วารสารวิชาการและวิจัย มทร.พระนคร ฉบับพิเศษ
การประชุมวิชาการมหาวิทยาลัยเทคโนโลยีราชมงคล ครั้งที่ 5

การรักษาความมั่นคงแบบสมบูรณ์สำหรับการเข้าถึงไมโครซอฟท์วินโดว์เซิร์ฟเวอร์จากระยะไกลด้วย Remote Desktop

Complete Security Protection for Remote Desktop – Microsoft Windows Server

ชาญศักดิ์ สุวรรณกุล[1*] และ สานนท์ ฉิมมณี[2]

[1]นักศึกษา [2]ผู้ช่วยศาสตราจารย์ สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต จังหวัดปทุมธานี 12000

บทคัดย่อ

Remote Desktop เป็นวิธีการที่แพร่หลายที่สุดอย่างหนึ่งในการเข้าไปจัดการไมโครซอฟท์วินโดว์เซิร์ฟเวอร์ที่ตั้งแบบ Co-location ที่ Internet Data Center แต่ยังมีปัญหาเรื่องความปลอดภัยเพราะรหัสผ่าน (Password) สามารถถูกดักจับจากเครื่องลูกข่ายที่ติด Trojan หรือถูกดักจับข้อมูลระหว่างการสื่อสารผ่านเครือข่าย หรือการสุ่มหารหัสผ่านด้วยวิธีการ Password Generator บทความนี้จะนำเสนอวิธีการป้องกันอย่างสมบูรณ์แบบ แม้ว่ารหัสผ่านของผู้ใช้จะถูกดักจับ หรือถูกขโมยไป ก็ไม่สามารถเข้าไปทำการ Remote Desktop ได้ วิธีการที่นำเสนอนี้จะช่วยป้องกันเรื่องความปลอดภัยจากผู้ที่ไม่ได้รับอนุญาตและสร้างความมั่นใจให้กับผู้ดูแลระบบได้เป็นอย่างดี โดยหลักการจะทำการปิดพอร์ต 3389 ซึ่งเป็นพอร์ตของ Remote Desktop ดังนั้นเครื่องใดๆในอินเทอร์เน็ตจะไม่สามารถเรียกขอเข้าใช้งานได้ สำหรับการขออนุญาตเข้าใช้จะต้องมีวิธีการร้องขอแบบพิเศษ และมีรหัสผ่านอีกชั้นหนึ่ง โดยเรียกผ่านพอร์ต 80 (พอร์ตของเว็บเซิร์ฟเวอร์) ซึ่งเปิดไว้ตามปกติของเว็บทั่วๆไป และการขอเข้าใช้จะเข้าได้แค่เพียงไอพีแอดเดรสเดียวที่ได้รับอนุญาตเท่านั้น วิธีการป้องกันนี้เป็นวิธีการอีกแบบหนึ่งที่ยังไม่มีการนำเสนอในที่ใดมาก่อน ผลจากการทดลองใช้หลักการนี้ในเว็บที่เกี่ยวโทรศัพท์เคลื่อนที่อันดับต้นๆ ของประเทศไทย มาเป็นระยะเวลากว่า 2 ปี สรุปได้ว่ายังไม่มีใครสามารถเจาะระบบเข้ามาได้แม้แต่ครั้งเดียว

Abstract

Remote Desktop is one of the most popular method to access to the microsoft windows server, which locate as Co-location in the Internet Data Center. But there is still a security problem because a password can be hacked by Trojan infected PC or password can be sniffed via network or even taking a random for password from Password Generator program. This paper presents the completed security protection, even the password has been hacked or stolen, the hacker can not access to the server via the remote desktop. Normally the port 3389 of Remote Desktop will be closed, thus, any computer from the internet cannot be accessed. To get access permission, it must be done with special requisition with the other password which access through the port 80 (port of web server) that is always generally opened. Only single IP address can get the permission at the time. This method of protection was never published anywhere yet. Result of using this method in the most popular mobile web in Thailand for more than 2 years, there is no one can hack into the system at all.

