy: 92%]

Microsoft Windows 2000, SP0, SP1, or SP2 [Accuracy: 92%]

Microsoft Windows 2000 Server SP4 [Accuracy: 89%]

Other Detail

- **Network distance** : 1 hops

Exploitation

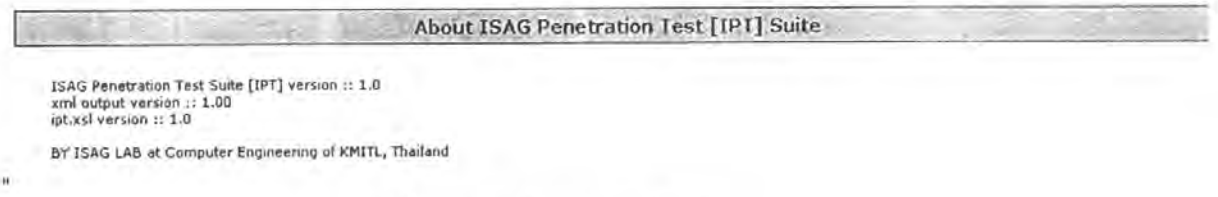
-**ipt_dos04** : Microsoft Windows SMB PIPE Remote Denial of Service Vulnerability

Recommendation For Prevention

Causes		Name	Recommendation
80	tcp	http	**Description :** World Wide Web HTTP **Risk :** This is the primary portused by the world wide web (www) system. Web servers open this portthen listen for incoming connections from web browsers. Similarly, when a web browser is given a remote address (like grc.com or amazon.com), it assumes that a remote web server will be listening for connections on port80 at that location
135	tcp	msrpc	**Description :** Microsoft RPC services
139	tcp	netbios-ssn	**Description :** NETBIOS Session Service **Risk :** NetBIOS Session (TCP), Windows File and Printer Sharing **Solution :** It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port139 or
3306	tcp	mysql	**Description :** #mySQL
123	udp	ntp	**Description :** Network Time Protocol **Risk :** The network time protocol is a clean, simple, lightweight, and efficient protocol allowing clients to query servers for the current time (including the date) - (RFC2030, RFC1129) **Solution :** #An NTP (Network Time Protocol) server is listening on this port.It provides information about the current date and time of the remote system and may provide system information. (CVE-1999-0621)
137	udp	netbios-ns	**Description :** NETBIOS Name Service **Solution :** The remote host listens on udp port137 and replies to NetBIOS nbtscan requests. By sending a wildcard request it is possible to obtain the name of the remote system and the name of its domain.(CVE : CVE-1999-0621)
ipt_dos04		Microsoft Windows SMB PIPE Remote Denial of Service Vulnerability	**Description :** Microsoft Windows is prone to a remote denial-of-service vulnerability because the operating system fails to properly handle network traffic and the Server service fails to properly handle network messages. **Risk :** Impact of Vulnerability: Denial of Service and Remote Code Execution Microsoft Security Bulletin: MS06-063 **Solution :** Microsoft Security Update for Windows XP (KB923414) http://www.microsoft.com/downloads/details.aspx?familyid=08ab17b9-149c-44d4-96cf-B7a8c6b9dc22&displaylang=en

รูปที่ 3.8 ตัวอย่างรายงานส่วนที่ 3

3.4. รายละเอียดเกี่ยวกับโปรแกรม เป็นส่วนของการแสดงว่าข้อมูลเกี่ยวกับโปรแกรมทั้งหมด ได้แก่ ISAG Penetration Test Suite [IPT] version, xml output version, ipt.xsl version



รูปที่ 3.9 ตัวอย่างรายงานส่วนที่ 4

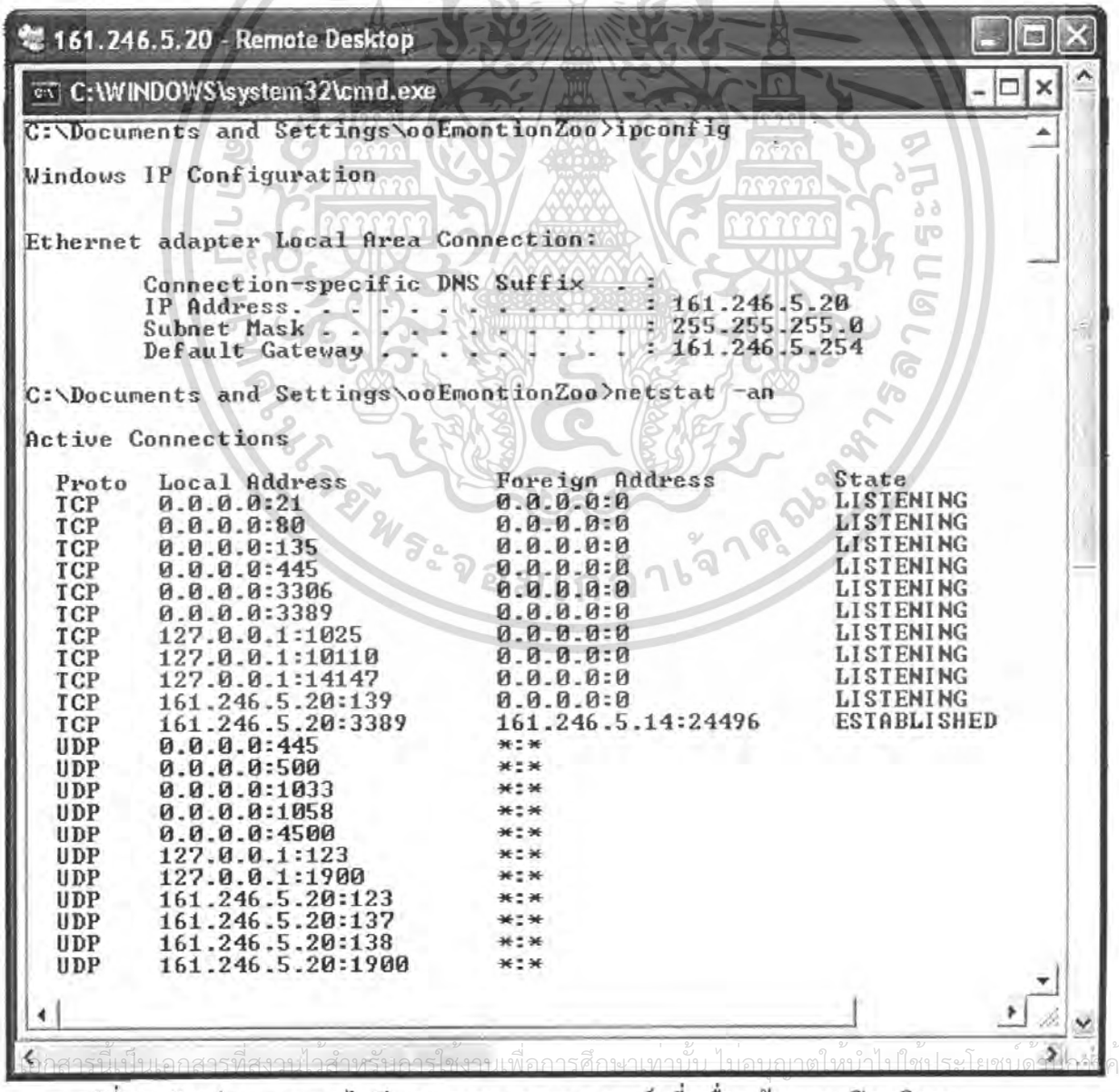
บทที่ 4

การทดลองและผลการทดลอง

4.1 บทนำ

ในการทดลองจะเป็นการทดสอบการทำงานของชุดโปรแกรม โดยจะแยกการทดสอบออกเป็น 3 ส่วน คือ

1. การทดสอบตัวเลือกของส่วนการสแกน (Scanner)
2. การทดสอบตัวเลือกของส่วนการแสวงหาประโยชน์ (Exploitation)
3. การทดสอบโดยรวมของชุดโปรแกรม



รูปที่ 4.1 ตัวอย่างหมายเลขไอพี และสถานะภาพของพอร์ตที่เครื่องเป้าหมายเปิดบริการ

จากรูปที่ 4.1 จะเห็นได้ว่า เครื่องเป้าหมายได้ทำการเปิดพอร์ต 21, 80, 135, 445, 3306, 3389, 1025, 10110, 14147, 139, 3389 ให้สามารถใช้บริการทางเครือข่ายได้

4.2 การทดสอบตัวเลือกของส่วนการสแกน (Scanner)

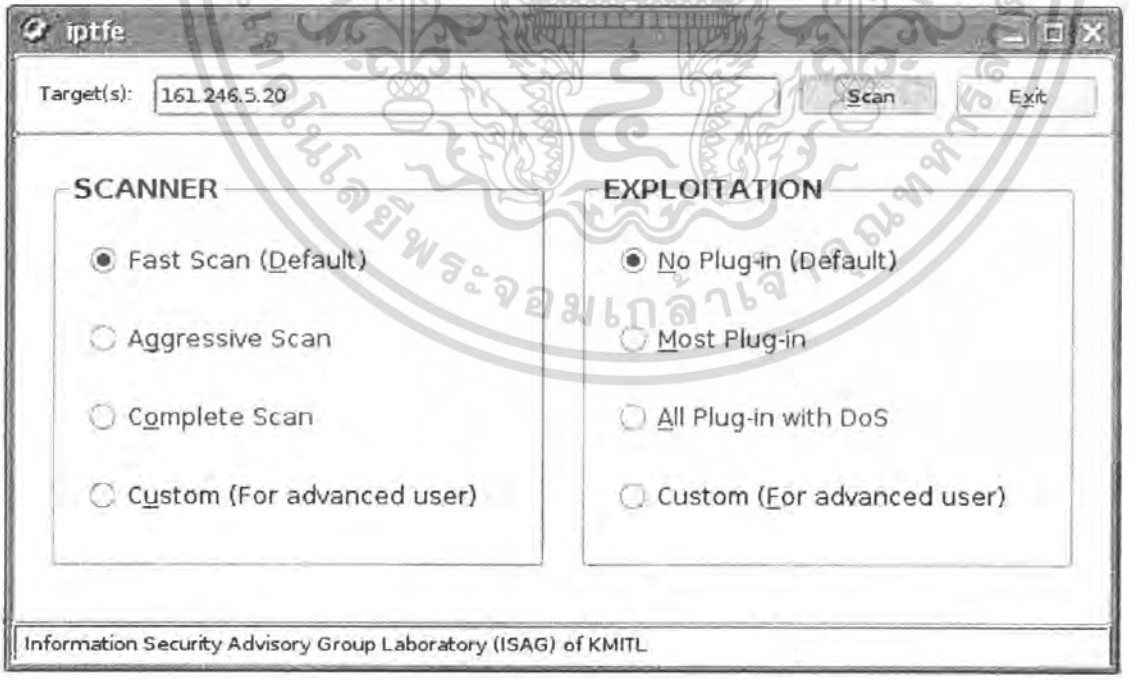
ในการทดสอบส่วนนี้จะเป็นการทดสอบในส่วนของการสแกน ในแต่ละตัวเลือกที่ได้ทำการสร้างขึ้นมา

4.2.1 วิธีการทดสอบ

1. ทำการตั้งค่าตัวเลือกต่างๆกันในส่วนการสแกน ไปทดสอบที่เป้าหมายเดียวกัน
2. ตรวจสอบผลที่ได้ว่าสามารถตรวจสอบ ได้มีความแม่นยำมากแค่ไหน
3. ตรวจสอบเวลาที่ใช้ในการสแกน

4.2.2 ผลการทดสอบ

1. การทดสอบตัวเลือก Fast Mode ของส่วนการสแกน



รูปที่ 4.2 หน้าต่างการตั้งค่าส่วนการสแกน และส่วนการแสวงหาประโยชน์

ISAG Penetration Test [IPT] Suite Report

Start Time :: Wed Feb 6 01:37:28 2008
Finish Time :: Wed Feb 6 01:39:24 2008
Total Scan :: 116 second
IPT's Option :: ipt -fast 161.246.5.20
Scan info :: 161.246.5.20 / isag20.ce.kmitl.ac.th |
Report :: Overview Scanning | Port | Exploitation | Scan Info | About IPT

Overview Scanning

Overview Scanning

IPT scan 1 host(s) :: Online 1 hosts(s) | Offline 0 hosts(s)
Microsoft Windows :: 161.246.5.20 |

Port Detection

Port		Service	Host (ip address)
1058	udp	nim	161.246.5.20 |
123	udp	ntp	161.246.5.20 |
135	tcp	msrpc	161.246.5.20 |
137	udp	netbios-ns	161.246.5.20 |
138	udp	netbios-dgm	161.246.5.20 |
139	tcp	netbios-ssn	161.246.5.20 |
1900	udp	UPnP	161.246.5.20 |
21	tcp	ftp	161.246.5.20 |
3306	tcp	mysql	161.246.5.20 |
3389	tcp	microsoft-rdp	161.246.5.20 |
445	tcp	microsoft-ds	161.246.5.20 |
4500	udp	sae-urn	161.246.5.20 |
500	udp	isakmp	161.246.5.20 |
80	tcp	http	161.246.5.20 |

161.246.5.20 / isag20.ce.kmitl.ac.th(online)

General

-- **Address** : 161.246.5.20 (ipv4) | 00:15:F2:A5:4D:A5 (mac) |

-- **Hostnames** : isag20.ce.kmitl.ac.th (PTR)

Port Detection

-- The 2258 ports scanned but not shown below are in state: **closed**

Port		State	Service	Product	Version	Extra info
21	tcp	open	ftp	FileZilla ftpd		
80	tcp	open	http	Apache httpd		(Win32) PHP/5.2.1
135	tcp	open	msrpc	Microsoft Windows RPC		
139	tcp	open	netbios-ssn			
445	tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds		
3306	tcp	open	mysql	MySQL		unauthorized
3389	tcp	open	microsoft-rdp	Microsoft Terminal Service		
123	udp	open	ntp	Microsoft NTP		
137	udp	open	netbios-ns	Microsoft Windows NT netbios-ssn		workgroup: WORKGROUP
138	udp	open|filtered	netbios-dgm			
445	udp	open|filtered	microsoft-ds			
500	udp	open|filtered	isakmp			
1058	udp	open|filtered	nim			
1900	udp	open|filtered	UPnP			
4500	udp	open|filtered	sae-urn			

Remote Operating System Guess

-- **IPT Suite used port** :: 21/tcp |

-- OS Match :: **Microsoft Windows XP SP2 (firewall disabled)** [Accuracy: 100%]

Other Detail

-- **Network distance** : 1 hops

รูปที่ 4.3 รายงานการทดสอบตัวเลือก Fast Mode ของส่วนการสแกน (1)

Recommendation For Prevention

Causes		Name	Recommendation
21	tcp	ftp	**Description :** File Transfer [Control Channel] **Risk :** File Transfer Protocol (FTP) is one of the oldest Internet protocols. FTP servers open their machine's port21 and listen for incoming client connections. FTP clients connect to port21 of remote FTP servers to initiate file transfer operations.
80	tcp	http	**Description :** World Wide Web HTTP **Risk :** This is the primary portused by the world wide web (www) system. Web servers open this portthen listen for incoming connections from web browsers. Similarly, when a web browser is given a remote address (like grc.com or amazon.com), it assumes that a remote web server will be listening for connections on port80 at that location
135	tcp	msrpc	**Description :** Microsoft RPC services
139	tcp	netbios-ssn	**Description :** NETBIOS Session Service **Risk :** NetBIOS Session (TCP), Windows File and Printer Sharing **Solution :** It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port139 or
445	tcp	microsoft-ds	**Description :** Microsoft-DS SMB file sharing **Solution :** #It is possible to get the remote operating system name andversion (Windows and/or Samba) by sending an authentication request to port139 or445. #The remote host is running one of the Microsoft Windows operating systems (CVE : CVE-1999-0504, CVE-1999-0505, CVE-1999-0506, CVE-2000-0222, CVE-2002-1117, CVE-2005-3595) #It was not possible to connect to PIPE\winreg on the remote host. If you intend to use Nessus to perform registry based checks, the registry checks will not work because the 'Remote Registry Access' service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.
3306	tcp	mysql	**Description :** #mySQL
3389	tcp	microsoft-rdp	
123	udp	ntp	**Description :** Network Time Protocol **Risk :** The network time protocol is a clean, simple, lightweight, and efficient protocol allowing clients to query servers for the current time (including the date) - (RFC2030, RFC1129) **Solution :** #An NTP (Network Time Protocol) server is listening on this port.It provides information about the current date and time of the remote system and may provide system information. (CVE-1999-0621)
137	udp	netbios-ns	**Description :** NETBIOS Name Service **Solution :** The remote host listens on udp port137 and replies to NetBIOS nbtscan requests. By sending a wildcard request it is possible to obtain the name of the remote system and the name of its domain.(CVE - CVE-1999-0621)

About ISAG Penetration Test [IPT] Suite

ISAG Penetration Test Suite [IPT] version :: 1.0
xml output version :: 1.00
ipt.xsl version :: 1.0

BY ISAG LAB at Computer Engineering of KMITL, Thailand

รูปที่ 4.4 รายงานการทดสอบตัวเลือก Fast Mode ของส่วนการสแกน (2)

2. การทดสอบตัวเลือก Aggressive Mode ของส่วนการสแกน

ISAG Penetration Test [IPT] Suite Report

Start Time :: Wed Feb 6 01:45:30 2008
Finish Time :: Wed Feb 6 01:48:24 2008
Total Scan :: 174 second
IPT's Option :: ipt -aggressive 161.246.5.20
Scan info :: 161.246.5.20 / isag20.ce.kmitl.ac.th |
Report :: Overview Scanning | Port | Exploitation | Scan Info | About IPT

Overview Scanning

Overview Scanning

IPT scan 1 host(s) :: Online 1 hosts(s) | Offline 0 hosts(s)
Microsoft Windows :: 161.246.5.20 |

Port Detection

Port		Service	Host (ip address)
1058	udp	nim	161.246.5.20 |
123	udp	ntp	161.246.5.20 |
135	tcp	msrpc	161.246.5.20 |
137	udp	netbios-ns	161.246.5.20 |
138	udp	netbios-dgm	161.246.5.20 |
139	tcp	netbios-ssn	161.246.5.20 |
1900	udp	UPnP	161.246.5.20 |
3306	tcp	mysql	161.246.5.20 |
3389	tcp	microsoft-rdp	161.246.5.20 |
445	udp	microsoft-ds	161.246.5.20 |
4500	udp	sae-urn	161.246.5.20 |
500	udp	isakmp	161.246.5.20 |
80	tcp	http	161.246.5.20 |

161.246.5.20 / isag20.ce.kmitl.ac.th(online)

General

-- **Address** : 161.246.5.20 (ipv4) | 00:15:F2:A5:4D:A5 (mac) |

-- **Hostnames** : isag20.ce.kmitl.ac.th (PTR)

Port Detection

-- The 3172 ports scanned but not shown below are in state: **closed**

Port		State	Service	Product	Version	Extra info
80	tcp	open	http	Apache httpd		(Win32) PHP/5.2.1
135	tcp	open	msrpc	Microsoft Windows RPC		
139	tcp	open	netbios-ssn			
3306	tcp	open	mysql	MySQL		unauthorized
3389	tcp	open	microsoft-rdp	Microsoft Terminal Service		
123	udp	open	ntp	Microsoft NTP		
137	udp	open	netbios-ns	Microsoft Windows NT netbios-ssn		workgroup: WORKGROUP
138	udp	open|filtered	netbios-dgm			
445	udp	open|filtered	microsoft-ds			
500	udp	open|filtered	isakmp			
1058	udp	open|filtered	nim			
1900	udp	open|filtered	UPnP			
4500	udp	open|filtered	sae-urn			

รูปที่ 4.5 รายงานการทดสอบตัวเลือก Aggressive Mode ของส่วนการสแกน (1)

Remote Operating System Guess

-- IPT Suite used port :: 80/tcp |

-- OS Match ::

