



บทที่ 3 : การป้องกันการเจาะระบบ Part4

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

การป้องกันการถูกเจาะระบบ



- IDS (Intrusion Detection System)
- IPS (Intrusion Prevention System)
- Firewall
- Antivirus
- เครื่องมือวิเคราะห์ระดับองค์กร
 - GFI LANguard N.S.S. (Network Security Scanner)
 - eEye Retina N.S.S.
 - Nessus Security Scanner

การป้องกันการถูกเจาะระบบ

- วิธีพื้นฐานคือการสแกนหาจุดอ่อนในระบบ และอัปเดตแพตช์เพื่อปิดช่องโหว่นั้นๆ
- ผู้ดูแลระบบต้องรู้ว่าเครือข่ายมีช่องโหว่ตรงไหนบ้าง การใช้เครื่องมือด้านการรักษาความปลอดภัยเป็นวิธีที่ง่ายและได้ผลที่สุด
- การสแกนควรทำทั้งจากภายในและภายนอกเครือข่าย ทั้งในรูปแบบมีสิทธิ์และไม่มีสิทธิ์เข้าถึงระบบ
- หลังจากทีสแกนแล้วต้องทำการอัปเดตแพตช์ โดยปกติแล้วเครื่องมือสำหรับใช้สแกนช่องโหว่ส่วนใหญ่จะสามารถอัปเดตแพตช์ได้อยู่แล้ว
- **การไม่อัปเดตแพตช์เป็นการเพิ่มความเสี่ยงให้สูงยิ่งขึ้น**