คำสำคัญ : Remote desktop Security Hacking MS Windows

Keywords : Remote desktop, Security, Hacking, MS Windows

[*]ผู้นิพนธ์ประสานงานไปรษณีย์อิเล็กทรอนิกส์ chansak@dit.daikin.co.jp โทร. 0 3821 3032 ต่อ 110 , 08 3111 0011

1. บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

จากการที่ขอบเขตของอินเทอร์เน็ตที่เปิดกว้าง ทำให้ผู้ใช้ทั่วโลกสามารถแชร์และอัพเดทข้อมูลได้ร่วมกันทุกที่ทุกเวลาผ่านเว็บเซิร์ฟเวอร์ ในทางกลับกันก็เกิดการโจมตีโดยแฮกเกอร์อาจจะทำด้วยวิธีปล่อย Trojan หรือ Spyware ที่เครื่องลูกเพื่อขโมยพาสเวิร์ดหรือดักจับพาสเวิร์ดจากเครือข่าย หรือการสุ่มหารหัสผ่านด้วยวิธีการ Password Generator เมื่อแฮกเกอร์สามารถเข้าระบบได้แล้วก็จะสามารถควบคุมได้ทั้งระบบอาจจะไปทำให้เซิร์ฟเวอร์นั้นเปลี่ยนแปลงได้ตามต้องการซึ่งจะทำให้เว็บหยุดการทำงานหรือเข้าไปเปลี่ยนแปลงเนื้อหาดังตัวอย่างเช่น ข่าวเกี่ยวกับการแฮกเว็บสำนักนายกรัฐมนตรี วันที่ 8 พฤษภาคม พ.ศ. 2556 ที่ผ่านมา ดังนั้นผู้ดูแลเซิร์ฟเวอร์จะต้องหาวิธีการป้องกันไม่ให้เซิร์ฟเวอร์ถูกแฮกได้ ในบทความนี้จะนำเสนอวิธีการแบบใหม่ ที่สามารถป้องกันการเข้าถึงไมโครซอฟท์เซิร์ฟเวอร์ด้วยรีโมทเดสก์ท็อปโดยไม่ได้รับอนุญาตอย่างสมบูรณ์แบบ

1.1.1 ทบทวนวรรณกรรม

ปัจจุบันนี้เริ่มนิยมใช้ Thin Client (เครื่อง PC ที่มีเพียงจอภาพ เมาส์ คีย์บอร์ด เท่านั้น) รีโมทเดสก์ท็อปมาที่เซิร์ฟเวอร์ A Closer Look at Thin-Client Connections: Statistical Application Identification for QoE Detection (สถิติของคุณภาพของประสบการณ์ในใช้งาน) ซึ่งได้วัดประสบการณ์ของผู้ใช้กับ Thin-Client ที่ Remote เข้าสู่ Server และแม้ตอนนี้จะมีเครื่องมือในการตรวจติดตามการเข้าใช้งานรีโมทเดสก์ท็อปได้ด้วย Proxy-based Security Audit System for Remote Desktop Access (ระบบตรวจสอบการงานรีโมทเดสก์ท็อปผ่านพร็อคซี่) ก็เป็นเพียงการตรวจติดตามซึ่งยังไม่สามารถป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตได้

1.2 วัตถุประสงค์ของการวิจัย

มีวัตถุประสงค์เพื่อศึกษาและคิดค้นวิธีการรักษาความมั่นคงแบบสมบูรณ์สำหรับการเข้าถึงไมโครซอฟท์วินโดว์เซิร์ฟเวอร์จากระยะไกลด้วย Remote Desktop

1.3 ขอบเขตการวิจัย

งานวิจัยนี้ได้วิจัยกับไมโครซอฟท์วินโดว์เซิร์ฟเวอร์ในการเข้าถึงผ่าน Remote Desktop

1.4 ขั้นตอนการดำเนินการวิจัย

1.4.1. ศึกษาการตั้งเวลาการทำงานโปรแกรมภายใน ในไมโครซอฟท์วินโดว์เซิร์ฟเวอร์

1.4.2. ศึกษาและโปรแกรมไฟร์วอลล์ SoftPerfect Personal Firewall เพื่อสามารถเปิดหรือปิดพอร์ต ใดๆ