Microsoft Windows 2000 Server SP4 [Accuracy: 96%]
Microsoft Windows XP SP2 [Accuracy: 96%]
Microsoft Windows 2000 SP4 [Accuracy: 96%]
Microsoft Windows 2003 Server SP1 [Accuracy: 94%]
Microsoft Windows 2000 SP3 [Accuracy: 93%]
Microsoft Windows 2000, SP0, SP1, or SP2 [Accuracy: 93%]
Microsoft Windows Server 2003 Enterprise Edition 64-Bit SP1 [Accuracy: 93%]
Microsoft Windows 2000 Server SP4 [Accuracy: 90%]

Other Detail

-- Network distance : 1 hops

Recommendation For Prevention

Causes		Name	Recommendation
80	tcp	http	**Description :** World Wide Web HTTP **Risk :** This is the primary portused by the world wide web (www) system. Web servers open this portthen listen for incoming connections from web browsers. Similarly, when a web browser is given a remote address (like grc.com or amazon.com), it assumes that a remote web server will be listening for connections on port80 at that location
135	tcp	msrpc	**Description :** Microsoft RPC services
139	tcp	netbios-ssn	**Description :** NETBIOS Session Service **Risk :** NetBIOS Session (TCP), Windows File and Printer Sharing **Solution :** It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port139 or
3306	tcp	mysql	**Description :** #mySQL
3389	tcp	microsoft-rdp	
123	udp	ntp	**Description :** Network Time Protocol **Risk :** The network time protocol is a clean, simple, lightweight, and efficient protocol allowing clients to query servers for the current time (including the date) - (RFC2030, RFC1129) **Solution :** #An NTP (Network Time Protocol) server is listening on this port.It provides information about the current date and time of the remote system and may provide system information. (CVE-1999-0621)
137	udp	netbios-ns	**Description :** NETBIOS Name Service **Solution :** The remote host listens on udp port137 and replies to NetBIOS nbtscan requests. By sending a wildcard request it is possible to obtain the name of the remote system and the name of its domain.(CVE : CVE-1999-0621)

About ISAG Penetration Test [IPT] Suite

ISAG Penetration Test Suite [IPT] version :: 1.0
xml output version :: 1.00
ipt.xsl version :: 1.0

BY ISAG LAB at Computer Engineering of KMITL, Thailand

รูปที่ 4.6 รายงานการทดสอบตัวเลือก Aggressive Mode ของส่วนการสแกน (2)

3. การทดสอบด้วย Complete Mode ของส่วนการสแกน

ISAG Penetration Test [IPT] Suite Report

Start Time ::	Wed Feb 6 01:51:28 2008
Finish Time ::	Wed Feb 6 01:54:26 2008
Total Scan ::	178 second
IPT's Option ::	ipt -complete 161.246.5.20
Scan info ::	161.246.5.20 / isag20.ce.kmitl.ac.th |
Report ::	Overview Scanning | Port | Exploitation | Scan Info | About IPT

Overview Scanning

Overview Scanning

IPT scan 1 host(s) ::	Online 1 hosts(s) | Offline 0 hosts(s)
Microsoft Windows ::	161.246.5.20 |

Port Detection

Port		Service	Host (ip address)
1058	udp	nim	161.246.5.20 |
123	udp	ntp	161.246.5.20 |
135	tcp	msrpc	161.246.5.20 |
137	udp	netbios-ns	161.246.5.20 |
138	udp	netbios-dgm	161.246.5.20 |
139	tcp	netbios-ssn	161.246.5.20 |
1900	udp	UPnP	161.246.5.20 |
3306	tcp	mysql	161.246.5.20 |
445	udp	microsoft-ds	161.246.5.20 |
4500	udp	sae-urn	161.246.5.20 |
500	udp	isakmp	161.246.5.20 |
80	tcp	http	161.246.5.20 |

161.246.5.20 / isag20.ce.kmitl.ac.th(online)

General

-- **Address** : 161.246.5.20 (ipv4) \| 00:15:F2:A5:4D:A5 (mac) \|

-- **Hostnames** : isag20.ce.kmitl.ac.th (PTR)

Port Detection

-- The 3173 ports scanned but not shown below are in state: **closed**

Port		State	Service	Product	Version	Extra info
80	tcp	open	http	Apache httpd		(Win32) PHP/5.2.1
135	tcp	open	msrpc	Microsoft Windows RPC		
139	tcp	open	netbios-ssn			
3306	tcp	open	mysql	MySQL		unauthorized
123	udp	open	ntp	Microsoft NTP		
137	udp	open	netbios-ns	Microsoft Windows NT netbios-ssn		workgroup: WORKGROUP
138	udp	open|filtered	netbios-dgm			
445	udp	open|filtered	microsoft-ds			
500	udp	open|filtered	isakmp			
1058	udp	open|filtered	nim			
1900	udp	open|filtered	UPnP			
4500	udp	open|filtered	sae-urn			

รูปที่ 4.7 รายงานการทดสอบตัวเลือก Complete Mode ของส่วนการสแกน (1)

Remote Operating System Guess

-- IPT Suite used port :: 80/tcp]

-- OS Match ::

Microsoft Windows 2000 Server SP4 [Accuracy: 97%]
Microsoft Windows XP SP2 [Accuracy: 96%]
Microsoft Windows 2000 SP4 [Accuracy: 95%]
Microsoft Windows 2003 Server SP1 [Accuracy: 94%]
Microsoft Windows 2000 SP3 [Accuracy: 93%]
Microsoft Windows Server 2003 Enterprise Edition 64-Bit SP1 [Accuracy: 93%]
Microsoft Windows 2000, SP0, SP1, or SP2 [Accuracy: 92%]
Microsoft Windows 2000 Server SP4 [Accuracy: 90%]

Other Detail

-- Network distance : 1 hops

Recommendation For Prevention

Causes		Name	Recommendation
80	tcp	http	**Description :** World Wide Web HTTP **Risk :** This is the primary portused by the world wide web (www) system. Web servers open this portthen listen for incoming connections from web browsers. Similarly, when a web browser is given a remote address (like grc.com or amazon.com), it assumes that a remote web server will be listening for connections on port80 at that location
135	tcp	msrpc	**Description :** Microsoft RPC services
139	tcp	netbios-ssn	**Description :** NETBIOS Session Service **Risk :** NetBIOS Session (TCP), Windows File and Printer Sharing **Solution :** It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port139 or
3306	tcp	mysql	**Description :** #mySQL
123	udp	ntp	**Description :** Network Time Protocol **Risk :** The network time protocol is a clean, simple, lightweight, and efficient protocol allowing clients to query servers for the current time (including the date) - (RFC2030, RFC1129) **Solution :** #An NTP (Network Time Protocol) server is listening on this port.It provides information about the current date and time of the remote system and may provide system information. (CVE-1999-0621)
137	udp	netbios-ns	**Description :** NETBIOS Name Service **Solution :** The remote host listens on udp port137 and replies to NetBIOS nbtscan requests. By sending a wildcard request it is possible to obtain the name of the remote system and the name of its domain.(CVE : CVE-1999-0621)

About ISAG Penetration Test [IPT] Suite

ISAG Penetration Test Suite [IPT] version :: 1.0
xml output version :: 1.00
ipt.xsl version :: 1.0

BY ISAG LAB at Computer Engineering of KMITL, Thailand

รูปที่ 4.8 รายงานการทดสอบตัวเลือก Complete Mode ของส่วนการสแกน (2)

4.3 การทดสอบตัวเลือกของส่วนการแสวงหาประโยชน์ (Exploitation)

ในการทดสอบส่วนนี้จะเป็นการทดสอบในส่วนของการแสวงหาประโยชน์ ในแต่ละตัวเลือกที่ได้ทำการสร้างขึ้นมา

4.3.1 วิธีการทดสอบ

1. ทำการตั้งค่าตัวเลือกต่างๆกัน ในส่วนการแสวงหาประโยชน์ ไปทดสอบที่เป้าหมายเดียวกัน

2. ตรวจสอบผลการทดสอบ เวลาที่ใช้ในการทดสอบ และสภาพของเครื่องที่ทำการทดสอบ ณ เวลาที่ทำการทดสอบ

4.3.2 ผลการทดสอบ

1. การทดสอบตัวเลือก No Plug-in ของส่วนการแสวงหาประโยชน์ ร่วมกับการสแกนแบบ Fast

-- ผลการทดสอบนั้นจะอยู่ที่รูป 4.3 และ 4.4

2. การทดสอบตัวเลือก Most Plug-in ของส่วนการแสวงหาประโยชน์ ร่วมกับการสแกนแบบ Fast

ISAG Penetration Test [IPT] Suite Report

Start Time ::	Thu Feb 7 02:04:22 2008
Finish Time ::	Thu Feb 7 02:06:49 2008
Total Scan ::	147 second
IPT's Option ::	ipt -fast -exploit --most-plugin 161.246.5.20
Scan info ::	161.246.5.20 / isag20.ce.kmitl.ac.th |
Report ::	Overview Scanning | Port | Exploitation | Scan Info | About IPT

Overview Scanning

Overview Scanning

IPT scan 1 host(s) ::	Online 1 hosts(s) | Offline 0 hosts(s)
Microsoft Windows ::	161.246.5.20 |

Port Detection

Port		Service	Host (ip address)
1025	udp	blackjack	161.246.5.20 |
123	udp	ntp	161.246.5.20 |
135	tcp	msrpc	161.246.5.20 |
137	udp	netbios-ns	161.246.5.20 |
138	udp	netbios-dgm	161.246.5.20 |
139	tcp	netbios-ssn	161.246.5.20 |
1900	udp	UPnP	161.246.5.20 |
21	tcp	ftp	161.246.5.20 |
3306	tcp	mysql	161.246.5.20 |
3389	tcp	microsoft-rdp	161.246.5.20 |
445	tcp	microsoft-ds	161.246.5.20 |
4500	udp	sae-urn	161.246.5.20 |
500	udp	isakmp	161.246.5.20 |
80	tcp	http	161.246.5.20 |

161.246.5.20 / isag20.ce.kmitl.ac.th(online)

General

-- **Address** : 161.246.5.20 (ipv4) | 00:15:F2:A5:4D:A5 (mac) |

-- **Hostnames** : isag20.ce.kmitl.ac.th (PTR)

Port Detection

-- The 2258 ports scanned but not shown below are in state: **closed**

Port		State	Service	Product	Version	Extra info
21	tcp	open	ftp	FileZilla ftpd		
80	tcp	open	http	Apache httpd		(Win32) PHP/5.2.1
135	tcp	open	msrpc	Microsoft Windows RPC		
139	tcp	open	netbios-ssn			
445	tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds		
3306	tcp	open	mysql	MySQL		unauthorized
3389	tcp	open	microsoft-rdp	Microsoft Terminal Service		
123	udp	open	ntp	NTP		
137	udp	open	netbios-ns	Microsoft Windows NT netbios-ssn		workgroup: WORKGROUP
138	udp	open|filtered	netbios-dgm			
445	udp	open|filtered	microsoft-ds			
500	udp	open|filtered	isakmp			
1025	udp	open|filtered	blackjack			
1900	udp	open|filtered	UPnP			
4500	udp	open|filtered	sae-urn			

รูปที่ 4.9 รายงานการทดสอบตัวเลือก Most Plug-in ของส่วนการแสวงหาประโยชน์ (1)

Remote Operating System Guess

-- **IPT Suite used port :: 21/tcp |**

-- OS Match :: **Microsoft Windows XP SP2 (firewall disabled) [Accuracy: 100%]**

Other Detail

-- **Network distance : 1 hops**

Exploitation

Recommendation For Prevention

Causes		Name	Recommendation
21	tcp	ftp	**Description :** File Transfer [Control Channel] **Risk :** File Transfer Protocol (FTP) is one of the oldest Internet protocols. FTP servers open their machine's port21 and listen for incoming client connections. FTP clients connect to port21 of remote FTP servers to initiate file transfer operations.
80	tcp	http	**Description :** World Wide Web HTTP **Risk :** This is the primary portused by the world wide web (www) system. Web servers open this portthen listen for incoming connections from web browsers. Similarly, when a web browser is given a remote address (like grc.com or amazon.com), it assumes that a remote web server will be listening for connections on port80 at that location
135	tcp	msrpc	**Description :** Microsoft RPC services
139	tcp	netbios-ssn	**Description :** NETBIOS Session Service **Risk :** NetBIOS Session (TCP), Windows File and Printer Sharing **Solution :** It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port139 or
445	tcp	microsoft-ds	**Description :** Microsoft-DS SMB file sharing **Solution :** #It is possible to get the remote operating system name andversion (Windows and/or Samba) by sending an authentication request to port139 or445. #The remote host is running one of the Microsoft Windows operating systems (CVE : CVE-1999-0504, CVE-1999-0505, CVE-1999-0506, CVE-2000-0222, CVE-2002-1117, CVE-2005-3595) #It was not possible to connect to PIPE\winreg on the remote host. If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access' service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.
3306	tcp	mysql	**Description :** #mySQL
3389	tcp	microsoft-rdp	
123	udp	ntp	**Description :** Network Time Protocol **Risk :** The network time protocol is a clean, simple, lightweight, and efficient protocol allowing clients to query servers for the current time (including the date) - (RFC2030, RFC1129) **Solution :** #An NTP (Network Time Protocol) server is listening on this port.It provides information about the current date and time of the remote system and may provide system information. (CVE-1999-0621)
137	udp	netbios-ns	**Description :** NETBIOS Name Service **Solution :** The remote host listens on udp port137 and replies to NetBIOS nbtscan requests. By sending a wildcard request it is possible to obtain the name of the remote system and the name of its domain.(CVE : CVE-1999-0621)

About ISAG Penetration Test [IPT] Suite

ISAG Penetration Test Suite [IPT] version :: 1.0
xml output version :: 1.00
ipt.xsl version :: 1.0

BY ISAG LAB at Computer Engineering of KMITL, Thailand

"

รูปที่ 4.10 รายงานการทดสอบตัวเลือก Most Plug-in ของส่วนการแสวงหาประโยชน์ (2)

3. การทดสอบตัวเลือก All Pug-in with DoS ของส่วนการแสวงหาประโยชน์ ร่วมกับการสแกนแบบ Fast

ISAG Penetration Test [IPT] Suite Report

Start Time ::	Thu Feb 7 03:18:12 2008
Finish Time ::	Thu Feb 7 03:21:53 2008
Total Scan ::	221 second
IPT's Option ::	ipt -fast -exploit --all-plugin 161.246.5.20
Scan info ::	[redacted]
Report ::	Overview Scanning | Port | Exploitation | Scan Info | About IPT

Overview Scanning

Overview Scanning

IPT scan 1 host(s) ::	Online 1 hosts(s) | Offline 0 hosts(s)
Microsoft Windows ::	161.246.5.20 |

Port Detection

Port		Service	Host (ip address)
1025	udp	blackjack	161.246.5.20 |
123	udp	ntp	161.246.5.20 |
135	tcp	msrpc	161.246.5.20 |
137	udp	netbios-ns	161.246.5.20 |
138	udp	netbios-dgm	161.246.5.20 |
139	tcp	netbios-ssn	161.246.5.20 |
1900	udp	UPnP	161.246.5.20 |
21	tcp	ftp	161.246.5.20 |
3306	tcp	mysql	161.246.5.20 |
3389	tcp	microsoft-rdp	161.246.5.20 |
445	tcp	microsoft-ds	161.246.5.20 |
4500	udp	sae-urn	161.246.5.20 |
500	udp	isakmp	161.246.5.20 |
80	tcp	http	161.246.5.20 |

Exploitation

Exploit ID	Exploit Name	Host (ip address)
ipt_dos04	Microsoft Windows SMB PIPE Remote Denial of Service Vulnerability	161.246.5.20 |

161.246.5.20 / isag20.ce.kmitl.ac.th(online)

General

-- **Address** : 161.246.5.20 (ipv4) | 00:15:F2:A5:4D:A5 (mac) |

-- **Hostnames** : isag20.ce.kmitl.ac.th (PTR)

Port Detection

-- The 2258 ports scanned but not shown below are in state: closed

Port		State	Service	Product	Version	Extra Info
21	tcp	open	ftp	FileZilla ftpd		
80	tcp	open	http	Apache httpd		(Win32) PHP/5.2.1
135	tcp	open	msrpc	Microsoft Windows RPC		
139	tcp	open	netbios-ssn			
445	tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds		
3306	tcp	open	mysql	MySQL		unauthorized
3389	tcp	open	microsoft-rdp	Microsoft Terminal Service		
123	udp	open	ntp	NTP		
137	udp	open	netbios-ns	Microsoft Windows NT netbios-ssn		workgroup: WORKGROUP
138	udp	open|filtered	netbios-dgm			
445	udp	open|filtered	microsoft-ds			
500	udp	open|filtered	isakmp			
1025	udp	open|filtered	blackjack			
1900	udp	open|filtered	UPnP			
4500	udp	open|filtered	sae-urn			

Remote Operating System Guess

-- **IPT Suite used port** :: 21/tcp |

-- OS Match ::

Microsoft Windows 2000 Server SP4 [Accuracy: 97%]
Microsoft Windows XP SP2 [Accuracy: 96%]
Microsoft Windows 2000 SP4 [Accuracy: 96%]
Microsoft Windows 2003 Server SP1 [Accuracy: 95%]
Microsoft Windows Server 2003 Enterprise Edition 64-Bit SP1 [Accuracy: 93%]
Microsoft Windows 2000 SP3 [Accuracy: 93%]
Microsoft Windows 2000, SP0, SP1, or SP2 [Accuracy: 93%]
Microsoft Windows 2000 Server SP4 [Accuracy: 89%]

รูปที่ 4.11 รายงานการทดสอบตัวเลือก All Pug-in with DoS ของส่วนการแสวงหาประโยชน์ (1)

Other Detail

-- **Network distance** : 1 hops

Exploitation

-ipt_dos04 : Microsoft Windows SMB PIPE Remote Denial of Service Vulnerability

Recommendation For Prevention

Causes		Name	Recommendation
21	tcp	ftp	**Description :** File Transfer [Control Channel] **Risk :** File Transfer Protocol (FTP) is one of the oldest Internet protocols. FTP servers open their machine's port21 and listen for incoming client connections. FTP clients connect to port21 of remote FTP servers to initiate file transfer operations.
80	tcp	http	**Description :** World Wide Web HTTP **Risk :** This is the primary portused by the world wide web (www) system. Web servers open this portthen listen for incoming connections from web browsers. Similarly, when a web browser is given a remote address (like grc.com or amazon.com), it assumes that a remote web server will be listening for connections on port80 at that location
135	tcp	msrpc	**Description :** Microsoft RPC services
139	tcp	netbios-ssn	**Description :** NETBIOS Session Service **Risk :** NetBIOS Session (TCP), Windows File and Printer Sharing **Solution :** It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port139 or
445	tcp	microsoft-ds	**Description :** Microsoft-DS SMB file sharing **Solution :** #It is possible to get the remote operating system name andversion (Windows and/or Samba) by sending an authentication request to port139 or445. #The remote host is running one of the Microsoft Windows operating systems (CVE : CVE-1999-0504, CVE-1999-0505, CVE-1999-0506, CVE-2000-0222, CVE-2002-1117, CVE-2005-3595) #It was not possible to connect to PIPE\winreg on the remote host. If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access' service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.
3306	tcp	mysql	**Description :** #mySQL
3389	tcp	microsoft-rdp	
123	udp	ntp	**Description :** Network Time Protocol **Risk :** The network time protocol is a clean, simple, lightweight, and efficient protocol allowing clients to query servers for the current time (including the date) - (RFC2030, RFC1129) **Solution :** #An NTP (Network Time Protocol) server is listening on this port.It provides information about the current date and time of the remote system and may provide system information. (CVE-1999-0621)
137	udp	netbios-ns	**Description :** NETBIOS Name Service **Solution :** The remote host listens on udp port137 and replies to NetBIOS nbtscan requests. By sending a wildcard request it is possible to obtain the name of the remote system and the name of its domain.(CVE : CVE-1999-0621)
ipt_dos04		Microsoft Windows SMB PIPE Remote Denial of Service Vulnerability	**Description :** Microsoft Windows is prone to a remote denial-of-service vulnerability because the operating system fails to properly handle network traffic and the Server service fails to properly handle network messages. **Risk :** Impact of Vulnerability: Denial of Service and Remote Code Execution Microsoft Security Bulletin: MS06-063 **Solution :** Microsoft Security Update for Windows XP (KB923414) http://www.microsoft.com/downloads/details.aspx?familyid=08ab17b9-149c-44d4-96cf-87a8c6b9dc22&displaylang=en