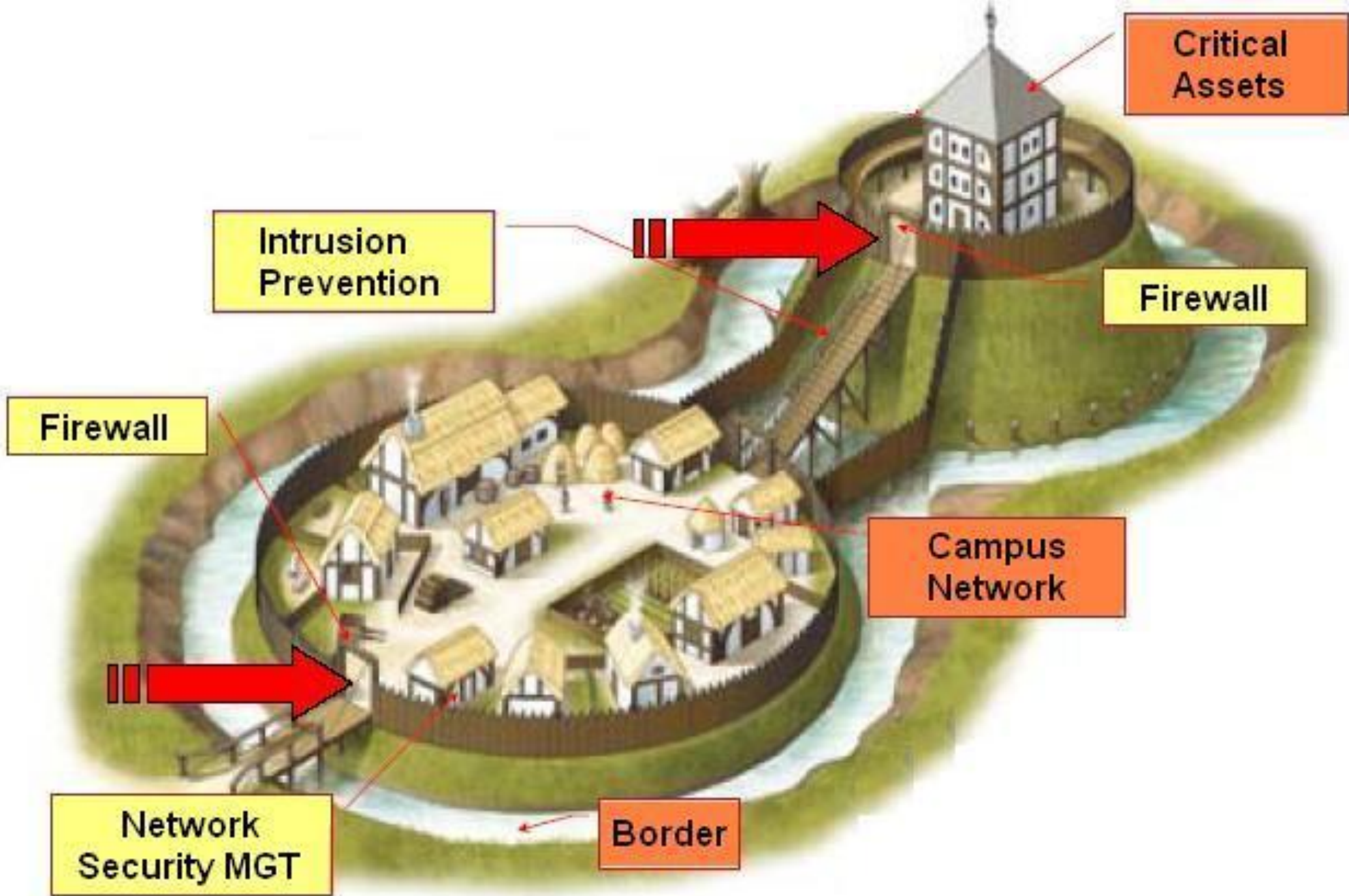


การป้องกันการถูกเจาะระบบ



- การติดตั้งแพตช์ หรือบางที่เรียกว่าฮ็อตฟิกส์ (Hot Fixes) เป็นสิ่งสำคัญมาก แต่ในระดับองค์กรควรมีการสำรองข้อมูล ก่อนการติดตั้งแพตช์ เพื่อป้องกันผลกระทบที่อาจเกิดขึ้นกับระบบ
- ที่สำคัญควรมีการติดตามข่าวสารด้านความปลอดภัยอยู่เสมอ





ระบบตรวจจับการบุกรุก

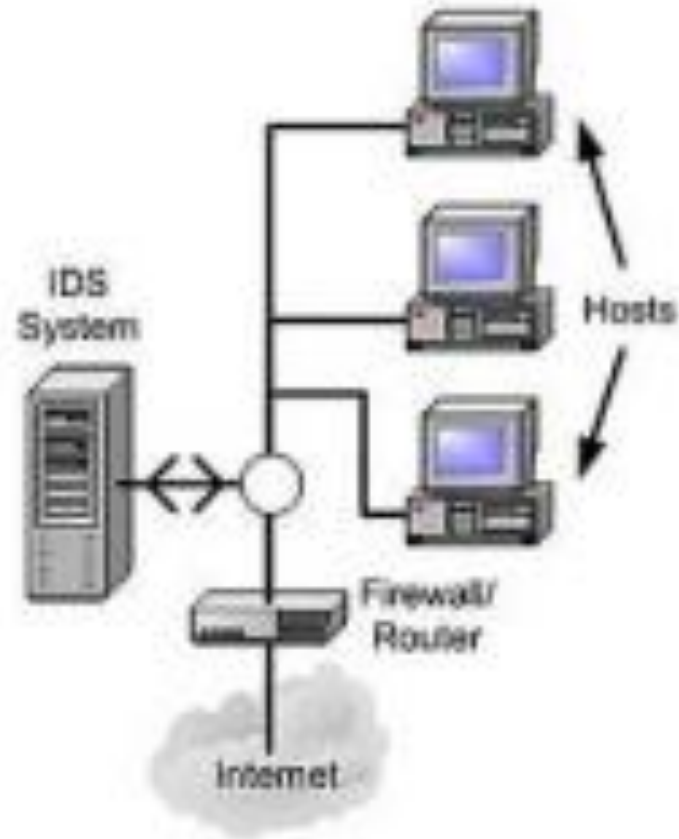
Intrusion Detection System (IDS)