1.4.3. ศึกษาและเขียนโปรแกรม VB Script สคริปต์ เพื่อรันบนเว็บเซิร์ฟเวอร์

1.4.4. ศึกษาและเขียนโปรแกรม ASP เพื่อใช้ด้วยการเรียกผ่านเว็บเซิร์ฟเวอร์

1.5 ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

สามารถป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าถึงไมโครซอฟท์วินโดว์เซิร์ฟเวอร์จากระยะไกลด้วย Remote Desktop ซึ่งทำให้ระบบมีความมั่นคงปลอดภัยอย่างสมบูรณ์

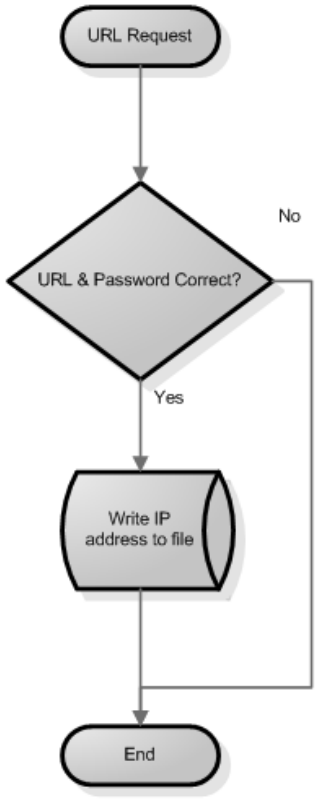
2. วิธีการทดลอง

2.1 วิธีการนำเสนอ

1. การเข้าถึงไมโครซอฟท์วินโดว์เซิร์ฟเวอร์ด้วยรีโมตเดสก์ท็อป จะมีการร้องขอใช้พอร์ต 3389 ดังนั้นถ้าปิดพอร์ต 3389 เครื่องลูกข่ายก็ไม่สามารถเข้าถึง และในงานวิจัยนี้จะอนุญาตเฉพาะไอพีเดียวของเครื่องลูกข่ายที่ได้รับอนุญาตจะสามารถเข้าถึงได้

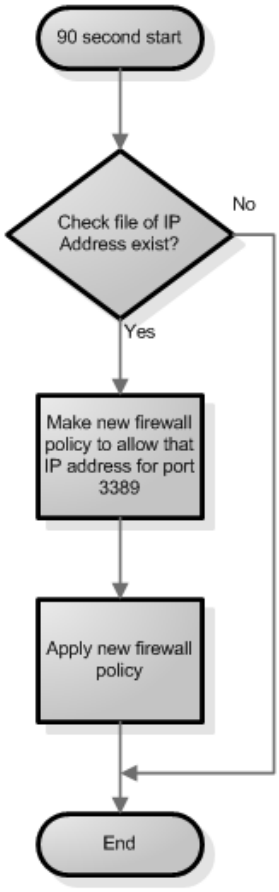
2. เพื่อป้องกันการเข้าถึงเซิร์ฟเวอร์ทุกๆทางจะปิดพอร์ตทุกๆพอร์ตที่ไม่ได้ใช้งาน แต่จะเปิดเฉพาะพอร์ตที่เป็นเว็บเซิร์ฟเวอร์คือ 80 และ 443 เท่านั้น การปิดพอร์ตจะใช้ซอฟท์แวร์ไฟร์วอลล์ชื่อ Softperfect Personal Firewall

3. เขียนโปรแกรม ASP เพื่อรองรับการร้องขอเพื่อใช้งานรีโมตเดสก์ท็อป และเมื่อได้รับการร้องขออย่างถูกต้อง ก็จะมีการสร้างไฟล์ใหม่โดยเก็บเบอร์ไอพีแอดเดรสในไฟล์นั่น