About ISAG Penetration Test [IPT] Suite

ISAG Penetration Test Suite [IPT] version :: 1.0
xml output version :: 1.00
ipt.xsl version :: 1.0

BY ISAG LAB at Computer Engineering of KMITL, Thailand

รูปที่ 4.12 รายงานการทดสอบตัวเลือก All Pug-in with DoS ของส่วนการแสวงหาประโยชน์ (2)

4.4 การทดสอบโดยรวมของชุดโปรแกรม - รวมกันทั้งส่วนการสแกน และส่วนการแสวงหาประโยชน์

4.4.1 วิธีการทดสอบ

1. ทำการตั้งค่าตัวเลือกต่างๆกัน ในส่วนการแสวงหาประโยชน์ และส่วนของการสแกนไปทดสอบที่เป้าหมายเดียวกัน

2. ตรวจสอบผลการทดสอบ เวลาที่ใช้ในการทดสอบ และสภาพของเครื่องที่ทำการทดสอบ ณ เวลาที่ทำการทดสอบ

4.4.2 ผลการทดสอบ

1. ทดสอบตัวเลือก Fast Mode ร่วมกับ No Plug-in
   - ผลการทดสอบในรูปที่ 4.3 และ 4.4
2. ทดสอบตัวเลือก Fast Mode ร่วมกับ Most Plug-in
   - ผลการทดสอบในรูปที่ 4.9 และ 4.10
3. ทดสอบตัวเลือก Fast Mode ร่วมกับ All Plug-in with DoS
   - ผลการทดสอบในรูปที่ 4.11 และ 4.12
4. ทดสอบตัวเลือก Aggressive Mode ร่วมกับ No Plug-in
   - ผลการทดสอบในรูปที่ 4.5 และ 4.6

5. ทดสอบตัวเลือก Aggressive Mode ร่วมกับ Most Plug-in

ISAG Penetration Test [IPT] Suite Report

Start Time :: Thu Feb 7 03:48:08 2008
Finish Time :: Thu Feb 7 03:50:44 2008
Total Scan :: 156 second
IPT's Option :: ipt -aggressive -exploit --most-plugin 161.246.5.20
Scan info :: 161.246.5.20 / isag20.ce.kmitl.ac.th |
Report :: Overview Scanning | Port | Exploitation | Scan Info | About IPT

Overview Scanning

Overview Scanning

IPT scan 1 host(s) :: Online 1 hosts(s) | Offline 0 hosts(s)
Microsoft Windows :: 161.246.5.20 |

Port Detection

Port		Service	Host (ip address)
1025	udp	blackjack	161.246.5.20 |
123	udp	ntp	161.246.5.20 |
135	tcp	msrpc	161.246.5.20 |
137	udp	netbios-ns	161.246.5.20 |
138	udp	netbios-dgm	161.246.5.20 |
139	tcp	netbios-ssn	161.246.5.20 |
1900	udp	UPnP	161.246.5.20 |
227	udp		161.246.5.20 |
3306	tcp	mysql	161.246.5.20 |
3389	tcp	microsoft-rdp	161.246.5.20 |
445	udp	microsoft-ds	161.246.5.20 |
4500	udp	sae-urn	161.246.5.20 |
500	udp	isakmp	161.246.5.20 |
80	tcp	http	161.246.5.20 |

161.246.5.20 / isag20.ce.kmitl.ac.th(online)

General

-- **Address :** 161.246.5.20 (ipv4) | 00:15:F2:A5:4D:A5 (mac) |

-- **Hostnames :** isag20.ce.kmitl.ac.th (PTR)

Port Detection

-- The 3171 ports scanned but not shown below are in state: **closed**

Port		State	Service	Product	Version	Extra info
80	tcp	open	http	Apache httpd		(Win32) PHP/5.2.1
135	tcp	open	msrpc	Microsoft Windows RPC		
139	tcp	open	netbios-ssn			
3306	tcp	open	mysql	MySQL		unauthorized
3389	tcp	open	microsoft-rdp	Microsoft Terminal Service		
123	udp	open	ntp	NTP		
137	udp	open	netbios-ns	Microsoft Windows NT netbios-ssn		workgroup: WORKGROUP
138	udp	open|filtered	netbios-dgm			
227	udp	open|filtered				
445	udp	open|filtered	microsoft-ds			
500	udp	open|filtered	isakmp			
1025	udp	open|filtered	blackjack			
1900	udp	open|filtered	UPnP			
4500	udp	open|filtered	sae-urn			

รูปที่ 4.13 รายงานการทดสอบตัวเลือก Aggressive Mode ร่วมกับ Most Plug-in (1)

Remote Operating System Guess

-- **IPT Suite used port** :: 80/tcp |

-- OS Match :: **Microsoft Windows XP SP2 (firewall disabled)** [Accuracy: 100%]

Other Detail

-- **Network distance** : 1 hops

Exploitation

Recommendation For Prevention

Causes		Name	Recommendation
80	tcp	http	**Description :** World Wide Web HTTP **Risk :** This is the primary portused by the world wide web (www) system. Web servers open this portthen listen for incoming connections from web browsers. Similarly, when a web browser is given a remote address (like grc.com or amazon.com), it assumes that a remote web server will be listening for connections on port80 at that location
135	tcp	msrpc	**Description :** Microsoft RPC services
139	tcp	netbios-ssn	**Description :** NETBIOS Session Service **Risk :** NetBIOS Session (TCP), Windows File and Printer Sharing **Solution :** It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port139 or
3306	tcp	mysql	**Description :** #mySQL
3389	tcp	microsoft-rdp	
123	udp	ntp	**Description :** Network Time Protocol **Risk :** The network time protocol is a clean, simple, lightweight, and efficient protocol allowing clients to query servers for the current time (including the date) - (RFC2030, RFC1129) **Solution :** #An NTP (Network Time Protocol) server is listening on this port.It provides information about the current date and time of the remote system and may provide system information. (CVE-1999-0621)
137	udp	netbios-ns	**Description :** NETBIOS Name Service **Solution :** The remote host listens on udp port137 and replies to NetBIOS nbtscan requests. By sending a wildcard request it is possible to obtain the name of the remote system and the name of its domain.(CVE : CVE-1999-0621)

About ISAG Penetration Test [IPT] Suite

ISAG Penetration Test Suite [IPT] version :: 1.0
xml output version :: 1.00
ipt.xsl version :: 1.0

BY ISAG LAB at Computer Engineering of KMITL, Thailand

รูปที่ 4.14 รายงานการทดสอบตัวเลือก Aggressive Mode ร่วมกับ Most Plug-in (2)

1. การทดสอบตัวเลือก Aggressive Mode ร่วมกับ All Plug-in with DoS

ISAG Penetration Test [IPT] Suite Report

Start Time :: Thu Feb 7 03:59:25 2008
Finish Time :: Thu Feb 7 04:04:24 2008
Total Scan :: 299 second
IPT's Option :: ipt -aggressive -exploit --all-plugin 161.246.5.20
Scan info :: 161.246.5.20 / isag20.ce.kmitl.ac.th |
Report :: Overview Scanning | Port | Exploitation | Scan Info | About IPT

Overview Scanning

Overview Scanning

IPT scan 1 host(s) :: Online 1 hosts(s) | Offline 0 hosts(s)
Microsoft Windows :: 161.246.5.20 |

Port Detection

Port		Service	Host (ip address)
1025	udp	blackjack	161.246.5.20 |
123	udp	ntp	161.246.5.20 |
135	tcp	msrpc	161.246.5.20 |
137	udp	netbios-ns	161.246.5.20 |
138	udp	netbios-dgm	161.246.5.20 |
139	tcp	netbios-ssn	161.246.5.20 |
1900	udp	UPnP	161.246.5.20 |
3306	tcp	mysql	161.246.5.20 |
3389	tcp	microsoft-rdp	161.246.5.20 |
445	udp	microsoft-ds	161.246.5.20 |
4500	udp	sae-urn	161.246.5.20 |
500	udp	isakmp	161.246.5.20 |
80	tcp	http	161.246.5.20 |

Exploitation

Exploit ID	Exploit Name	Host (ip address)
ipt_dos04	Microsoft Windows SMB PIPE Remote Denial of Service Vulnerability	161.246.5.20 |

161.246.5.20 / isag20.ce.kmitl.ac.th(online)

General

-- **Address** : 161.246.5.20 (ipv4) | 00:15:F2:A5:4D:A5 (mac) |

-- **Hostnames** : isag20.ce.kmitl.ac.th (PTR)

Port Detection

-- The 3172 ports scanned but not shown below are in state: **closed**

Port		State	Service	Product	Version	Extra Info
80	tcp	open	http	Apache httpd		(Win32) PHP/5.2.1
135	tcp	open	msrpc	Microsoft Windows RPC		
139	tcp	open	netbios-ssn			
3306	tcp	open	mysql	MySQL		unauthorized
3389	tcp	open	microsoft-rdp	Microsoft Terminal Service		
123	udp	open	ntp	NTP		
137	udp	open	netbios-ns	Microsoft Windows NT netbios-ssn		workgroup: WORKGROUP
138	udp	open|filtered	netbios-dgm			
445	udp	open|filtered	microsoft-ds			
500	udp	open|filtered	isakmp			
1025	udp	open|filtered	blackjack			
1900	udp	open|filtered	UPnP			
4500	udp	open|filtered	sae-urn			

รูปที่ 4.15 รายงานการทดสอบตัวเลือก Aggressive Mode ร่วมกับ All Plug-in with DoS (1)

Remote Operating System Guess

-- **IPT Suite used port** :: 80/tcp]

-- OS Match ::

Microsoft Windows 2000 Server SP4 [Accuracy: 96%]
Microsoft Windows XP SP2 [Accuracy: 96%]
Microsoft Windows 2000 SP4 [Accuracy: 96%]
Microsoft Windows 2003 Server SP1 [Accuracy: 94%]
Microsoft Windows Server 2003 Enterprise Edition 64-Bit SP1 [Accuracy: 93%]
Microsoft Windows 2000 SP3 [Accuracy: 93%]
Microsoft Windows 2000, SP0, SP1, or SP2 [Accuracy: 93%]
Microsoft Windows 2000 Server SP4 [Accuracy: 89%]

Other Detail

-- **Network distance** : 1 hops

Exploitation

-**Ipt_dos04** : Microsoft Windows SMB PIPE Remote Denial of Service Vulnerability

Recommendation For Prevention

Causes		Name	Recommendation
80	tcp	http	**Description :** World Wide Web HTTP **Risk :** This is the primary portused by the world wide web (www) system. Web servers open this portthen listen for incoming connections from web browsers. Similarly, when a web browser is given a remote address (like grc.com or amazon.com), it assumes that a remote web server will be listening for connections on port80 at that location
135	tcp	msrpc	**Description :** Microsoft RPC services
139	tcp	netbios-ssn	**Description :** NETBIOS Session Service **Risk :** NetBIOS Session (TCP), Windows File and Printer Sharing **Solution :** It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port139 or
3306	tcp	mysql	**Description :** #mySQL
3389	tcp	microsoft-rdp	
123	udp	ntp	**Description :** Network Time Protocol **Risk :** The network time protocol is a clean, simple, lightweight, and efficient protocol allowing clients to query servers for the current time (including the date) - (RFC2030, RFC1129) **Solution :** #An NTP (Network Time Protocol) server is listening on this port.It provides information about the current date and time of the remote system and may provide system information. (CVE-1999-0621)
137	udp	netbios-ns	**Description :** NETBIOS Name Service **Solution :** The remote host listens on udp port137 and replies to NetBIOS nbtscan requests. By sending a wildcard request it is possible to obtain the name of the remote system and the name of its domain.(CVE : CVE-1999-0621)
ipt_dos04		Microsoft Windows SMB PIPE Remote Denial of Service Vulnerability	**Description :** Microsoft Windows is prone to a remote denial-of-service vulnerability because the operating system fails to properly handle network traffic and the Server service fails to properly handle network messages. **Risk :** Impact of Vulnerability: Denial of Service and Remote Code Execution Microsoft Security Bulletin: MS06-063 **Solution :** Microsoft Security Update for Windows XP (KB923414) http://www.microsoft.com/downloads/details.aspx?familyid=08ab17b9-149c-44d4-96cf-87a8c6b9dc228displaylang=en

About ISAG Penetration Test [IPT] Suite

ISAG Penetration Test Suite [IPT] version :: 1.0
xml output version :: 1.00
ipt.xsl version :: 1.0

BY ISAG LAB at Computer Engineering of KMITL, Thailand

"

รูปที่ 4.16 รายงานการทดสอบตัวเลือก Aggressive Mode ร่วมกับ All Plug-in with DoS (2)

7. การทดสอบตัวเลือก Complete Mode ร่วมกับ No Plug-in

   - ผลการทดสอบในรูปที่ 4.7 และ 4.8

8. การทดสอบตัวเลือก Complete Mode ร่วมกับ Most Plug-in

ISAG Penetration Test [IPT] Suite Report

Start Time ::	Thu Feb 7 04:14:17 2008
Finish Time ::	Thu Feb 7 04:18:50 2008
Total Scan ::	273 second
IPT's Option ::	ipt -complete -exploit --most-plugin 161.246.5.20
Scan info ::	161.246.5.20 / isag20.ce.kmitl.ac.th |
Report ::	Overview Scanning | Port | Exploitation | Scan Info | About IPT

Overview Scanning

Overview Scanning

IPT scan 1 host(s) ::	Online 1 hosts(s) | Offline 0 hosts(s)
Microsoft Windows ::	161.246.5.20 |

Port Detection

Port		Service	Host (ip address)
1025	udp	blackjack	161.246.5.20 |
123	udp	ntp	161.246.5.20 |
135	tcp	msrpc	161.246.5.20 |
137	udp	netbios-ns	161.246.5.20 |
138	udp	netbios-dgm	161.246.5.20 |
139	tcp	netbios-ssn	161.246.5.20 |
1900	udp	UPnP	161.246.5.20 |
3306	tcp	mysql	161.246.5.20 |
445	udp	microsoft-ds	161.246.5.20 |
4500	udp	sae-urn	161.246.5.20 |
500	udp	isakmp	161.246.5.20 |
80	tcp	http	161.246.5.20 |

161.246.5.20 / isag20.ce.kmitl.ac.th(online)

General

-- **Address** : 161.246.5.20 (ipv4) \| 00:15:F2:A5:4D:A5 (mac) \|

-- **Hostnames** : isag20.ce.kmitl.ac.th (PTR)

Port Detection

-- The 3173 ports scanned but not shown below are in state: **closed**

Port		State	Service	Product	Version	Extra info
80	tcp	open	http	Apache httpd		(Win32) PHP/5.2.1
135	tcp	open	msrpc	Microsoft Windows RPC		
139	tcp	open	netbios-ssn			
3306	tcp	open	mysql	MySQL		unauthorized
123	udp	open|filtered	ntp			
137	udp	open|filtered	netbios-ns			
138	udp	open|filtered	netbios-dgm			
445	udp	open|filtered	microsoft-ds			
500	udp	open|filtered	isakmp			
1025	udp	open|filtered	blackjack			
1900	udp	open|filtered	UPnP			
4500	udp	open|filtered	sae-urn			

รูปที่ 4.17 รายงานการทดสอบตัวเลือก Complete Mode ร่วมกับ Most Plug-in (1)

Remote Operating System Guess

-- IPT Suite used port :: 80/tcp |

-- OS Match ::

Microsoft Windows 2000 Server SP4 [Accuracy: 97%]
Microsoft Windows XP SP2 [Accuracy: 96%]
Microsoft Windows 2000 SP4 [Accuracy: 95%]
Microsoft Windows 2003 Server SP1 [Accuracy: 94%]
Microsoft Windows Server 2003 Enterprise Edition 64-Bit SP1 [Accuracy: 93%]
Microsoft Windows 2000 SP3 [Accuracy: 92%]
Microsoft Windows 2000, SP0, SP1, or SP2 [Accuracy: 92%]
Microsoft Windows 2000 Server SP4 [Accuracy: 89%]

Other Detail

-- Network distance : 1 hops

Exploitation

Recommendation For Prevention

Causes		Name	Recommendation
80	tcp	http	**Description :** World Wide Web HTTP **Risk :** This is the primary portused by the world wide web (www) system. Web servers open this portthen listen for incoming connections from web browsers. Similarly, when a web browser is given a remote address (like grc.com or amazon.com), it assumes that a remote web server will be listening for connections on port80 at that location
135	tcp	msrpc	**Description :** Microsoft RPC services
139	tcp	netbios-ssn	**Description :** NETBIOS Session Service **Risk :** NetBIOS Session (TCP), Windows File and Printer Sharing **Solution :** It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port139 or
3306	tcp	mysql	**Description :** #mySQL

About ISAG Penetration Test [IPT] Suite

ISAG Penetration Test Suite [IPT] version :: 1.0
xml output version :: 1.00
ipt.xsl version :: 1.0

BY ISAG LAB at Computer Engineering of KMITL, Thailand

"

รูปที่ 4.18 รายงานการทดสอบตัวเลือก Complete Mode ร่วมกับ Most Plug-in (2)

9. การทดสอบตัวเลือก Complete Mode ร่วมกับ All Pug-in with DoS

ISAG Penetration Test [IPT] Suite Report

Start Time :: Thu Feb 7 04:32:32 2008
Finish Time :: Thu Feb 7 04:38:12 2008
Total Scan :: 340 second
IPT's Option :: ipt -complete -exploit --all-plugin 161.246.5.20
Scan info :: 161.246.5.20 / isag20.ce.kmitl.ac.th |
Report :: Overview Scanning | Port | Exploitation | Scan Info | About IPT

Overview Scanning

Overview Scanning

IPT scan 1 host(s) :: Online 1 hosts(s) | Offline 0 hosts(s)
Microsoft Windows :: 161.246.5.20 |

Port Detection

Port		Service	Host (ip address)
1025	udp	blackjack	161.246.5.20 |
123	udp	ntp	161.246.5.20 |
135	tcp	msrpc	161.246.5.20 |
137	udp	netbios-ns	161.246.5.20 |
138	udp	netbios-dgm	161.246.5.20 |
139	tcp	netbios-ssn	161.246.5.20 |
1900	udp	UPnP	161.246.5.20 |
3306	tcp	mysql	161.246.5.20 |
445	udp	microsoft-ds	161.246.5.20 |
4500	udp	sae-urn	161.246.5.20 |
500	udp	isakmp	161.246.5.20 |
80	tcp	http	161.246.5.20 |

Exploitation

Exploit ID	Exploit Name	Host (ip address)
ipt_dos04	Microsoft Windows SMB PIPE Remote Denial of Service Vulnerability	161.246.5.20 |

161.246.5.20 / isag20.ce.kmitl.ac.th(online)

General

-- **Address** : 161.246.5.20 (ipv4) | 00:1S:F2:A5:4D:A5 (mac) |

-- **Hostnames** : isag20.ce.kmitl.ac.th (PTR)

Port Detection

-- The 3173 ports scanned but not shown below are in state: **closed**

Port		State	Service	Product	Version	Extra Info
80	tcp	open	http	Apache httpd		(Win32) PHP/5.2.1
135	tcp	open	msrpc	Microsoft Windows RPC		
139	tcp	open	netbios-ssn			
3306	tcp	open	mysql	MySQL		unauthorized
123	udp	open	ntp	NTP		
137	udp	open	netbios-ns	Microsoft Windows NT netbios-ssn		workgroup: WORKGROUP
138	udp	open|filtered	netbios-dgm			
445	udp	open|filtered	microsoft-ds			
500	udp	open|filtered	isakmp			
1025	udp	open|filtered	blackjack			
1900	udp	open|filtered	UPnP			
4500	udp	open|filtered	sae-urn			

รูปที่ 4.19 รายงานการทดสอบตัวเลือก Complete Mode ร่วมกับ All Plug-in with DoS (1)