- มีหน้าที่ตรวจจับการทำงานภายในเครือข่ายจากการตรวจสอบแพ็คเก็ต (Packet Monitoring) ที่วิ่งในเครือข่าย
- การตรวจสอบจะใช้ Pattern Matching เป็นหลัก เช่น เมื่อมีการตรวจจับการพยายามเชื่อมต่อพอร์ตที่ไม่ได้เปิดใช้งานไว้
- เสมือนเป็นกล้องวงจรปิด หรือสัญญาณกันขโมยมีหน้าที่ตรวจจับและแจ้งเตือน Admin เท่านั้น

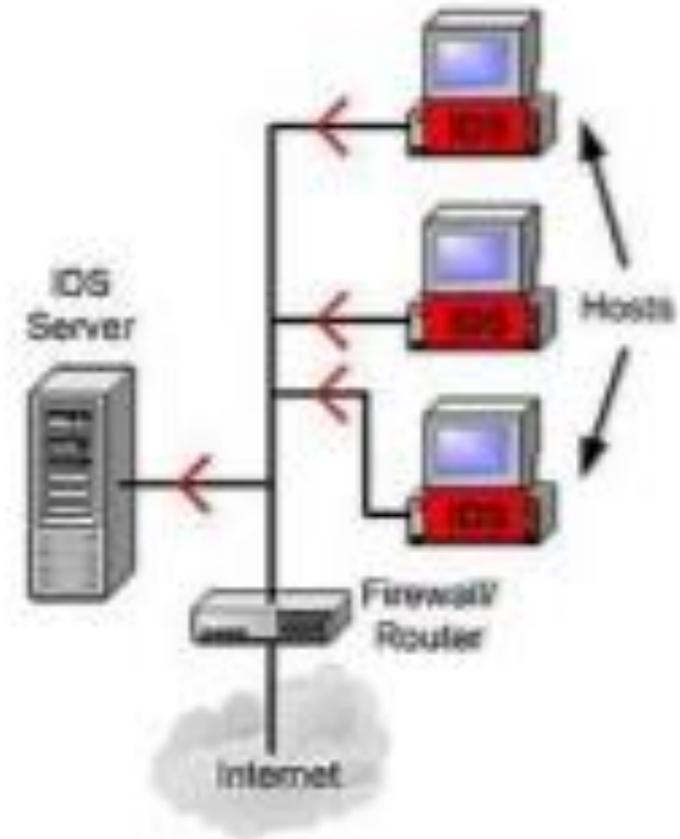


ประเภทของ IDS

Network Based IDS



Host Based IDS





Access denied

Intrusion Prevention System : IPS

หรือ Intrusion Detection and Prevention System (IDPS)

- ➡ พัฒนาต่อยอดมาจาก IDS
- ➡ หน้าที่คือ Monitoring, Logging, Block/Stop, Alarm, Drop Packet, Reset Connection และ Report
- ➡ * ผู้นำ IDPS คือ McAfee, Trend Micro, Cisco
- ➡ * ปัจจุบันระบบนี้ได้ถูกรวมเข้ากับผลิตภัณฑ์ Next-Generation Firewall (NGFW) ทำให้มีความนิยมลดลงมาก

*(ข้อมูลจาก Gartner ปี 2018)



SECURITY

SNORT

The Opensource IDPS

Download

<https://snort.org/>



Basic Analysis and Security Engine (BASE)