รูปที่ 1 Flowchart การทำงานของโปรแกรมที่เว็บเซิร์ฟเวอร์

เขียนโปรแกรมสคริปต์เพื่อนำค่าในไฟล์ที่ได้มาแก้ไขค่าของโปรแกรมไฟร์วอลล์ แต่โปรแกรมนี้จะถูกเรียกรันด้วย เครื่องมือที่สามารถให้เรียกรันโปรแกรมได้ตามเวลาชื่อ Task Scheduler ในงานวิจัยนี้ได้กำหนดไว้ทุกๆ 90 วินาที จะมีการเรียกรันโปรแกรมสคริปต์ เพื่อตรวจสอบว่ามีการร้องขอเข้าใช้รีโมตเดสก์ท็อป



รูปที่ 2 Flowchart แสดงงาน Task Scheduler รันทุกๆ 90 วินาที

เซิร์ฟเวอร์ Dell PowerEdge R810 - Eight-Core Intel® Xeon® processor 7500 2 CPU Memory 32 GBs (Materials and Methods) ติดตั้งที่ True Internet Data Center แจ้งวัฒนะ กรุงเทพฯ ซึ่งมีการเขียนโปรแกรม ติดตั้งโปรแกรมและสคริปต์ไว้ที่เซิร์ฟเวอร์ตามข้อ 2.1

เครื่องลูกข่าย PC 2 เครื่อง และ Notebook 5 เครื่องเชื่อมต่ออินเทอร์เน็ต 3BB TOT True AIS 3G DTAC 3G True H 3G

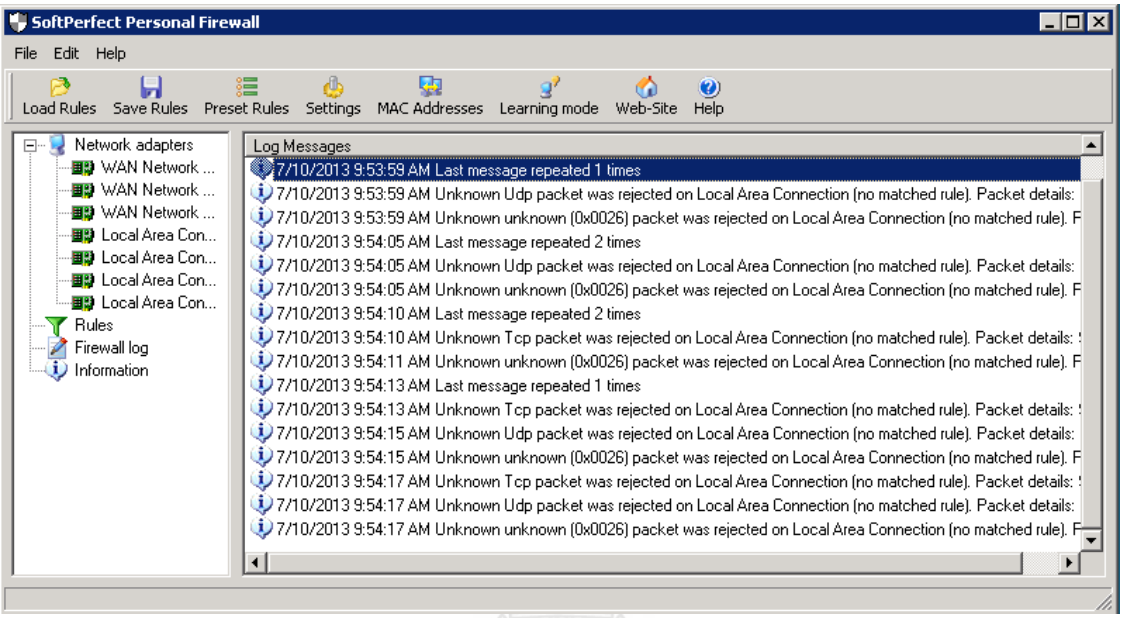
1. แบบไม่ได้รับอนุญาต โดยทดลองเครื่องละ 10 ครั้ง
2. ขออนุญาตผ่าน URL ที่กำหนดไว้ ทดลองทั้งหมด 10 ครั้ง
3. ใช้งานจริงด้วยวิธีการบนเว็บเซิร์ฟเวอร์ตั้งแต่ปี 2010 จนถึงปัจจุบัน