Remote Operating System Guess

-- **IPT Suite used port** :: 80/tcp]

-- OS Match ::

Microsoft Windows 2000 Server SP4 [Accuracy: 96%]
Microsoft Windows XP SP2 [Accuracy: 96%]
Microsoft Windows 2000 SP4 [Accuracy: 95%]
Microsoft Windows 2003 Server SP1 [Accuracy: 94%]
Microsoft Windows Server 2003 Enterprise Edition 64-Bit SP1 [Accuracy: 93%]
Microsoft Windows 2000 SP3 [Accuracy: 92%]
Microsoft Windows 2000, SP0, SP1, or SP2 [Accuracy: 92%]
Microsoft Windows 2000 Server SP4 [Accuracy: 89%]

Other Detail

-- **Network distance** : 1 hops

Exploitation

-**ipt_dos04** : Microsoft Windows SMB PIPE Remote Denial of Service Vulnerability

Recommendation For Prevention

Causes		Name	Recommendation
80	tcp	http	**Description :** World Wide Web HTTP **Risk :** This is the primary portused by the world wide web (www) system. Web servers open this portthen listen for incoming connections from web browsers. Similarly, when a web browser is given a remote address (like grc.com or amazon.com), it assumes that a remote web server will be listening for connections on port80 at that location
135	tcp	msrpc	**Description :** Microsoft RPC services
139	tcp	netbios-ssn	**Description :** NETBIOS Session Service **Risk :** NetBIOS Session (TCP), Windows File and Printer Sharing **Solution :** It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port139 or
3306	tcp	mysql	**Description :** #mySQL
123	udp	ntp	**Description :** Network Time Protocol **Risk :** The network time protocol is a clean, simple, lightweight, and efficient protocol allowing clients to query servers for the current time (including the date) - (RFC2030, RFC1129) **Solution :** #An NTP (Network Time Protocol) server is listening on this port.It provides information about the current date and time of the remote system and may provide system information. (CVE-1999-0621)
137	udp	netbios-ns	**Description :** NETBIOS Name Service **Solution :** The remote host listens on udp port137 and replies to NetBIOS nbtscan requests. By sending a wildcard request it is possible to obtain the name of the remote system and the name of its domain.(CVE : CVE-1999-0621)
ipt_dos04		Microsoft Windows SMB PIPE Remote Denial of Service Vulnerability	**Description :** Microsoft Windows is prone to a remote denial-of-service vulnerability because the operating system fails to properly handle network traffic and the Server service fails to properly handle network messages. **Risk :** Impact of Vulnerability: Denial of Service and Remote Code Execution Microsoft Security Bulletin: MS06-063 **Solution :** Microsoft Security Update for Windows XP (KB923414) http://www.microsoft.com/downloads/details.aspx?familyid=08ab17b9-149c-44d4-96cf-87a8c6b9dc22&displaylang=en

About ISAG Penetration Test [IPT] Suite

ISAG Penetration Test Suite [IPT] version :: 1.0
xml output version :: 1.00
ipt.xsl version :: 1.0

BY ISAG LAB at Computer Engineering of KMITL, Thailand

รูปที่ 4.20 รายงานการทดสอบตัวเลือก Complete Mode ร่วมกับ All Plug-in with DoS (2)

บทที่ 5
บทวิจารณ์และสรุป

5.1) วิเคราะห์และสรุปผลการทดลอง

วิเคราะห์และสรุปผลการทดลอง

จากการทดลองแล้ว จะเห็นได้ว่า ตัวเลือกต่างๆของส่วนการสแกนนั้น สามารถใช้งานได้จริง ทั้งในส่วนของตัวเลือก Fast Mode, Aggressive Mode และ Complete Mode ขึ้นกับความต้องการทางด้านเวลาที่ใช้ในการสแกน และความแม่นยำในการสแกนของผู้ทำการทดสอบ รวมทั้งจะเห็นได้ว่าที่ปลายทางแทบระบุไม่ได้เลยว่ามีการโจมตีมาจากเครื่องใด โดยรู้เพียงว่ามีการโจมตีเข้ามาเท่านั้น และผลของการสแกนนั้นก็ได้ผลที่ถูกต้อง โดยถ้าการปรับแต่งค่าการป้องกันของระบบเป้าหมายไม่ดีพอ ชุดโปรแกรมทดสอบความปลอดภัยระบบคอมพิวเตอร์นี้ก็สามารถที่จะทำการสแกนเข้าไปได้ว่ามีพอร์ต/เซอร์วิส อะไรที่เปิดอยู่ และทำงานระบบปฏิบัติการอะไร เพื่อนำข้อมูลไปใช้ในการเอ็กซ์พลอยท์ต่อไป

ในส่วนของการเอ็กซ์พลอยท์ จะเห็นได้ว่า ตัวเลือกต่างๆนั้นสามารถทำงานได้จริง โดยสามารถทดสอบได้ว่า เครื่องเป้าหมายที่ทำงานบนระบบปฏิบัติการวินโดวส์เอ็กซ์พี เซอร์วิสแพ็ค 2 อาจถูกโจมตีที่ทำให้เครื่องเป้าหมายปฏิเสธการให้บริการ (Denial of Service Attack) ได้จริง และกรณีที่เครื่องเป้าหมายให้บริการ Apache ก็สามารถที่จะทดสอบได้ว่า เครื่องเป้าหมายนั้นอาจถูกเอ็กซ์พลอยท์ได้หรือไม่

ในส่วนของการวิเคราะห์การป้องกัน นั้นโปรแกรมสามารถทำการสร้างเอกสาร XML และแสดงเอกสาร XML ด้วย XSL ตามรูปแบบที่ได้ทำการออกแบบไว้ได้

5.2) ปัญหาอุปสรรค

ในระหว่างการทดสอบและพัฒนาชุดโปรแกรมทดสอบความปลอดภัยระบบคอมพิวเตอร์ได้ประสบปัญหาหลายประการ ซึ่งได้ทำการรวบรวมและสรุปเป็นข้อๆ โดยแบ่งออกเป็น 4 ส่วนตามโครงสร้างและการออกแบบชุดโปรแกรม ดังนี้

5.2.1 การสแกน (Scanner)

- ชุดโปรแกรมทำการสแกนระบบคอมพิวเตอร์ได้ยาก เมื่อมีการติดตั้งและตั้งค่าความปลอดภัยไฟร์วอลล์ หรือเครื่องมือที่ทำการป้องกันการสแกน ซึ่งมักขึ้นกับการตั้งค่าของผู้ดูแลระบบที่ทำการทดสอบนั้น

- ความไม่แน่นอนของการสแกน โดยเฉพาะอย่างยิ่งการสแกนด้วยยูดีพี ที่อาจจะช้ามาก หรืออาจจะเร็วขึ้นกับ สภาพของเครื่องเป้าหมาย และสภาพของเครือข่าย

5.2.2 การแสวงหาประโยชน์ (Exploitation)

- โค้ดเอ็กซ์พลอยท์ มีเพียงของระบบปฏิบัติการวินโดวส์เอ็กซ์พี เซอร์วิสแพ็ค 2 และแอปพลิเคชัน Apache เท่านั้น เนื่องจากเวลาที่จำกัด จึงระบุไปยังขอบเขตของโครงงาน และแอปพลิเคชันที่นิยมให้บริการทางอินเทอร์เน็ต

- การทดสอบโค้ดที่ใช้ในการทำเอ็กซ์พลอยท์ ในแต่ละการทดสอบโค้ดเหล่านั้น บางครั้งจำเป็นต้องตั้งเครื่องเป้าหมาย และเนื่องจากบางความไม่ชำนาญการในการติดตั้ง รวมถึงการไม่เข้าใจโค้ดอย่างละเอียด อาจส่งผลให้ไม่มีการนำเอ็กซ์พลอยท์ นั้นมาใช้งานโปรแกรม

- โค้ดที่ทำการเอ็กซ์พลอยท์ ในอินเทอร์เน็ตส่วนใหญ่มักนิยมใช้งานไลบรารีที่อ้างอิงกับระบบปฏิบัติการวินโดวส์ (winsock.h, window.h)

- ไม่สามารถนำโค้ดที่ใช้ในการทำคาดเดารหัสผ่าน, โค้ดที่ใช้ในการหาข้อมูลเกี่ยวกับ NetBIOS และโค้ดที่ใช้ในการดัมพ์ค่าเกี่ยวกับ Registry ของระบบปฏิบัติการวินโดวส์มาอิมพลีเมนต์ลงในโปรแกรมได้

5.2.3 การวิเคราะห์การป้องกัน (Prevention)

- ข้อมูลที่นำมาใช้ในการอ้างอิงนั้นค้นหามาจากอินเทอร์เน็ต เนื่องจากเวลาที่ใช้ในการพัฒนานั้นมีระยะเวลาที่จำกัด จึงทำให้ได้ข้อมูลที่อาจมีความละเอียดน้อยไปบ้าง หรืออาจไม่ทันสมัย

- การเขียนโค้ดเพื่อทำการติดต่อ XML ทำได้ค่อนข้างยาก เนื่องจากจำเป็นที่ต้องสร้าง object ในการนำข้อมูลออกจากเอกสาร XML

- การเขียนโค้ดส่วนการแสดงรายงานด้วย XSL นั้น ไม่สามารถสร้างรายงานที่ซับซ้อนได้มากกว่านี้เนื่องจากตัวภาษา XSL มีเพื่อใช้แสดงข้อมูล XML ไม่ได้มีไว้สำหรับการเขียนโปรแกรม

5.2.4 ภาพรวมของชุดโปรแกรม

- ชุดโปรแกรมทำการสแกนระบบคอมพิวเตอร์ได้อย่างประสิทธิภาพ เมื่อทำสแกนจากเครือข่ายภายในระบบเป้าหมาย (Local Area Network) เนื่องจากถ้าสแกนจากภายนอกอาจจะถูกขัดขวางจากอุปกรณ์ต่างๆ เช่น Switch, IPS, Firewall, และอื่นๆ

- ปัญหาเรื่องของส่วนต่อประสานกราฟิกกับผู้ใช้งาน ที่ทำการเขียนในระบบปฏิบัติการลินุกซ์ ทำให้ต้องศึกษาการเขียนส่วนนี้ใหม่ทั้งหมด รวมทั้งปัญหาเกี่ยวกับการทำงานแบบเทรด ที่เมื่อทำการเขียนเพื่อทำการสนับสนุนการทำงาน จะทำให้ชุดโปรแกรมไม่สามารถทำงานได้ตามปกติ

5.3 แนวทางในการพัฒนาและประยุกต์ใช้ร่วมกับงานอื่นๆ

5.3.1 ทำการวิเคราะห์ว่าผลของการสแกนพอร์ตนั้นมีแอปพลิเคชันใดที่ทำงานอยู่บนเครื่องเป้าหมาย เนื่องจากปัจจุบันนั้น แอปพลิเคชันนั้นมีการใช้งานหลายพอร์ต ซึ่งในส่วนนี้เราอาจจะทำการรวมกลุ่ม แล้วแสดงออกรายงานเป็นแอปพลิเคชันเดียว เพื่อลดความยุ่งยากในการวิเคราะห์ของผู้ใช้งาน

5.3.2 ทำการเก็บข้อมูลที่เกี่ยวข้องกับการเอ็กซ์พลอยท์ และการป้องกันปัญหาต่างๆในแต่ละเอ็กซ์พลอยท์ เพิ่มเติม

5.3.3 ชุดโปรแกรมสามารถทำการทดสอบระบบปฏิบัติการอื่นๆ ได้ดี เทียบเท่ากับการทดสอบกับระบบปฏิบัติการวินโดวส์เอ็กซ์พี และอาจจะมีการเพิ่มเติมในส่วนอุปกรณ์ embedded อื่นๆ เช่น พวกเครื่อง Printer เนื่องจากส่วนใหญ่อุปกรณ์ประเภทนี้มักไม่มีการรักษาความปลอดภัยในส่วนนี้

5.3.4 ชุดโปรแกรมสามารถปรับปรุงชุดโปรแกรมให้สามารถใช้งานเทรดได้

5.3.5 ชุดโปรแกรมสามารถทำการคาดเดารหัสผ่าน,หาข้อมูลเกี่ยวกับ NetBIOS และดัมพ์ค่าเกี่ยวกับ Registry ของระบบปฏิบัติการวินโดวส์ได้ เพื่อให้สามารถช่วยผู้ทำการทดสอบระบบคอมพิวเตอร์ ในการทดสอบตามรายการที่เตรียมไว้ (Check Lists) ที่มักเป็นมาตรฐานที่แตกต่างกันในการตรวจสอบของแต่ละองค์กร

5.3.6 ชุดโปรแกรมสามารถปรับปรุงโค้ดเอ็กซ์พลอยท์ที่ทันสมัยผ่านทางอินเทอร์เน็ตได้

5.3.7 ในอนาคตพัฒนาโปรแกรมให้สามารถทำงานผ่านทางเว็บได้ โดยอาจจะอนุญาตให้สามารถทำการทดสอบคอมพิวเตอร์ได้เฉพาะในส่วนของหมายเลขไอพี ของเครื่องที่ทำการติดต่อมาเท่านั้น เพื่อลดความยุ่งยากในการติดตั้งโปรแกรม

บรรณานุกรม

Douglas E. Comer, 2000. **Internetworking With TCP/IP Principles, Protocols, and Architecture Forth Edition.** New Jersey : Prentice Hall.

Joel Scambray and Sturat McClure, 2001. **Hacking Exposed: Network Security Secrets & Solution Second Edition**. New York : McGraw-Hill Companies.

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2007. **พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์** . [Online].

Available : http://www.etcommission.go.th/documents/laws/20070618_CC_Final.pdf

Vlad Alexa Mancini, 2002. **Nmap Security**. [Online].

Available : http://insecure.org/nmap/

Tenable Network Security, 2002. Inc. **Nessus**. [Online].

Available : http://www.nessus.org/

SecurityFocus Symantec Corporation, 2002. **SecurityFocus** . [Online].

Available : http://www.securityfocus.com/

ภาคผนวก ก
วิธีการใช้งานโปรแกรม Nmap

โปรแกรม Nmap (Network Mapper) เป็นเครื่องที่สำหรับการสำรวจเครือข่ายหรือตรวจสอบความปลอดภัยของเครือข่าย โดยสามารถใช้งานได้ฟรีและเปิดเผยซอร์สโค้ด (open source) อีกทั้งเป็นเครื่องมือที่มีประโยชน์ในหลายๆระบบในการทำระบบคงคลังเครือข่าย (network inventory) การบริหารตารางการปรับปรุงเซอร์วิส (managing service upgrade schedules) และการตรวจสอบเวลาการทำงานของโฮสต์ / เซอร์วิส

โปรแกรม Nmap ใช้แพ็คเก็ตไอพี ในแง่มุมใหม่ๆในการตัดสินว่าโฮสต์ใดเปิดใช้งานอยู่ในเครือข่าย เซอร์วิสใดเปิดให้บริการบนโฮสต์ โฮสต์ทำงานบนระบบปฏิบัติการอะไร แพ็คเก็ตฟิลเตอร์ริง /ไฟล์วอลล์เป็นชนิดใด และลักษณะเฉพาะอื่นๆ

โปรแกรม Nmap ถูกออกแบบให้ทำงานได้อย่างรวดเร็วกับเครือข่ายเป้าหมายขนาดใหญ่ แต่จะทำงานได้ดีเมื่อเป้าหมายเป็นเครื่องคอมพิวเตอร์เพียงเครื่องเดียว นอกจากนี้ Nmap สามารถทำงานได้ในทุกๆระบบปฏิบัติการและมีการใช้งานทั้งคอมมานไลน์ และส่วนต่อประสานกราฟิกกับผู้ใช้งาน(GUI)

คุณสมบัติของโปรแกรม Nmap

* Flexible: ความยืดหยุ่นในการรองรับเทคนิคใหม่ๆ เช่น การทำแผนที่เครือข่าย การตรวจสอบพอร์ตที่เปิดใช้งาน การตรวจสอบระบบปฏิบัติการ การตรวจสอบเวอร์ชัน เป็นต้น

* Powerful: โNmap ผ่านการทดสอบใช้งานกับเครือข่ายขนาดใหญ่

* Portable: รองรับระบบปฏิบัติการส่วนใหญ่ รวมถึง Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga เป็นต้น

* Easy: นอกจากมีตัวเลือกการทำงานสำหรับผู้ใช้ระดับสูง (power users) แล้ว Nmap ยังสามารถใช้งานได้ง่ายๆ เช่น nmap -v -A targethost และใช้งานได้ทั้งคอมมานไลน์และกราฟฟิค

* Free: Nmap สามารถดาวน์โหลด Nmap ใช้งานได้ฟรี พร้อมทั้งมีซอร์สโค้ดที่สามารถดัดแปลงแก้ไขได้ภายใต้เงื่อนไขลิขสิทธิ์

* Well Documented: Nmap มีเอกสารวิธีใช้งานที่เข้าใจได้ง่าย และหาอ่านได้หลายภาษา

* Supported: การทำงานของ Nmap ไม่ได้รับการรับประกันใดๆ แต่คุณสามารถสืบค้นวิธีแก้ไขข้อผิดพลาดได้จากเว็บไซต์ของเรา

ตัวอย่างเอกสารวิธีการใช้งานโปรแกรม Nmap

Nmap 4.20 (http://insecure.org)

Usage: Nmap [Scan Type(s)] [Options] {target specification}

TARGET SPECIFICATION:

Can pass hostnames, IP addresses, networks, etc.

Ex: scanme.Nmap.org, microsoft.com/24, I92.168.0.1; 10.0.0-255.1-254

-iL <inputfilename>: Input from list of hosts/networks

-iR <num hosts>: Choose random targets

--exclude <host1[,host2][,host3],...>: Exclude hosts/networks

--excludefile <exclude_file>: Exclude list from file

HOST DISCOVERY:

-sL: List Scan - simply list targets to scan

-sP: Ping Scan - go no further than determining if host is online

-P0: Treat all hosts as online -- skip host discovery

-PS/PA/PU [portlist]: TCP SYN/ACK or UDP discovery to given ports

-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes

-n/-R: Never do DNS resolution/Always resolve [default: sometimes]

--dns-servers <serv1[,serv2],...>: Specify custom DNS servers

--system-dns: Use OS's DNS resolver

SCAN TECHNIQUES:

-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans

-sU: UDP Scan

-sN/sF/sX: TCP Null, FIN, and Xmas scans

--scanflags <flags>: Customize TCP scan flags

-sI <zombie host[:probeport]>: Idlescan

-sO: IP protocol scan

-b <ftp relay host>: FTP bounce scan

PORT SPECIFICATION AND SCAN ORDER:

-p <port ranges>: Only scan specified ports

Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080

-F: Fast - Scan only the ports listed in the Nmap-services file)

-r: Scan ports consecutively - don't randomize

SERVICE/VERSION DETECTION:

-sV: Probe open ports to determine service/version info

--version-intensity <level>: Set from 0 (light) to 9 (try all probes)

--version-light: Limit to most likely probes (intensity 2)

--version-all: Try every single probe (intensity 9)

--version-trace: Show detailed version scan activity (for debugging)

OS DETECTION:

-O: Enable OS detection (try 2nd generation w/fallback to 1st)

-O2: Only use the new OS detection system (no fallback)

-O1: Only use the old (1st generation) OS detection system

--osscan-limit: Limit OS detection to promising targets

--osscan-guess: Guess OS more aggressively

TIMING AND PERFORMANCE:

Options which take <time> are in milliseconds, unless you append 's'
(seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).

-T[0-5]: Set timing template (higher is faster)

--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes

--min-parallelism/max-parallelism <time>: Probe parallelization

--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
probe round trip time.

--max-retries <tries>: Caps number of port scan probe retransmissions.

--host-timeout <time>: Give up on target after this long

--scan-delay/--max-scan-delay <time>: Adjust delay between probes

FIREWALL/IDS EVASION AND SPOOFING:

-f; --mtu <val>: fragment packets (optionally w/given MTU)

-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys

-S <IP_Address>: Spoof source address

-e <iface>: Use specified interface

-g/--source-port <portnum>: Use given port number

--data-length <num>: Append random data to sent packets

--ip-options <options>: Send packets with specified ip options

--ttl <val>: Set IP time-to-live field

--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address

--badsum: Send packets with a bogus TCP/UDP checksum

OUTPUT:

-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,

and Grepable format, respectively, to the given filename.

-oA <basename>: Output in the three major formats at once

-v: Increase verbosity level (use twice for more effect)

-d[level]: Set or increase debugging level (Up to 9 is meaningful)

--open: Only show open (or possibly open) ports

--packet-trace: Show all packets sent and received

--iflist: Print host interfaces and routes (for debugging)

--log-errors: Log errors/warnings to the normal-format output file

--append-output: Append to rather than clobber specified output files

--resume <filename>: Resume an aborted scan

--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML

--webxml: Reference stylesheet from Insecure.Org for more portable XML

--no-stylesheet: Prevent associating of XSL stylesheet w/XML output

MISC:

-6: Enable IPv6 scanning

-A: Enables OS detection and Version detection

--datadir <dirname>: Specify custom Nmap data file location

--send-eth/--send-ip: Send using raw ethernet frames or IP packets

--privileged: Assume that the user is fully privileged

--unprivileged: Assume the user lacks raw socket privileges

-V: Print version number

-h: Print this help summary page.

EXAMPLES:

Nmap -v -A scanme.Nmap.org

Nmap -v -sP 192.168.0.0/16 10.0.0.0/8

Nmap -v -iR 10000 -P0 -p 80

SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES

รายละเอียดของการใช้งานโปรแกรม Nmap

ในส่วนของการอธิบายการใช้งานตัวเลือกต่างๆของโปรแกรม Nmap เราจะทำการแบ่งออกตามลักษณะหมวดหมู่ดังต่อไปนี้

- การกำหนดเป้าหมาย (Target Specification)
- การค้นหาโฮสต์ (Host Discovery)
- พื้นฐานของการสแกนพอร์ต (Port Scanning Basics)
- เทคนิคของการสแกนพอร์ต (Port Scanning Techniques)
- การกำหนดพอร์ต และลักษณะในการสแกน (Port Specification and Scan Order)
- การตรวจสอบบริการและเวอร์ชัน (Service and Version Detection)
- การตรวจสอบระบบปฏิบัติการ (OS Detection)
- เวลาและประสิทธิภาพ (Timing and Performance)
- การหลบหลีกไฟร์วอลล์/IDS และการปลอมตัว (Firewall/IDS Evasion and Spoofing)
- การนำออก (Output)

การกำหนดเป้าหมาย (Target Specification)

-iL <inputfilename> (การรับข้อมูลขาเข้าจากไฟล์)

การสแกนผ่านโดยรับรายชื่อของโฮสต์ผ่านทาง inputfilename

--exclude <host1[,host2][,host3],...> (การยกเว้นการสแกนบางเครื่อง)

การยกเว้นเครื่องบางเครื่อง หรือบางเครือข่ายที่ไม่ต้องการสแกน

--excludefile <exclude_file> (การยกเว้นการสแกนบางเครื่องโดยดูจากไฟล์)

ตัวเลือกนี้จะมีลักษณะคล้ายกับตัวเลือก --exclude ต่างกันที่สามารถทำการยกเว้นจากไฟล์ที่กำหนดแทนที่จะใช้คอมมานไลน์

การค้นหาโฮสต์ (Host Discovery)

-sL (การสแกนแบบ List)

โดยปกติแล้ว Nmap จะทำการ reverse-DNS resolution บนเครื่องคอมพิวเตอร์ เพื่อที่ทำการเรียนรู้ชื่อเหล่านั้น ถ้าคุณต้องการที่จะไม่ใช้การสแกน ping เมื่อมีการทำงานที่ฟังก์ชันระดับสูง

(เช่น การสแกนพอร์ต, การตรวจสอบระบบปฏิบัติการ, หรือการสแกน Ping ซึ่งไม่สามารถทำงานร่วมกับการสแกนแบบ List ได้) ให้ใช้ตัวเลือก -P0

-sP (การสแกนด้วย Ping)

ทำการสแกนด้วยวิธีการสแกน Ping เท่านั้น โดยทำเพื่อการตอบสนองการสแกนไม่มีการทดสอบเกี่ยวกับการสแกนพอร์ต หรือการตรวจสอบระบบปฏิบัติการ โดยได้ผลมากกว่าการสแกนแบบ list (-sL)โดยการสแกนนี้มักถูกเรียกว่า *ping sweep*

ตัวเลือก -sP โดยปกติ มันจะทำการส่ง ICMP echo request และแพ็คเก็ตทีซีพีไปยังพอร์ต 80 ของเป้าหมายกรณีถูกประมวลโดยผู้ไม่มีสิทธิ เมื่อเป็นผู้ใช้ที่มีสิทธิแล้วพยายามสแกนเป้าหมายภายในเครือข่าย (Local Ethernet Network) จะเป็นการใช้ ARP request (-PR) จะถูกใช้ในการส่งไปยังไอพีที่กำหนด โดยตัวเลือกนี้ถูกผสมด้วยการทดสอบอื่นๆ (-P*, ยกเว้น -P0) ตามความต้องการ

-P0 (การไม่ใช้เทคนิคการ Ping)

ตัวเลือกนี้จะทำการข้ามขั้นตอนการค้นหา (Host Discovery) ของโปรแกรม Nmap โดยปกติแล้ว Nmap ใช้ในขั้นตอนของการกำหนดว่าเครื่องไหนทำงานอยู่ โดยการสแกนการทดสอบได้แก่การสแกนพอร์ต การตรวจสอบเวอร์ชัน หรือการตรวจสอบระบบปฏิบัติการ ไปยังโฮสต์ ซึ่งจะไม่มีทำการค้นหาโฮสต์ ทำได้ด้วย -P0 เนื่องจาก Nmap พยายามที่จะทำการสแกนร้องขอไปยังทุกไอพี ที่กำหนด ดังนั้นถ้าคลาส B นั้นเป้าหมายจะมีถึง 65536 ไอพี โดยทำการค้นหาโฮสต์ (host discovery) เหมือนการแสกนแบบ list แต่แทนที่ด้วยการหยุดและแสดงรายชื่อเป้าหมายออกมา ซึ่ง Nmap จะยังคงทำการร้องขอต่อไปประหนึ่งว่าเป้าหมายแต่ละเครื่องทำงานอยู่

-PS [portlist] (การสแกนด้วย TCP SYN Ping)

ทำการส่ง แพ็คเก็ตทีซีพีเปล่าที่มีการตั้งค่าแฟล็ก SYN โดยปกติจะส่งไปที่พอร์ต 80 (สามารถเปลี่ยนแปลงได้ที่ DEFAULT_TCP_PROBE_PORT ในไฟล์ Nmap.h) ปลายทางอาจถูกปิด และจะทำการส่งแพ็คเก็ต RST (reset) กลับมา ถ้าพอร์ตนั้นทำการเปิด เป้าหมายจะพยามที่จะทำ 3-way-handshake ใน ทีซีพี ด้วยการส่งแพ็คเก็ต SYN/ACK โฮสต์ทำการรันโปรแกรม Nmap จะมีการทำ tears down โดยการตอบกลับไปด้วยแพ็คเก็ต RST แทนที่จะทำการส่ง ACK เพื่อที่จะสร้างการติดต่อที่สมบูรณ์ -PA [portlist] (TCP ACK Ping)

TCP ACK ping นั้นจะเหมือนกับการใช้ SYN ping ต่างกันที่แฟล็ก ACK ของทีซีพีจะถูกตั้งค่าแทน การทำรีโมตโฮสต์ (remote host) ควรที่จะมีการตอบด้วยแพ็คเก็ต RST ตลอดเวลา ซึ่งจะเป็นการเปิดเผยที่โปรเซสดำเนินการอยู่ โดยปกติจะส่งไปที่พอร์ต 80 เหมือนกับการทดสอบ SYN

เหตุผลของการทดสอบด้วย SYN และ ACK Ping เพื่อที่จะเพิ่มโอกาสในการผ่านไฟร์วอลล์เข้าไป ซึ่งหลายๆครั้งที่มีการปรับแต่งอุปกรณ์จัดเส้นทาง (router) และไฟล์วอลล์ อื่นๆเพื่อที่ป้องกันการเข้ามาของแพ็คเก็ต SYN ในกรณีที่มีการทดสอบด้วย ACK ก็อาจจะผ่านกฎเหล่านั้นได้ตามกฎได้ ซึ่งในขณะที่แพ็คเก็ต ACK ที่ถูกสร้างขึ้นนั้นอาจถูกวิเคราะห์ว่ามีการปลอม และอาจถูกดรอป (drop) ทางแก้ไขที่มีดี นั้นคือการส่งพิสูจน์โดยทั้ง SYN และ ACK โดยการกำหนด -PS และ -PA.

-PU [portlist] (UDP Ping)

ทำการส่งแพ็คเก็ตยูดีพีเปล่า ไปยังพอร์ตที่กำหนด โดยปกติพอร์ตจะมีค่าเป็น 31338 เนื่องจากเป็น พอร์ต ที่ไม่ค่อยมีบริการเรียกใช้งาน (DEFAULT_UDP_PROBE_PORT ใน Nmap.h) ผลดีของการสแกนประเภทนี้ คือมันจะทำการทะลุผ่านไฟล์วอลล์ (bypasses firewalls) และกรองที่ทีซีพีเท่านั้น

-PE; -PP; -PM (การทดสอบค้นหาโฮร์ตแบบ ICMP echo, timestamp, และ netmask request)

นอกจากการค้นหาโฮสต์ด้วยวิธีทีซีพี และยูดีพีก่อนหน้านี้แล้วโปรแกรม Nmap สามารถส่งแพ็คเก็ตมาตรฐานอื่นๆได้อีกด้วย ได้แก่ การใช้งาน ICMP ด้วยการ ping โปรแกรม Nmap จะทำการส่งแพ็คเก็ตICMP type 8 (echo request) ไปยังเป้าหมาย ซึ่งจะคาดหวัง type 0 (Echo Reply) ที่ได้จากการตอบรับจากโฮสต์ที่มีอยู่ แต่ส่วนใหญ่แล้วเครือข่ายที่ได้ทำการสำรวจที่มีโฮร์ตจำนวนมากและไฟร์วอลล์ (firewall) มักจะทำการหยุดแพ็คเก็ตเหล่านั้น มากกว่าการตอบสนองตามที่ได้ระบุใน RFC 1122 ซึ่งทำให้การสแกน ICMP-อย่างเดียวนั้นไม่น่าเชื่อถือเพียงพอสำหรับเป้าหมายที่ไม่รู้จักบนอินเทอร์เน็ตแต่สำหรับผู้ดูแลระบบ นั้นเพียงพอต่อการทดสอบเครือข่ายภายใน (ตัวเลือก -PE จะมีใช้ echo request)

ส่วนการใช้งาน Timestamp และ address mask queries สามารถทำได้ด้วยการใช้งานตัวเลือก –PP และ -PM ตามลำดับ โดย timestamp reply (ICMP code 14) หรือ address mask reply (code 18) จะเปิดเผย โฮสต์ที่หามาได้ โดยการร้องขอทั้งสองนั้น มีประโยชน์เมื่อผู้ดูแลทำการป้องกันแพ็คเก็ต echo request แต่ลืมที่จะทำการป้องกันแพ็คเก็ตอื่นๆของ ICMP queries ที่ใช้สำหรับเป้าหมายเดียวกันได้

-PR (ARP Ping)

การสแกนโดยใช้งาน ARP นี้เร็วและน่าเชื่อถือกว่าการสแกนที่มีพื้นฐานบนไอพี สำหรับเป้าหมายที่อยู่ภายในเครือข่ายภายใน (local Ethernet network) ถ้าคุณไม่ต้องการสแกน ARP ให้

กำหนด --send-ip (ปกติแล้วเป็นค่าเริ่มต้นของการสแกนเป้าหมายที่อยู่ภายในเครือข่าย -- local Ethernet network)

--traceroute (การตามรอยเส้นทางไปยังโฮร์ต)

โปรแกรม Nmap จะทำงานร่วมกับการสแกนหลายๆประเภทยกเว้น –sT และ –sI โดยจะมีการทำงานในแบบคู่ขนาน (parallel) โดยปกติแล้ว traceroute จะเริ่มจากการส่งแพ็คเก็ตด้วยค่า TTL (time-to-live) = 1 แล้วค่อยๆเพิ่มที่ละ 1 จนถึงปลายทาง

แต่โปรแกรม Nmap นั้นใช้ขั้นตอนวิธี (algorithm) ในการทำ traceroute แบบการย้อนกลับทำการเพิ่มความเร็วของการตามรอยข้ามไปยังหลายๆ โฮสต์ ซึ่งจะมีการส่ง 5-10 แพ็คเก็ต/โฮสต์ ขึ้นกับสภาพของเครือข่าย โดยการแสดงผลนั้นจะมีการรวบกลุ่มแบ่งออกเป็น 2 แบบ คือ timed out และ reference trace (ใช้ได้เฉพาะระบบปฏิบัติการ Linux เท่านั้น)

-n (ไม่ทำการแปลงชื่อโฮร์ตด้วย DNS)

ตั้งค่าโปรแกรม Nmap ให้ไม่มีการทำการแปลงชื่อโฮร์ตด้วย DNS ย้อนกลับ (reverse DNS resolution) ของหมายเลขไอ ที่ได้พบว่าทำงานอยู่ โดยตัวเลือกนี้สามารถลดเวลาของการสแกนได้ (เป็นค่าเริ่มต้น)

-R (ทำการแปลงชื่อโฮร์ตด้วย DNS สำหรับเป้าหมายทั้งหมด)

เพื่อที่จะทำการแปลงชื่อโฮร์ตด้วย DNS ย้อนกลับ (reverse DNS resolution) อย่างตลอด โดยปกติแล้วโปรแกรมจะทำเฉพาะการตอบสนองของโฮสต์ที่กำลังทำงานบนเครือข่าย

--system-dns

ส่วนใหญ่ถูกใช้ในการสแกนไอพีเวอร์ชัน 6 ใช้ในการแปลงหมายเลขไอพี(ไม่จำเป็น)

--dns-servers

กำหนดผู้ให้บริการ DNS ที่น่าเชื่อในการสแกน โดยจะเป็นการเพิ่มประสิทธิภาพเมื่อคุณได้ทำการเลือกผู้ให้บริการที่น่าเชื่อถือได้ (authoritative servers) จะสามารถส่งเสริมการทำตัวเลือกการแอบทำอย่างลับๆ (stealth) โดยใช้งานได้สะดวกเมื่อทำการสแกนเครือข่ายส่วนตัว (private network)

พื้นฐานของการสแกนพอร์ต (Port Scanning Basics)

สถานะของพอร์ตทีทำการสแกนทั้งหมดที่ถูกโปรแกรม Nmap ทำการวิเคราะห์จะแบ่งออกเป็น 6ลักษณะ ดังต่อไปนี้

open

แอปพลิเคชันที่ทำงานอยู่ (active) ที่ได้ยอมรับการติดต่อแพ็คเก็ตทีซีพี หรือยูดีพีบนพอร์ตนี้

closed

พอร์ตที่ถูกปิดสามารถที่เข้ามา (รับและตอบสนองต่อแพ็คเก็ตที่ Nmap ใช้ในการทดลอง) ซึ่งใช้ในการระบุว่า โฮสต์ นั้นทำงานด้วยหมายเลขไอพีไหม (การค้นหาโฮร์ตที่เปิด, หรือการสแกนด้วย ping) และเป็นส่วนหนึ่งของการตรวจสอบระบบปฏิบัติการ เนื่องจากพอร์ตที่ถูกปิดนั้นสามารถเข้าถึงได้

filtered

โปรแกรม Nmap ไม่สามารถกำหนดได้ว่าพอร์ตนั้นเปิด เนื่องจากมีการกรองแพ็คเก็ตป้องกันการทดสอบจากการเข้าถึงพอร์ต การกรองสามารถทำจากอุปกรณ์ไฟร์วอลล์ กฎของอุปกรณ์จัดเส้นทาง (router) หรือซอฟต์แวร์ไฟร์วอลล์ที่อยู่บนโฮสต์ (host-based firewall software) พอร์ตเหล่านั้นทำให้ผู้บุกรุกไม่สมหวัง เนื่องจากพวกเข้าได้ข้อมูลเพียงน้อยนิด บางครั้งมันจะทำการตอบด้วย ICMP error message ได้แก่ ประเภท 3 โค้ด 13 (destination unreachable: ซึ่งเป็นการติดต่อที่ถูกห้ามโดยผู้ดูแลระบบ) ซึ่งมักจะถูกกรอง ในกรณีของการทดสอบมักถูกยกเลิกการตรวจสอบ เนื่องจากความคับคั่งของเครือข่าย มากกว่าการกรอง ซึ่งทำให้ความเร็วของการสแกนลดลง

unfiltered

พอร์ตที่สามารถทำการเข้าถึงได้ แต่โปรแกรม Nmap ไม่สามารถระบุได้ว่ามันเปิดหรือปิด การสแกนด้วย ACK เท่านั้นที่ถูกใช้ในการตรวจสอบกลุ่มของกฎไฟร์วอลล์ (firewall rulesets) การจัดกลุ่มของพอร์ต (classifies ports) ที่เกี่ยวกับสถานะนี้ โดยการสแกนที่ไม่ได้รับการกรองจากการสแกนประเภทต่างๆ ได้แก่ การสแกนด้วยเทคนิค Window, การสแกนด้วยเทคนิค SYN, หรือการสแกนด้วยเทคนิค FIN ที่อาจจะช่วยแก้ไขปัญหาให้ได้ว่า พอร์ตใดทำการเปิดบ้าง

open|filtered

สถานะนี้ถูกใช้เมื่อโปรแกรม Nmap ไม่สามารถกำหนดว่า พอร์ตนั้นถูกเปิดหรือถูกกรอง เกิดในกรณีของการสแกนในกรณีที่ พอร์ตที่ทำการตรวจสอบไม่มีการตอบสนองจากการสแกนด้วยเทคนิค UDP, IP Protocol, FIN, Null, และ Xmas

closed|filtered

สถานะนี้ถูกใช้เมื่อโปรแกรม Nmap ไม่สามารถกำหนดว่า พอร์ตนั้นถูกปิดหรือถูกกรองจะเกิดในกรณีของการสแกน IPID Idle เท่านั้น

เทคนิคของการสแกนพอร์ต (Port Scanning Techniques)

-sS (การสแกนแบบ TCP SYN)

การสแกน SYN เป็นค่าปกติ และเป็นที่นิยมเนื่องจากสามารถทำการสแกนได้รวดเร็วเป็นพันพอร์ตต่อวินาทีบนเครือข่ายความเร็วสูงที่ไม่ถูกขัดขวางโดยไฟร์วอลล์

โดยเทคนิคนี้บ่อยครั้งที่ได้อ้างอิงถึงการสแกนแบบ Half-open เนื่องจากโปรแกรมไม่ได้ทำการเปิดการเชื่อมต่อทีซีพีแบบเต็มรูปแบบ โปรแกรมจะทำการส่งแพ็คเก็ต SYN แล้วรอการตอบสนองของ SYN/ACK ที่บอกว่า พอร์ตนั้นกำลังรอรับฟัง (listening (open)), หลังจากนั้นทำการตอบด้วยแพ็คเก็ต RST (reset) ถ้าไม่มีการตอบสนองหลังจากมีการ retransmission แล้วพอร์ตนั้นจะถูกกำหนดว่า พอร์ตถูกกรอง และพอร์ตจะถูกกำหนด ว่ากรองแล้ว ถ้า ICMP นั้น unreachable error (type 3, code 1,2, 3, 9, 10, หรือ 13) ที่ได้รับ

-sT (การสแกนแบบ TCP connect)