3. ผลการทดลองและวิจารณ์ผล

1. จากการทดสอบตามข้อ 2.2.1 พบว่าไม่สามารถเข้าถึงได้แม้แต่ครั้งเดียว โดยที่โปรแกรมไฟร์วอลล์ที่เซิร์ฟเวอร์จะมี log แจ้งมาว่ามีการร้องขอที่ไม่เข้ากฎที่กำหนด

2. จากการทดสอบตามข้อ 2.2.2 สามารถเข้าถึงได้ทุกเครื่องตามลำดับ

3. จากการใช้งานจริงมาตั้งแต่ปี 2010 จากการตรวจ Log ที่เซิร์ฟเวอร์พบว่าไม่มีการล็อกอินจากผู้ที่ไม่ได้รับอนุญาตมาแม้แต่ครั้งเดียว



รูปที่ 3 ตัวอย่างผลของการพยายามขอเข้าระบบแต่ได้รับการปฏิเสธเนื่องจากไม่เข้ากฎที่กำหนดไว้

4. สรุป

จากการศึกษาในเรื่องการป้องกันการเข้าถึงแบบไม่ได้รับอนุญาต สามารถนำวิธีการการอนุญาตร้องขอโดยผ่านเว็บเซิร์ฟเวอร์ได้ ซึ่งสามารถประยุกต์วิธีการนี้ไปใช้กับโปรโตคอลอื่นๆได้เช่น FTP (file transfer protocol) Telnet และอื่นๆ เป็นต้น

วิธีการนี้เป็นวิธีการใหม่ที่ยังไม่มีใครตีพิมพ์หรือเผยแพร่ ผู้วิจัยคาดหวังว่าวิธีการนี้จะช่วยอำนวยความสะดวกและความปลอดภัยให้ผู้ดูแลเซิร์ฟเวอร์แบบไมโครซอร์ฟวินโดว์ได้เป็นอย่างดี

5. กิตติกรรมประกาศ

บทความนี้เป็นส่วนหนึ่งของวิทยานิพนธ์ของการศึกษาในหลักสูตรปริญญาวิทยาศาสตร์มหาบัณฑิตซึ่งผู้เขียนใคร่ขอขอบคุณ ผศ.ดร. สานนท์ ฉิมมณี อาจารย์ที่ปรึกษา และคณะอาจารย์ผู้ทรงคุณวุฒิทุกท่านที่กรุณาให้คำแนะนำและขอขอบคุณทุกท่านที่ให้การสนับสนุนในด้านต่าง ๆ ให้งานฉบับนี้สำเร็จลงได้ด้วยดี

6. เอกสารอ้างอิง

เดลินิวส์. 2556. **เหิม! แฮกเว็บสำนักนายกฯ ด่าเละ "ยิ่งลักษณ์" [Exclusive]** วันพุธที่ 8 พฤษภาคม 2556 จาก http://www.dailynews.co.th/crime/202988

Maurizio Dusi, Stefano Napolitano, and Saverio Niccolini, NEC Laboratories Europe Salvatore Longo, University of Napoli Federico II. 2555. **A Closer Look at Thin-Client Connections: Statistical Application Identification for QoE Detection**, Published in: Communications Magazine, IEEE (Volume:50 , Issue: 11) Date of Publication: November 2012

Shi-hai Huang, Chuang Lin, An'an Luo, Zhen Chen, Xin Jiang, Kai Wang, Hui Zhang, Xue-hai Peng. 2552. **Proxy-based Security Audit System for Remote Desktop Access**, Computer Communications and Networks, 2009. ICCCN 2009. Proceedings of 18th International Conference on Digital Object Identifier

SoftPerfect. 2551. **SoftPerfect Personal Firewall** สืบค้นวันที่ 3 พฤษภาคม 2556 http://www.softperfect.com/products/firewall/