การสแกน TCP connect เป็นค่าเริ่มต้นของประเภทการสแกนทีซีพี เมื่อไม่มีการสแกนด้วยตัวเลือก SYN (-sS) ซึ่งการสแกน TCP connect เป็นเทคนิคการสแกนแบบพื้นฐานและง่ายที่สุด คือจะใช้ connect system call ของระบบปฏิบัติการไปบนระบบเป้าหมายเพื่อเปิดการเชื่อมต่อไปยังทุก ๆ พอร์ตที่เปิดอยู่ การ scan ชนิดนี้สามารถจับได้ง่ายมาก โดยล็อก (log) ต่าง ๆ ของระบบที่เป็นเป้าหมายจะแสดงการร้องขอการเชื่อมต่อ (connection requests) และข้อความแสดงข้อผิดพลาด (error messages) สำหรับบริการที่ตอบรับการเชื่อมต่อนั้น แต่การสแกนด้วย TCP connect( ) นั้นมักได้รายละเอียดที่มากกว่าการสแกน SYN เนื่องจาก Nmap มีการควบคุม high level connect() call น้อยกว่าแพ็คเก็ตใหม่ ทำให้ประสิทธิภาพของมันลดลง system call ของการติดต่ออย่างสมบูรณ์ในการเปิดพอร์ตเป้าหมายมากกว่าการทำ half-open reset ที่การสแกน SYN ทำ IDS นั้นพอที่จะจับทั้งสองแต่เครื่องส่วนมากไม่มีระบบเตือน

-sU (การสแกนแบบยูดีพี)

บริการส่วนมากนิยมทำงานบนโพรโตคอลทีซีพี แต่บริการยูดีพี ก็ยังมีการใช้งานอย่างแพร่หลายเช่น DNS, SNMP และ DHCP เป็น 3 บริการที่นิยมใช้มาก โดยในการสแกนยูดีพี นั้นทำได้ช้า และยากกว่าทีซีพี ซึ่งทางผู้ตรวจสอบความปลอดภัยอาจละทิ้งพอร์ตเหล่านั้น ก่อให้เกิดความผิดพลาด หรืออาจโดนเอ็กซ์พลอยท์ (Exploit) บริการยูดีพีได้

การสแกนยูดีพี สามารถทำงานร่วมกับการสแกนประเภททีซีพี ได้เช่นการแสกน SYN (-sS) เพื่อที่จะทำการตรวจสอบโพรโตคอลทั้งคู่ระหว่างการทำงาน โดยการสแกนยูดีพี จะทำการส่งแพ็คเก็ตยูดีพีเปล่า ไปยังทุกๆ พอร์ต ที่เป็นเป้าหมาย ถ้า ICMP port unreachable error (type 3, code 3) ถูกส่งกลับมา ซึ่งพอร์ตนั้นถูกปิดและ ICMP อื่นๆที่เกิดจากความผิดพลาด unreachable (type 3, codes 1, 2, 9, 10, หรือ 13) จะทำให้พอร์ตถูกกำหนดให้เป็นการกรอง แต่ถ้าตอบด้วยแพ็คเก็ตยูดีพีแสดงว่า พอร์ตเปิด ถ้าไม่มีการตอบกลับมาจะมีการ retransmissions ซึ่งจะถูกจัดออกเป็น open|filtered

โฮสต์ส่วนมากแล้วมีการกำหนด ICMP port unreachable messages ตามค่าปกติ โดย Linux และ Solaris มีความเข้มงวดในส่วนนี้มาก เช่น Linux 2.4.20 kernel จำกัด destination unreachable *messages* 1 ครั้งต่อ *second* (ใน *net/ipv4/icmp.c*) ซึ่งโปรแกรม Nmap มีการจำกัดอัตราการสแกนเพื่อหลีกเลี่ยงการล้นของแพ็คเก็ตที่ไม่มีประโยชน์ในการสแกน และหลีกเลี่ยงการตรวจจับ ซึ่งการสแกนจากหลังไฟร์วอลล์ให้ใช้ --host-timeout เพื่อที่จะข้ามโฮสต์ที่ช้าออกไป (ไม่น่าเชื่อถือ)

-sN; -sF; -sX (การสแกนแบบ TCP Null, FIN, และ Xmas)

การสแกน 3 ประเภทนี้ (ตัวเลือก--scanflags จะมีการอ้างอิงในส่วนถัดไป) จะทำการเอ็กซ์พลอยท์ (Exploit) ช่องโหว่ที่บอบบางในทีซีพี RFC ที่ถึงความแตกต่างระหว่างพอร์ตที่เปิด และปิด ในหน้าถัดไปจะกล่าวถึงการส่งแพ็คเก็ตไปยังพอร์ตที่เปิด โดยไม่มีการตั้งค่าบิต SYN, RST, หรือ ACK

เมื่อสแกนระบบทำตาม RFC นี้แล้ว แพ็คเก็ตที่ไม่มีการบรรจุบิต SYN, RST, หรือ ACK จะได้ผลลัพธ์ให้มีการ RST ตอบกลับมา ถ้าพอร์ตนั้นปิด และไม่มีการตอบสนอง ถ้าพอร์ตนั้นทำการเปิด ตราบเท่าที่ไม่มีบิตทั้งสามเป็นส่วนประกอบแล้ว ไปรวมกับส่วนอื่นๆอีก3อย่าง (FIN, PSH, และ URG) จะถือว่ายอมรับได้

Null scan (-sN)	ไม่มีการตั้งค่าบิตใดๆ (แฟล็กเฮดเดอร์ของทีซีพีเป็น 0)
FIN scan (-sF)	ตั้งค่าบิต FIN ของทีซีพี
Xmas scan (-sX)	ตั้งค่าแฟล็ก FIN PSH และ URG

การสแกนทั้งสามแบบนั้นมีพฤติกรรมอย่างชัดเจน ยกเว้นการตั้งค่าแฟล็กทีซีพี ในแพ็คเก็ตที่ทำการทดสอบ ถ้าได้รับการตอบด้วยแพ็คเก็ต RST พอร์ตนั้นจะถูกกำหนดว่า closed เมื่อไม่มีการตอบสนองหมายความว่าพอร์ต open|filtered ที่ถูกระบุว่า filtered เมื่อได้รับ ICMP unreachable error (type 3, code 1, 2, 3, 9, 10 หรือ 13)

การสแกนนี้สามารถผ่าน non-stateful firewalls และการกรองแพ็คเก็ตของอุปกรณ์จัดเส้นทาง (router) แต่มีการ stealthy ได้น้อยกว่าการสแกน SYN โดยอย่าวางใจกับพวก modern IDS ที่สามารถปรับแต่งให้พบพวกมันได้ จำนวนระบบที่ได้รับการตอบสนองด้วย RST เพื่อที่จะทำการทดสอบโดยไม่คำนึงพอร์ตว่าเปิดหรือไม่ สาเหตุนี้ทำให้พอร์ตทั้งหมดถูกระบุว่าปิด ซึ่งระบบปฏิบัติการพวก Microsoft Windows, อุปกรณ์ Cisco อื่นๆ, BSDI, และ IBM OS/400 จะทำมัน การสแกนนี้จะไม่สามารถทำงานได้กับพวก UNIX-based systems โดยทั่วไป

-sA (การสแกนแบบ TCP ACK)

เทคนิคที่ใช้ค้นหาเครื่องที่ทำงานอยู่ แต่ปฏิเสธการตอบสนองต่อ ICMP ping หรือตรวจสอบกลุ่มกฎ (rulesets) หรือนโยบาย (policy) ต่าง ๆ ที่ตั้งไว้ที่ไฟล์วอลล์เพื่อตรวจสอบดูว่าไฟล์วอลล์สามารถกรอง แพ็คเก็ต อย่างง่าย ๆ หรือเทคนิคชั้นสูง โดยการสแกนแบบนี้จะใช้แพ็คเก็ตทีซีพี ที่มีแฟล็กเป็น ACK ส่งไปยังพอร์ตเครื่องปลายทาง ถ้าพอร์ตเปิดอยู่ เครื่องเป้าหมายจะส่ง RST กลับมา แต่ถ้าปิดอยู่ก็จะไม่สนใจแพ็คเก็ตนั้น ซึ่งการสแกนนี้ต่างจากการสแกนอื่นๆที่กล่าวมามันจะไม่มีการกำหนดพอร์ตว่า open (หรือ open|filtered)

การสแกนนี้จะเป็นการทดสอบโดยการตั้งค่าแฟล็ก ACK เท่านั้น (นอกจากคุณจะใช้ --scanflags). เมื่อทำการสแกนระบบที่ไม่มีการกรอง ซึ่งทั้งพอร์ตที่เปิดและปิดจะมีการแพ็คเก็ต RST คืนกลับมา เพื่อที่จะบอกว่า unfiltered หมายถึงว่าพวกมันได้ทำการค้นหาได้ โดยการส่งแพ็คเก็ต ACK แต่ไม่ว่าพวกมันเป็น open หรือ closed มันจะไม่ถูกกำหนด พอร์ตที่ไม่มีการตอบสนอง หรือการส่ง ICMP error messages (type 3, code 1, 2, 3, 9, 10, or 13) กลับมาจะถูกระบุว่าเป็น filtered

-sW (การสแกนแบบ TCP Window)

Window scan คล้ายการแสกนด้วยการตั้งค่าแฟล็ก ACK (-sA) ยกเว้นว่าจะมีการเอ็กซ์พลอยท์ (exploits) รายละเอียดของการอิมพลีเมนต์ (implementation) ระบบของความแตกต่างของพอร์ตที่เปิดและพอร์ต ที่ปิด มากกว่าการแสดง unfiltered เมื่อได้รับการคืนค่ากลับมา โปรแกรมจะทำโดยการทดสอบฟิลด์ Window ของทีซีพี แพ็คเก็ต RST ที่ถูกคืนค่ากลับมา ในบางระบบที่เปิดพอร์ตจะใช้ขนาดของ window เป็นค่าบวก เมื่อเป้าหมายจะได้ทำการกรอง หลังจากนั้นโปรแกรม

จะได้รับแพ็คเก็ต RST กลับ ซึ่งการสแกน Window รายชื่อของพอร์ตที่เปิดหรือถูกปิด ถ้าค่าของ Window ที่ทำการตั้งค่าใหม่เป็น ค่าบวก หรือ ศูนย์

การตอบการสแกนนี้เป็นการบอกรายละเอียดของส่วนน้อยของระบบที่อยู่บน Internet ดังนั้นคุณไม่สามารถเชื่อใจทันได้ ระบบที่ไม่สนับสนุนมันจะถูกคืนค่ากลับมาว่าเป็น closed ทั้งหมด ซึ่งเป็นธรรมดาที่มันที่อาจจะเป็นไปได้ที่เครื่องนั้นไม่ทำการเปิดพอร์ต ถ้าพอร์ตที่ถูกสแกนนั้นปิด พอร์ตโดยทั่วไป เช่น พอร์ต 22, 25, 53 นั้นมักเป็นสถานะ filtered บางครั้งที่ระบบจะทำการแสดงพฤติกรรมที่ตรงข้าม ถ้าการสแกนของคุณแสดง 1000 พอร์ต ที่เปิด และ 3 พอร์ต ที่ปิด หรือถูกกรองนั้นก็มีโอกาสเป็นไปได้

-sM (การสแกนแบบ TCP Maimon)

การสแกนแบบ Maimon เป็นชื่อที่เกิดจากคนค้นพบ Uriel Maimon ซึ่งอธิบายเทคนิคใน Phrack Magazine issue #49 (November 1996). ใน 2 ฉบับต่อมาเค้าเอาเทคนิคที่อธิบายในฉบับแรกมารวมไว้ใน Nmap เทคนิคนี้เหมือนกับการสแกน Null, FIN, และ Xmas ยกเว้นการทดสอบด้วย FIN/ACK ตามที่ RFC 793 แพ็คเก็ตทีซีพี RST ถูกผลิตเพื่อตอบสนองการทดสอบว่า พอร์ต นั้นเปิดหรือปิดอยู่ อย่างไรตาม Uriel สังเกตว่าระบบ BSD-derived จะยกเลิกแพ็คเก็ต ถ้าพอร์ตนั้นเปิดอยู่

--scanflags (การสแกนแบบที่สามารถปรับแต่งแฟล็กทีซีพี)

ในความจริงแล้วพวกผู้ใช้งานในระดับผู้มีประสบการณ์ นั้นไม่ควรจำกัดความสามารถในการใช้งาน โดยการใช้ตัวเลือก –scanflag นั้นจะยอมให้คุณทำการออกแบบการสแกนของคุณโดยการกำหนดอย่างอิสระ เพื่อที่จะทำการสแกนผ่านระบบการตรวจจับ เนื่องจากส่วนใหญ่แล้วผู้จำหน่ายระบบการตรวจจับจะทำการออกกฎครอบคลุมการใช้งานของ Nmap

--scanflags อาร์กิวเมนต์ สามารถกำหนดเป็นค่าของตัวเลข เช่น 9(PSH และ FIN), แต่การใช้ชื่อที่เป็นสัญลักษณ์ (symbolic names) นั้นเป็นรูปแบบที่ใช้งานง่ายกว่า โดยอาจจะรวมของแฟล็กต่างๆได้แก่ URG, ACK, PSH, RST, SYN, และ FIN เช่น --scanflags URGACKPSHRSTSYNFIN เป็นการตั้งค่าแฟล็กทุกๆอย่าง แต่อาจจะไม่เป็นประโยชน์ในการสแกน และเป็นการดั้งค่าที่ไม่สัมพันธ์กับความเป็นจริง

นอกจากนี้การกำหนดแฟล็กสามารถกำหนดร่วมกับการสแกนทีซีพีได้ (เช่น –sA หรือ -sF) ซึ่งปกติแล้ว Nmap จะมีพื้นฐานของการรอการตอบสนองตามประเภทของการสแกนต่างๆ เช่น SYN scan จะพิจารณาว่าถ้าไม่มีการตอบสนองจะถูกระบุว่าเป็นพอร์ต filtered ในขณะที่การสแกน FIN เมื่อกรณีเดียวกันจะระบุเป็น open|filtered โดยถ้าคุณไม่กำหนดประเภทพื้นฐานของการสแกน SYN จะถูกใช้เป็นพื้นฐานของการสแกน

-sI <zombie host[:probeport]>

http://insecure.org/Nmap/idlescan.html.

-sO (การสแกนแบบใช้โพรโตคอลไอพี)

การสแกนด้วยโพรโตคอลไอพี จะยอมให้คุณทำการระบุโพรโตคอลทีซีพี, ICMP, IGMP และอื่นๆ ที่ใช้ในการสแกนเป้าหมาย ตัวเลือกนี้ไม่ใช่เทคนิคของการสแกน แต่เป็นระบุผ่านทางหมายเลขโพรโตคอล ไอพี มากกว่าหมายเลขทีซีพี หรือ ยูดีพี มันยังคงที่จะใช่งานตัวเลือก -p ในการเลือกหมายเลขโพรโตคอล ที่ใช้ในการสแกน ซึ่งรายงานผลลัพธ์ของพวกมันจะอยู่ในรูปแบบของตารางพอร์ตทั่วไป และทำให้การใช้งานได้ประโยชน์ในการสแกนพอร์ต

-b <ftp relay host> (การสแกนแบบ FTP bounce)

ยอมให้ผู้ใช้งานเพื่อทำการติดต่อกับผู้ให้บริการ FTP เมื่อได้ทำการถามถึงไฟล์เพื่อส่งไปยังผู้ให้บริการอื่นๆ เช่น คุณสมบัติในการ ripe ที่ใช้ในทางที่ไม่ดี ซึ่งส่วนมากแล้ว server จะสนับสนุนมัน โดยการถามปกติแล้ว FTP server จะทำการส่งไฟล์ไปยังแต่ละ port ที่สนใจ ซึ่งข้อความแจ้งความปิดจะเป็นการอ้างอิงว่า พอร์ต ได้ทำการเปิด หรือไม่ วิธีนี้เป็นทางที่ดีสำหรับการทะลุผ่านไฟร์วอลล์ (bypass firewall) เนื่องจาก FTP server ขององค์กรมักจะถูกเข้าถึงจากเครื่องภายใน มากกว่าทาง internet

ftp bounce scan จะมีอาร์กิวเมนต์ในรูปของ *username:password@server:port.* โดย server นั้นเป็นชื่อ หรือหมายเลขไอพี ของ FTP server ที่อ่อนแอ โดยปกติแล้วจะเป็น URL ซึ่งคุณอาจจะลืม *username:password* ในกรณีที่เป็น anonymous login (user: anonymous password:-wwwuser@) หมายเลขพอร์ต (และเงื่อนไขก่อนหน้าเครื่องหมายโคลอน) อาจจะถูกละเลยได้ ในกรณีที่เป็นผู้ให้บริการ (server) ใช้พอร์ตปกติ FTP (21)

ความอ่อนแอนั้นถูกแพร่หลายใน1997 เมื่อโปรแกรม Nmap ได้ทำการปล่อยตัวเลือกนี้ออกมา แต่ก็ขยายในวงจำกัด ผู้ให้บริการที่มีความอ่อนแอนั้นยังคงมีอยู่ ถ้าไม่การทำทะลุผ่านไฟร์วอลล์ (bypassing firewall) ก็สามารถไปสู่เป้าหมายได้ ซึ่งการสแกนเครือข่ายที่เปิดพอร์ต 21 (หรือ ftp services ต่างๆ ถ้าคุณได้ทำการสแกนทุกพอร์ตด้วยการตรวจสอบเวอร์ชัน --version detection) เมื่อใช้การสแกน bounce แต่ละพอร์ต แล้ว Nmap จะแสดงให้เห็นว่า โฮร์ต นั้นมีช่องโหว่หรือไม่

การกำหนดพอร์ต และลักษณะในการสแกน (Port Specification and Scan Order)

-p <port ranges> (กำหนดพอร์ตที่ใช้ในการสแกน)

ตัวเลือกเป็นการกำหนดพอร์ตที่ต้องการสแกน และเขียนทับค่าปกติเมื่อกำหนดหมายเลขพอร์ตซึ่งจะมีการแยกด้วยเครื่องหมายไฮเฟน - hyphen (ตัวอย่างเช่น 1-1023) การเริ่มต้นและหรือจุดสิ้นสุดของช่วงอาจจะถูกละเว้น เนื่องจากโปรแกรม Nmap ใช้ 1 และ 65535 ตามลำดับ

คุณสามารถกำหนดโพรโตคอล เฉพาะโดยเงื่อนไขของหมายเลขพอร์ต (TCP / UDP) ก่อนหน้านี้ว่าเป็น T หรือ U คุณสมบัติหลังสุดจนกระทั่งคุณได้กำหนดคุณสมบัติอื่น เช่น อาร์กิวเมนต์ -p U:53,111,137,T:21-25,80,139,8080

-F (การสแกนแบเร็ว – จำกัดจำนวนพอร์ตที่ใช้ในการสแกน)

การสแกนรายชื่อของพอร์ตในไฟล์ Nmap-services ซึ่งใช้งานกับโปรแกรม (หรือโพรโตคอลไฟล์สำหรับ -sO) มีความเร็วกว่าการสแกนพอร์ตทั้ง 65535 ของโฮร์ต เนื่องจากรายชื่อนี้ประกอบด้วยพอร์ตทีซีพี(มากกว่า 1200) ซึ่งมีความเร็วแตกต่างจากการสแกนทีซีพีปกติ (ประมาณ 1650 พอร์ต) ความแตกต่างนี้สามารถทำให้เกิดผลอย่างมากมาย ถ้าคุณได้กำหนดไฟล์ Nmap-services ของคุณเองโดยการใช้ตัวเลือก --datadir

-r (ไม่ทำการสุ่มค่าพอร์ตของการสแกน)

กำหนด -r เพื่อทำการสแกนตามลำดับแทน (ปกติทำการสแกนด้วยการสุ่ม)

การตรวจสอบบริการและเวอร์ชัน (Service and Version Detection)

-sV (การตรวจสอบเวอร์ชัน)

อีกทางเลือกหนึ่ง คือ -A เพื่อที่ใช้งานการตรวจสอบระบบปฏิบัติการ และเวอร์ชัน

--allports (ทำการตรวจสอบเวอร์ชันจากทุกๆพอร์ต)

โดยปกติแล้วโปรแกรม Nmap จะทำการตรวจจับเวอร์ชันผ่านทางพอร์ตทีซีพี 9100 เนื่องจากเครื่องพิมพ์บางเครื่อง ทำการส่งข้อมูลต่างๆทางพอร์ตนี้ ซึ่งจะนำไปสู่หน้าของ HTTP get requests, binary SSL session requests และอื่นๆ พฤติกรรมนี้นำไปสู่การเปลี่ยนแปลง หรือคุณสามารถกำหนด --allports เพื่อที่จะทำการสแกนโดยไม่สนใจ Exclude directive

--version-intensity <intensity> (การตั้งค่าความรุนแรงการสแกนเวอร์ชัน)

เมื่อได้ทำการสแกนเวอร์ชัน (-sV), ซึ่งได้มีการกำหนดค่าความยากระหว่าง 1-9 โดยตัวเลขต่ำจะเป็นการทดสอบ service โดยทั่วไป ซึ่งตัวเลขที่สูงนั้นจะมีความถูกต้องของการระบุ service ได้ดีกว่า อย่างไรก็ตามมันจะใช้เวลานานกว่าด้วย โดยปกติแล้วคือ 7

--version-light (การตั้งค่าความรุนแรงแบบเบาในการสแกนเวอร์ชัน)

สามารถเรียกอีกชื่อว่า --version-intensity 2 โหมดเบาบางทำให้การสแกนเวอร์ชันนั้นทำให้รวดเร็วขึ้นแต่มันจะทำอย่างเบาเพื่อที่จะชี้ถึงบริการ

--version-all (การสแกนเวอร์ชันในทุกช่องทางที่สามารถทำได้)

สามารถเรียกอีกชื่อว่า --version-intensity 9 ซึ่งเพื่อความมั่นใจว่าทุกการทดสอบนั้นได้พยายามที่จะเข้าไปยังแต่ละพอร์ต

--version-trace (Trace version scan activity)

หัวข้อของ Nmap เพื่อที่จะใช้แสดงเนื้อหาของการดีบักเกี่ยวกับว่าการสแกนที่ทำเป็นเวอร์ชันอะไร โดยจะเป็นซับเน็ตของค่าที่ได้จาก--packet-trace

-sR (RPC scan)

ใช้หลักการของการสแกนพอร์ต โปรแกรมจะทำการค้นหาพอร์ตทีซีพี ยูดีพี ที่เปิด แล้วจะทำการกระจายออกไปด้วยคำสั่ง SunRPC program NULL ในการพยายามที่จะทำการหา ไม่ว่าจะเป็นพอร์ตRPC หรือไม่ และถ้าสามารถหาโปรแกรมและหมายเลขเวอร์ชันมาได้ ดังนั้นถ้าเราสามารถใช้ คำสั่ง rpcinfo-p ถึงแม้ว่าการตรวจสอบพอร์ตของเป้าหมายจะอยู่ภายใต้ไฟร์วอลล์ หรือได้รับการคุ้มครอง (โดยอยู่ภายใต้การทำงานของโพรโตคอลทีซีพี) ซึ่งเหยื่อล่อจะไม่มีการทำงานรวมกับการสแกน RPC โดยจะมีการใช้งานอัตโนมัติงานในส่วนของการสแกนเวอร์ชัน(-sV)

การตรวจสอบระบบปฏิบัติการ (OS Detection)

-O (เปิดใช้งานการตรวจสอบระบบปฏิบัติ)

ใช้ในการตรวจสอบระบบปฏิบัติ โดยอาจจะใช้ –A ที่เป็นการตรวจสอบระบบปฏิบัติ และการตรวจสอบเวอร์ชัน โดยจะพยายามที่จะตรวจสอบระบบปฏิบัติ ในรุ่นที่ 2 ก่อน ถ้าไม่เจอก็จะทำการกลับไปหาในรุ่นที่ 1

-O2 (ตรวจสอบระบบปฏิบัติการรุ่นใหม่เท่านั้น)

ใช้งานตรวจสอบระบบปฏิบัติการรุ่นที่ 2 เท่านั้นแต่จะมีการกลับไปตรวจสอบระบบปฏิบัติการรุ่นที่ 1โดยถ้าไม่เจอจะทำการบันทึกเวลาและลดจำนวนแพ็คเก็ตที่ส่งไปยังแต่ละเครื่อง

-O1 (ตรวจสอบระบบปฏิบัติการรุ่น เก่าเท่านั้น)

ทำการตรวจสอบเฉพาะกรณีที่เป็นระบบปฏิบัติการรุ่น เก่าเท่านั้น ตัวเลือกนี้ถูกเอาออกเมื่อปลายปี 2006 หรือใน 2007

--osscan-limit (จำกัดการตรวจสอบระบบปฏิบัติการ)

การตรวจสอบระบบปฏิบัติการที่มีประสิทธิภาพ ถ้ามีการเปิดพอร์ตเพียงเล็กน้อย และปิดพอร์ตทีซีพี การใช้ตัวเลือกนี้จะไม่ทำการพยายามตรวจสอบโฮร์ตใหม่ เมื่อไม่พบตามเกณฑ์ ซึ่งสามารถทำการบันทึก เวลา โดยเฉพาะการสแกนด้วย -P0 โดยปกติแล้วจะมีการใช้งานด้วย -O หรือ -A.

--osscan-guess; --fuzzy (การคาดเดาผลของการตรวจสอบระบบปฏิบัติการ)

เมื่อ Nmap ไม่สามารถทำการตรวจสอบจับคู่ระบบปฏิบัติการได้สมบูรณ์ โดยอาจจะใกล้เคียง โดยจะมีการทำการคาดเดา แล้วแสดงผลของการจับคู่ออกมาในรูปแบบของเปอร์เซ็นต์

--max-os-tries (ตั้งค่าจำนวนครั้งสูงสุดในการตรวจสอบระบบปฏิบัติการ)

เมื่อ Nmap ทำการตรวจสอบระบบปฏิบัติการไปยังเป้าหมายและเกิดการล้มเหลวของการจับคู่ แล้วมันจะพยายามที่จะทำซ้ำ โดยปกติแล้วจะทำ 5 ครั้ง ถ้าเงื่อนไขนั้นถูกยอมรับจากการทำ fingerprint และ 2 ครั้งเมื่อเงื่อนไขนั้นไม่ดีพอ โดยสามารถกำหนด --max-os-tries value (เช่น 1) ซึ่งทำให้การทำงานเร็วขึ้น โดยตัวเลือกนี้มีผลต่อการตรวจสอบระบบปฏิบัติการรุ่นที่ (-O2, ค่าปกติ)

เวลาและประสิทธิภาพ (Timing and Performance)

สำหรับบางตัวเลือกจะมีการใช้พารามิเตอร์ของเวลา ซึ่งมีค่าเป็นมิลลิวินาทีตามปกติ ซึ่งคุณสามารถเพิ่ม 's', 'm', หรือ 'h' เพื่อที่จะกำหนดให้อยู่ในรูปแบบขอวินาที นาที หรือ ชั่งโมง ดังนั้นจึงกำหนด host-timeout อาร์กิวเมนต์ 900000 = 900s, และ 15m

--min-hostgroup <numhosts>; --max-hostgroup <numhosts>

--min-hostgroup <numhosts> เป็นค่าสูงสุดของขนาดกลุ่มโฮร์ต

--max-hostgroup<numhosts> เป็นค่าต่ำสุดของขนาดกลุ่มของโฮร์ตให้ Nmap พยายามที่จะรักษาระดับของขนาดกลุ่มให้มีค่ามากกว่าที่กำหนดเสมอ แต่มันสามารถต่ำกว่าได้เมื่อเหลือจำนวนเป้าหมายต่ำกว่าที่กำหนด

--min-parallelism <numprobes>; --max-parallelism <numprobes>

-min-parallelism เป็นจำนวนสูงสุดที่ได้ทำการสแกนเข้าไปยังเป้าหมาย โดยจะเพื่อความเร็วของการสแกนทำให้ได้ผลที่ไม่ค่อยจะดี จะมีความเสี่ยงเมื่อทำงานที่มีความต้องการความแม่นยำสูงมาก จะเป็นการลดความสามารถของ Nmap

--max-parallelism บางครั้งตั้งไว้เพื่อที่จะป้องกัน Nmap จากการส่งการทดสอบอื่นๆไปยังเป้าหมาย โดยสามารถที่จะรวมกับ --scan-delay เพื่อที่จะทำให้มันประสิทธิภาพที่ดีขึ้น

--min-rtt-timeout <time>, --max-rtt-timeout <time>, --initial-rtt-timeout <time>

--min-rtt-timeout <time> แทบจะไม่ได้ใช้งานเนื่องจากปกติแล้ว Nmap จะทำการสแกนโดยใช้แม่แบบชื่อว่า aggressive เมื่อเครือข่ายไม่น่าเชื่อถือ ถ้าน่าเชื่อก็จะทำการลดค่าลงมาได้

--max-rtt-timeout <time> , **--initial-rtt-timeout <time>** สามารถทำการกำหนดและทำงานได้กับการทำงาน -P0

--max-retries <numtries> (กำหนดจำนวนครั้งที่ทำการ retransmissions)

ใช้ในการกำหนดการ Retransmissions ถ้ามีค่าเป็น 0 จะเป็นการป้องกัน retransmissionโดยปกติแล้ว (ไม่มีตัวเลือก -T) จะทำการ retransmissions 10 ครั้ง

--host-timeout <time> (ค่าสูงสุดในการยกเลิกการสแกน)

เป็นจำนวนเวลาสูงสุดในการคอยบ่อยครั้งที่มีค่า 30 นาที เป็นค่าปกติ ต่อการสแกน 1 โฮร์ต

--scan-delay <time>; --max-scan-delay <time> (ปรับค่าดีเลย์ระหว่างการทดสอบ)

--scan-delay เป็นค่าเวลาในการรอการส่งแพ็คเก็ตที่จะทำการทดสอบในแต่ละการทดสอบโดย Nmap จำกัดช้าสุดที่ 1 วินาที

--max-scan-delay ปรับค่าสูงสุดของดีเลย์ที่ใช้ในการสแกน

--defeat-rst-ratelimit

ใช้งานเมื่อสนใจเฉพาะพอร์ตที่เปิดอยู่ และจะไม่แยกความแตกต่างระหว่างพอร์ตที่ถูกฟิลเตอร์กับพอร์ตที่ปิดอยู่ ทำให้ทำงานได้เร็วขึ้น

-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> (การตั้งค่าแม่แบบของเวลา)

ในส่วนนี้จะมีค่าตั้งแต่ 0-5 หรือการใช้ชื่อตามแบบ ดังนี้ paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4), และ insane (5)

- paranoid และ sneaky นั้นใช้ในการหลีกเลี่ยง IDS มักเป็นการทำเฉพาะพอร์ต เพราะทำนานมาก (15วินาที, 0.4 วินาที)

- Polite ทำการสแกนอย่างช้าๆกินช่วงความถี่ (bandwidth) และแหล่งข้อมูลของเครื่องเป้าหมายน้อย

- Normal ค่าปกติการทำงานของโปรแกรม

- Aggressive จะเพิ่มความเร็วของการสแกนทำให้คุณสามารถหาผลลัพธ์ได้เร็วยิ่งขึ้น และน่าเชื่อถือ (เพิ่มดีเลย์ในการสแกนเป็น 10 มิลลิวินาที สำหรับพอร์ตทีซีพี)

- Insane เป็นการสมมติว่าคุณนั้นจะทำการสแกนเร็วเป็นพิเศษหรือจะยอมเรื่องความแน่นอนสำหรับความเร็ว (เพิ่มดีเลย์ในการสแกนเป็น 5 มิลลิวินาที สำหรับพอร์ตทีซีพี)

การหลบหลีกไฟร์วอลล์/IDS และการปลอมตัว (Firewall/IDS Evasion and Spoofing)

-f (การทำแตกแพ็คเก็ตออกเป็นส่วนย่อยๆ – flagmentation); **--mtu** (กำหนดขนาดของ MTU)

การกำหนดตัวเลือกนี้ Nmap จะทำการแยกแพ็คเก็ตออกเป็น 8 ไบต์ หรือน้อยกว่า ดังนั้นเฮดเดอร์ของทีซีพีที่มีขนาด 20 ไบต์ จะแยกเป็น 3 แพ็คเก็ต โดย 2 แพ็คเก็ตแรกจะเป็นส่วนที่มาจาก 16 ไบต์แรกของ เฮดเดอร์ทีซีพี ส่วนอีกหนึ่งแพ็คเก็ตจะเป็น 4 ไบต์สุดท้ายของเฮดเดอร์ทีซีพี โดยแต่ละการแตกแพ็คเก็ตออกเป็นส่วนย่อยๆ จะมีเฮดเดอร์ไอพี การกำหนด -f เพื่อที่จะใช้ 16 ไบต์ ต่อการแตกแพ็คเก็ต 1 แพ็คเก็ต(ลดจำนวนของแตกแพ็คเก็ต) หรือคุณสามารถกำหนดขนาดของออฟเซ็ตได้ด้วยตัวเลือก --mtu ถ้าไม่มีการกำหนดตัวเลือก -f ถ้าคุณใช้ -mtu ขนาดของออฟเซ็ตจะต้องเป็นจำนวนเท่าของ 8 เท่านั้น มิฉะนั้นอาจเกิดปัญหากับระบบปฏิบัติการของคุณได้ นอกจากนี้แล้วมักให้ใช้ตัวเลือก --send-eth ในการทะลุผ่านชั้นไอพี และส่งเฟรมอีเทอร์เน็ตออกไปได้

-D <decoy1 [,decoy2][,ME],...> (การซ่อนตัวจากการสแกนด้วยนกต่อ)

เนื่องจากการสแกนด้วยนกต่อถูกกระทำได้โดยการทำรีโมทโฮร์ต โดยกำหนดว่าโฮร์ตที่ทำหน้าทีเป็นนกต่อที่ใช้ในการสแกนเครือข่ายเป้าหมายจำนวนมาก ด้วยเหตุนี้พวก IDS จะรายงาน 5-

10 พอร์ตจากการสแกนจากไอพีที่ไม่ซ้ำ แต่พวกมันจะไม่รู้ว่าถึงไอพีที่ทำการสแกน และคิดว่ามันเป็นเครื่องของนกต่อ เมื่อสามารถตามรอยเส้นทางของอุปกรณ์จัดเส้นทาง (router), การตอบสนอง-การยกเลิก (response-dropping) และกลไกอื่นๆ แล้วจะทำให้สามารถสร้างเทคนิคที่มีประสิทธิภาพสำหรับการซ่อนหมายเลขไอพีได้

การแยกนกต่อแต่ละโฮสต์ด้วยคอมมา และคุณสามารถใช้ตัวเลือก ME ลงในนกต่อเพื่อแสดงตำแหน่งของไอพีที่แท้จริงได้ ถ้าวาง ME ในตำแหน่งที่ 6 หรือหลังจากนั้น ซึ่งเครื่องตรวจจับการสแกนพอร์ตโดยทั่วไปแล้ว (เช่น Solar - scanlogd) ไม่น่าที่จะแสดงหมายเลขไอพีของคุณได้ ถ้าคุณไม่ใช้ ME Nmap จะใส่ให้คุณในตำแหน่งที่เกิดจากการสุ่มค่า

โฮสต์ที่คุณใช้เป็นนกต่อควรที่จะเปิดใช้งานอยู่ในขณะนั้นหรือคุณอาจจะใช้การประกาศ SYN ไปยังเป้าหมายของคุณ เพื่อความง่ายในการกำหนดเครื่องที่ทำการสแกน ควรที่จะทำงานในระบบเครือข่าย คุณอาจจะต้องการใช้หมายเลขไอพีแทนชื่อก็ได้ (ดังนั้นเครือข่ายของนกต่อจะไม่เห็นคุณใน nameserver logs)

นกต่อถูกใช้ในการเริ่มต้นการสแกน ping (ใช้ ICMP, SYN, ACK, หรืออื่นๆ) และใช้ระหว่างในขั้นตอนของการสแกนพอร์ต นกต่อจะถูกใช้งานระหว่างการตรวจสอบระบบปฏิบัติการ (-O) นกต่อจะไม่ทำงานกับการตรวจสอบเวอร์ชัน หรือการสแกนแบบ TCP connect (-sT)

มันจะไม่ประโยชน์เลย ถ้าใช้จำนวนนกต่อมากเกินไป โดยอาจจะทำให้การสแกนของคุณช้าและอาจจะทำให้ความถูกต้องนั้นน้อยลง ด้วยเหตุนี้บางผู้ให้บริการอินเทอร์เน็ตจะทำการกรองการแพ็คเก็ตที่ถูกปลอมออก แต่อาจจะไม่ห้ามการปลอมแพ็คเก็ตไอพีที่ถูกปลอมออกได้

-S <IP_Address> (การปลอมหมายเลขไอพีแหล่งที่มา)

ใช้ในการทำการปลอมหมายเลขไอพี โดยจะมีการรายงานผลกลับมา

-e <interface> (ใช้ในการกำหนดอินเทอร์เฟสในการสแกน)

บอกว่าอินเทอร์เฟสอะไรที่จะทำการส่งและรับแพ็คเก็ต โดยปกติแล้ว Nmap ควรที่จะสามารถตรวจจับได้อย่างอัตโนมัติ แต่มันจะไม่บอกคุณถ้ามันไม่สามารถรับและส่ง

--source-port <portnumber>; == -g <portnumber>

การปลอมหมายเลขพอร์ต)

--data-length <number> (การเพิ่มข้อมูลจากการสุ่มลงในแพ็คเก็ตที่จะทำการส่ง)

ปกติแล้ว Nmap จะทำการส่งแพ็คเก็ตที่ประกอบด้วยเฮดเดอร์เท่านั้น ดังนั้นแพ็คเก็ตทีซีพีจะมีค่าประมาณ 40 ไบต์และ ICMP echo request จะเหลือเพียง 28 ไบต์ โดยแพ็คเก็ตที่ใช้ในการ

ตรวจสอบระบบปฏิบัติการ (-O) จะได้รับผลกระทบเนื่องจากมันต้องการการทดสอบที่เหมาะสม แต่การ ping และการทำพอร์ตสแกน นั้นจะช้าลงเล็กน้อย แต่สามารถทำการสแกน slightly อย่างเห็นได้ชัด

-ip-options <S|R [route]|L [route]|T|U ... >; --ip-options <hex string>

โพรโตคอลไอพีได้มีการใช้ในหลายๆตัวเลือก ซึ่งอาจจะใช้ในส่วนหัวของแพ็คเก็ต ซึ่งทางอินเทอร์เน็ต อุปกรณ์จัดเส้นทาง (router) มักจะทำการป้องกันตัวเลือกของโปรแกรมที่อันตรายทั้งหมด เช่น source routing โดยตัวเลือกนี้สามารถใช้ในกรณีการระบุจุดของเครือข่ายเพื่อกำหนดเส้นทางไปยังเป้าหมาย ถ้าไฟล์วอลล์ทำการหยุดแพ็คเก็ต นั้นจะสามารถกำหนดความแตกต่างการกำหนดเส้นทางด้วยการหลีกเลี่ยงเส้นทางนั้นหรือตัวเลือก loose source routing

โดยการกำหนดไอพีนั้นเป็นอาร์กิวเมนต์ที่จะทำการส่งค่าของตัวเลือก --ip-option โดยแต่ละจำนวนฐานสิบหก และตามด้วย \x เมื่อเป็นเลข 2 ตัวเลข โดยการทำซ้ำนั้นสามารถใช้ด้วยการใช้ * เช่น \x01\x07\x04\x00*36\x01 เป็นการประกอบด้วย hex string ที่ประกอบด้วย 36 NULL ไบต์

โดย Nmap ได้ทำกลไกเส้นทางลัดของการกำหนดตัวเลือก โดยการส่งอักษร R, T, หรือ U เพื่อที่จะทำการ request record-route, record-timestamp หรือ ตัวเลือกทั้งคู่ ตามลำดับ และสามารถกำหนด Loose หรือ strict source routing โดยอาจจะกำหนดด้วย L หรือ S สำหรับพื้นที่ว่าง และพื้นที่ที่ใช้ในการแยกรายชื่อของหมายเลขไอพี

ถ้าคุณต้องการมองตัวเลือกในแพ็คเก็ตที่ทำการส่งใช้ --packet-trace โดยสามารถดูรายละเอียดเพิ่มเติมได้ที่ http://seclists.org/Nmap-dev/2006/q3/0052.html.

--ttl <value> (การตั้งค่า time-to-live ของโพรโตคอลไอพีเวอร์ชัน 4)

ตัวเลือกนี้เป็นการกำหนดค่าฟิลด์ time-to-live ในโพรโตคอลไอพีเวอร์ชัน 4

--randomize-hosts (การสุ่มค่าของโฮร์ดเป้าหมาย)

บอก Nmap ในการสุ่มแต่ละกลุ่มของโฮสต์ที่เปิดใช้งานอยู่ทั้งหมด 8096 โฮสต์ ก่อนที่จะทำการสแกนพวกมัน โดยตัวเลือกนี้สามารถทำการสแกน เพื่อที่จะทำดูแลระบบเครือข่ายได้อย่างหลากหลาย ถ้าคุณต้องการสุ่มค่ากลุ่มใหญ่ ให้ทำการเพิ่ม PING_GROUP_SZ ในไฟล์ Nmap.h และทำการรีคอมไฟล์ ซึ่งทางเลือกของการแก้ปัญหานั้นคือการสร้างรายชื่อไอพีเป้าหมาย ด้วยการสแกน List (-sL -n -oN *filename*) โดยสุ่มค่านั้นจะเป็นการทำด้วย Perl Script

--spoof-mac <mac address, prefix, or vendor name> (การปลอมหมายเลข Mac address)

Nmap นั้นจะมีการใช้ MAC address สำหรับเฟรมอีเทอร์เน็ตทั้งหมดที่ได้ทำการส่ง โดยตัวเลือกนี้จะทำการส่ง --send-eth เพื่อให้แน่ใจว่า โปรแกรม Nmap จะทำการส่งแพ็คเก็ตในระดับอีเทอร์เน็ต โดยหมายเลข MAC address มีการใช้ในรูปแบบมากมาย ถ้าทั่วๆไปแล้ว string "0" ซึ่งโปรแกรม Nmap จะทำการเลือกสุ่มค่าอย่างสมบูรณ์ MAC สำหรับช่วงเวลาสื่อสาร(session) จะมีการใช้งานเลขจำนวนคู่ของเลขฐานสิบหก (ซึ่งจะมีการแยกด้วย โคลอน (:) ถ้าโปรแกรม Nmap ได้รับเลขน้อยกว่า 12 ตัวเลขฐานสิบหก แล้วโปรแกรม Nmap จะมีการใช้ 6 ไบต์ กับค่าที่ได้จากการสุ่มค่า ถ้าไม่มีอาร์กิวเมนต์ - argument 0 หรือ hex string โปรแกรม Nmap จะทำการมองผ่าน Nmap-mac-prefixes เพื่อที่จะทำการหาชื่อของผู้ผลิต (ขนาดตัวอักษรไม่มีผล) ถ้าสามารถทำการจับคู่กันได้ โปรแกรม Nmap จะใช้ OUI ของผู้ผลิต (3-ไบต์หน้า) และเติมอีก 3 ไบต์ โดยการสุ่มค่า

--badsum (การส่งแพ็คเก็ตด้วยทีซีพี ยูดีพี checksums ปลอม)

เป็นตัวเลือกในการใช้งานค่า checksum ทีซีพี หรือ ยูดีพี ที่ผิดพลาด สำหรับแพ็คเก็ตที่ทำการส่งไปยังเป้าหมาย รายละเอียดสามารถดูได้ที่ http://www.phrack.org/phrack/60/p60-0x0c.txt

การนำออก (Output)

-oN <filespec> (Normal output)

ตัวเลือกในการนำออกออกในรูปแบบของเอกสารทั่วไป

-oX <filespec> (XML output)

ตัวเลือกในการนำออกออกในรูปแบบของเอกสาร XML ซึ่งเป็นเอกสารมาตรฐานสากลในการองค์กรใหญ่ๆ

-oS <filespec> (ScRipT KIdd|3 oUTpuT)

ตัวเลือกในการนำออกScript kiddie คล้ายการทำการนำออกเชิงโต้ตอบ (interactive output)

-oG <filespec> (Grepable output)

ตัวเลือกในการนำออกในรูปแบบของ Grepable

-oA <basename> (Output to all formats)

ตัวเลือกในการนำออกในรูปแบบหลักทั้ง 3 ของโปรแกรม Nmap (-oN, -oX)

ภาคผนวก ข

คู่มือการติดตั้งชุดโปรแกรมทดสอบความปลอดภัยระบบคอมพิวเตอร์

การติดตั้งชุดโปรแกรม ที่ใช้งานผ่านทางคอมมานด์ไลน์

```
isagl2:/home/inguan/Desktop/NSC2008# ls
IPT  iptfe
isagl2:/home/inguan/Desktop/NSC2008# ls -al ./*/configure
-rw-r--r-- 1 root root  270103 2007-12-26 22:25 ./IPT/configure
-rw-r--r-- 1 root root 1035165 2008-01-01 11:55 ./iptfe/configure
isagl2:/home/inguan/Desktop/NSC2008# chmod 744 ./*/configure
isagl2:/home/inguan/Desktop/NSC2008# ls -al ./*/configure
-rwxr--r-- 1 root root  270103 2007-12-26 22:25 ./IPT/configure
-rwxr--r-- 1 root root 1035165 2008-01-01 11:55 ./iptfe/configure
isagl2:/home/inguan/Desktop/NSC2008#
```

1. ติดตั้งโปรแกรม g++, gcc
2. รันไฟล์ ./configure ในโฟลเดอร์ของ IPT

*กรณีเกิดปัญหาให้ทำการแก้ค่าการอนุญาต (permission) ของไฟล์ configure ด้วยคำสั่ง chmod 744 configure

3. ใช้คำสั่ง make
4. ใช้คำสั่ง make install

```
isagl2:/home/inguan/Desktop/NSC2008# cd IPT/
isagl2:/home/inguan/Desktop/NSC2008/IPT# ./configure
checking for gcc... gcc
checking for C compiler default output file name... a.out
```

รูปที่ 1 แสดงการใช้คำสั่ง ./configure

```
isagl2:/home/inguan/Desktop/NSC2008/IPT# make
Compiling libpcap
make[1]: Entering directory `/home/inguan/Desktop/NSC2008/IPT/libpcap'
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/home/inguan/Desktop/NSC2008/IPT/libpcap'
Compiling libdnet
```

รูปที่ 2 แสดงการใช้คำสั่ง make

```
isagl2:/home/inguan/Desktop/NSC2008/IPT# make install
Compiling libpcap
make[1]: Entering directory `/home/inguan/Desktop/NSC2008/IPT/libpcap'
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/home/inguan/Desktop/NSC2008/IPT/libpcap'
Compiling libdnet
make[1]: Entering directory `/home/inguan/Desktop/NSC2008/IPT/libdnet-stripped'
Making all in include
```

รูปที่ 3 การใช้คำสั่ง make install

การติดตั้งชุดโปรแกรม ที่ใช้งานผ่านทางส่วนต่อประสานกราฟิกกับผู้ใช้งาน

1. ติดตั้งโปรแกรม g++, gcc, kdelibs4-dev, libice-dev, libtool, xlibs-dev
2. ติดตั้งชุดโปรแกรม ที่ใช้งานผ่านทาง command line
3. รันไฟล์ ./configure ในไดเรกทอรี iptfe
4. ใช้คำสั่ง make
5. ใช้คำสั่ง make install

```
isagl2:/home/inguan/Desktop/NSC2008/iptfe# ./configure
checking build system type... i686-pc-linux-gnu
checking host system type... i686-pc-linux-gnu
checking target system type... i686-pc-linux-gnu
checking for a BSD-compatible install... /usr/bin/install -c      ,
```

รูปแสดงการใช้คำสั่ง ./configure

```
isagl2:/home/inguan/Desktop/NSC2008/iptfe# make
Makefile:863: warning: overriding commands for target `clean-bcheck'
Makefile:826: warning: ignoring old commands for target `clean-bcheck'
Makefile:868: warning: overriding commands for target `bcheck-am'
Makefile:831: warning: ignoring old commands for target `bcheck-am'
make  all-recursive
```

รูปแสดงการใช้คำสั่ง make

```
isagl2:/home/inguan/Desktop/NSC2008/iptfe# make install
Makefile:863: warning: overriding commands for target `clean-bcheck'
Makefile:826: warning: ignoring old commands for target `clean-bcheck'
Makefile:868: warning: overriding commands for target `bcheck-am'
Makefile:831: warning: ignoring old commands for target `bcheck-am'
Making install in doc
```

รูปแสดงการใช้คำสั่ง make install

ภาคผนวก ค
คู่มือการใช้งานอย่างละเอียด
ชุดโปรแกรมทดสอบความปลอดภัยระบบคอมพิวเตอร์

การใช้งานชุดโปรแกรมที่ใช้งานผ่านทางคอมมานด์ไลน์

1. โปรแกรมทำงานบนสิทธิของ root
2. ทำการป้อนคำสั่งตามกฎการใช้งานของชุดโปรแกรม

ipt <scan option> <Target(s)>

<scan option> -exploit <exploit option> <Target(s)>

<scan option> -exploit --custom:<exploit's ID> <Target(s)>

ตัวอย่าง: (รูปแบบโหมดการทำงานของโปรแกรม IPT)

ipt -fast (no exploit plug-in)

-aggressive -exploit --most-plugin

-complete -exploit --all-plugin

-exploit --custom:dos01,dos02

ตัวเลือกของส่วนการสแกนโหมดต่างๆจะมีคุณสมบัติตามตารางข้างล่างนี้

Scan's Mode	Speed	Accuracy	Security	Average Time / Host
Fast	High	Low	None	80-180 sec.
Aggressive	Medium	Medium	Low	100-330 sec.
Complete	Low	High	Medium	120-400 sec.
Custom	-	-	-	-

ตัวเลือกของส่วนเอ็กซ์พลอยท์ แบ่งออกเป็น 4 โหมดดังนี้

1.exploit ไม่ทำการเอ็กซ์พลอยท์ (Exploit)

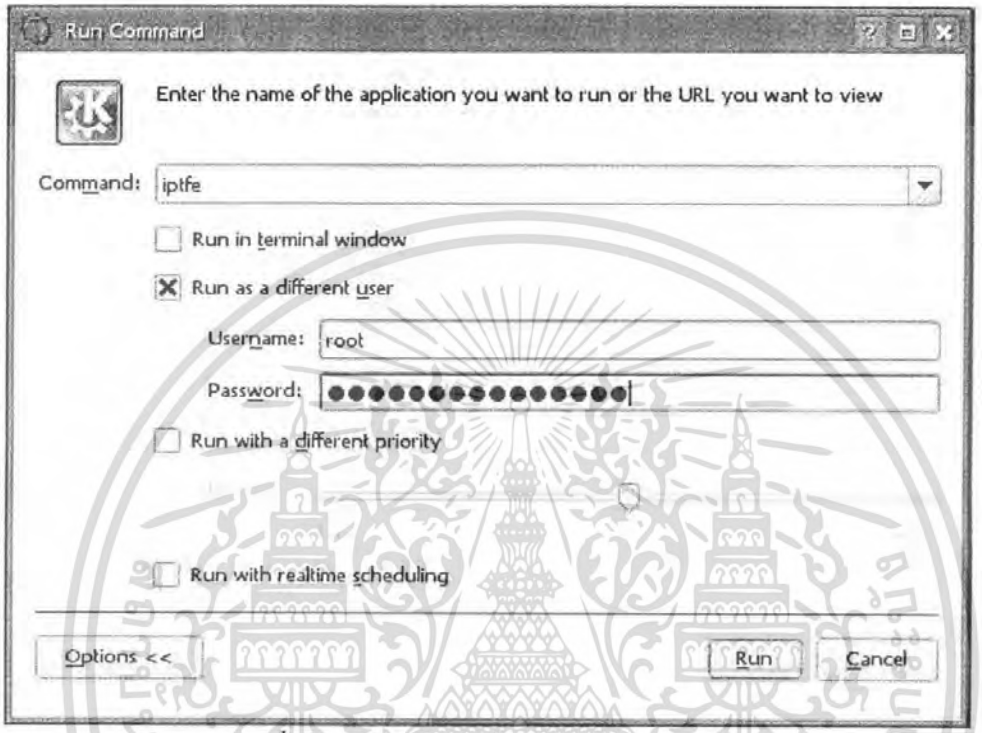
2.exploit --most-plugin ทำการเอ็กซ์พลอยท์ (Exploit) ส่วนโค้ดที่สำคัญ

3.exploit --all-plugin เลือกโค้ดเอ็กซ์พลอยท์ (Exploit) ทั้งหมด รวมถึงการทำ DoS

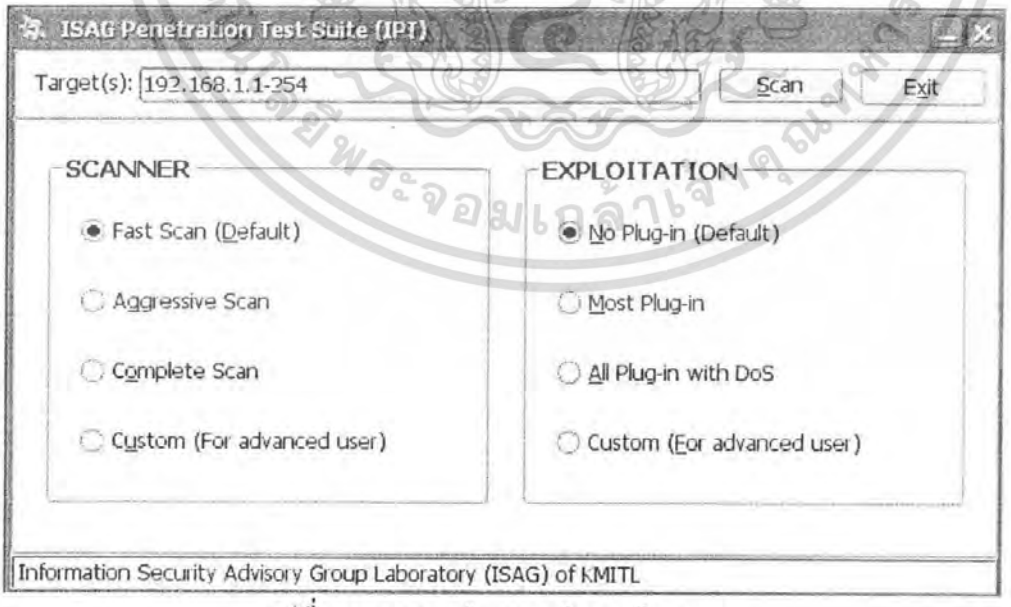
4.custom ให้ผู้ใช้งานเลือกโค้ดต่างๆที่ใช้ในการทำเอ็กซ์พลอยท์ (Exploit)

การใช้งานชุดโปรแกรมที่ใช้งานผ่านทางส่วนต่อประสานกราฟิกกับผู้ใช้งาน

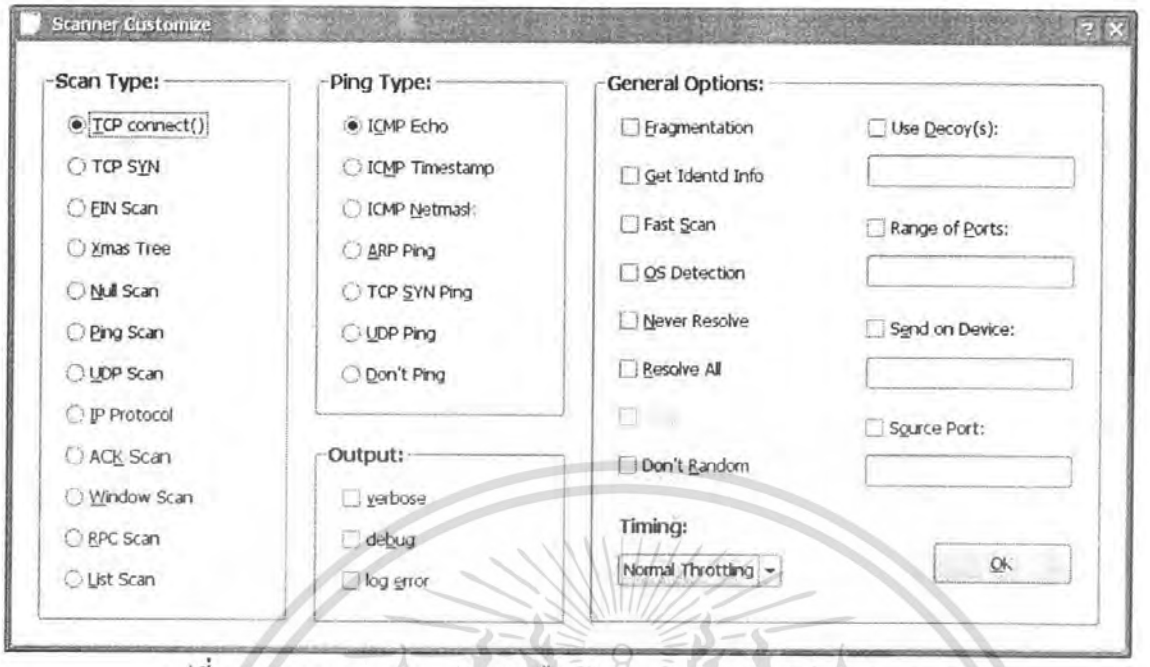
1. ทำการเรียก iptfe ผ่าน Run command ในสิทธิของ root



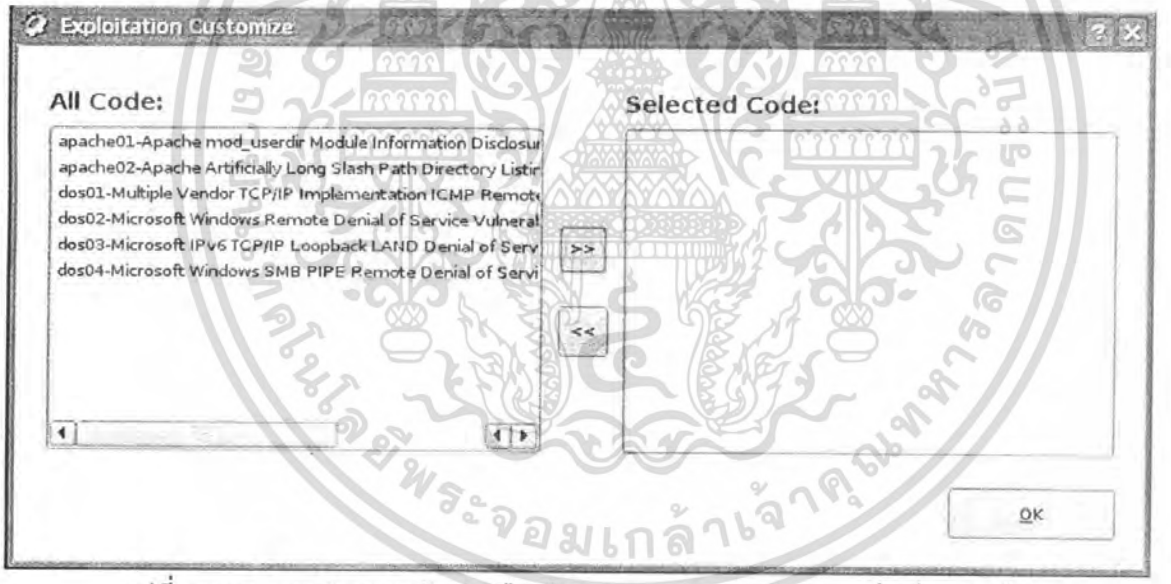
รูปที่ 1 การเรียก iptfe ผ่าน Run command



รูปที่ 2 แสดงการทำงานหลังการเรียก iptfe



รูปที่ 3 แสดงการทำงานหลังการเลือกโหมด custom ของส่วนการสแกน



รูปที่ 4 แสดงการทำงานหลังการเลือกโหมด custom ของส่วนการเอ็กซ์พลอยท์