- Today's alerts:	unique	listing	Source IP	Destination IP
- Last 24 Hours alerts:	unique	listing	Source IP	Destination IP
- Last 72 Hours alerts:	unique	listing	Source IP	Destination IP
- Most recent 15 Alerts:	any protocol	TCP	UDP	ICMP
- Last Source Ports:	any protocol	TCP	UDP	
- Last Destination Ports:	any protocol	TCP	UDP	
- Most Frequent Source Ports:	any protocol	TCP	UDP	
- Most Frequent Destination Ports:	any protocol	TCP	UDP	
- Most frequent 15 Addresses:	Source	Destination		
- Most recent 15 Unique Alerts				
- Most frequent 5 Unique Alerts				

Added 4 alert(s) to the Alert cache
 Queried on : Mon June 26, 2006 15:01:24
 Database: snort@localhost (Schema Version: 107)
 Time Window: [2006-06-26 13:24:43] - [2006-06-26 15:01:23]

Search
 Graph Alert Data
 Graph Alert Detection Time

Sensors/Total: 1 / 1
 Unique Alerts: 30
 Categories: 7
 Total Number of Alerts: 995

- Src IP addrs: 199
- Dest. IP addrs: 4
- Unique IP links 206

- Source Ports: 505
 - TCP (502) UDP (3)
- Dest Ports: 6
 - TCP (5) UDP (1)

Traffic Profile by Protocol

TCP (96%)

UDP (1%)

ICMP (1%)

Portscan Traffic (3%)

Alert Group Maintenance | Cache & Status | Administration

BASE 1.2.5 (sarah) (by Kevin Johnson and the BASE Project Team
 Built on ACID by Roman Danyliw)

[Loaded in 0 seconds]

Firewall



- ▶ เป็นเครื่องมือที่ใช้ในการควบคุมและป้องกันการเข้าถึงระบบเครือข่ายและการโจมตีจาก Hacker
- ▶ เน้นการควบคุมการเข้าถึงโดย Rules ของเครื่องต้นทางและปลายทางด้วย IP Address และ Port
- ▶ จะเรียนอย่างละเอียดอีกครั้งหลังสอบกลางภาค

Antivirus



- ▶ เป็นโปรแกรมสามัญประจำเครื่องและเครือข่ายที่ใช้ป้องกัน Malware ที่อาจจะถูกฝังลงสู่คอมพิวเตอร์
- ▶ Antivirus จะใช้งานได้เป็นอย่างดีหากผู้ใช้มีการอัปเดตอยู่เสมอๆ
- ▶ เป็นสิ่งพื้นฐานที่ช่วยลดความเสี่ยงจากการถูกโจมตีได้ไม่น้อย
- ▶ จะเรียนอย่างละเอียดอีกครั้งหลังสอบกลางภาค

Tom's Guide reviews products independently. When you click links to buy products we may earn money to support our work.

ANTIVIRUS > BEST PICKS

Best Antivirus Software and Apps 2018

by PAUL WAGENSEIL & TOM'S GUIDE STAFF Jul 20, 2018, 7:15 AM

Best Basic Antivirus Product

BITDEFENDER ANTIVIRUS PLUS



9/10

REVIEW >

25.99 > Bitdefender

Best Midrange Antivirus Product

KASPERSKY INTERNET SECURITY



9/10

REVIEW >

\$39.99 > Kaspersky

Best Premium PC Security Suite

KASPERSKY TOTAL SECURITY



9/10

REVIEW >

\$49.99 > Kaspersky

Best Free PC Antivirus

AVAST FREE ANTIVIRUS



8/10

REVIEW >

AVAST

Best Mac Antivirus

KASPERSKY INTERNET SECURITY FOR MAC



9/10

REVIEW >

\$19.99 > Kaspersky

Best Android Antivirus

BITDEFENDER MOBILE SECURITY



8/10

REVIEW >

\$14.99 > Bitdefender

เครื่องมือวิเคราะห์ระดับองค์กร

ซอฟต์แวร์สแกนเครือข่ายและติดตั้งแพตช์ระดับองค์กร เช่น

- GFI LANguard N.S.S.
- eEye Retina N.S.S.
- Microsoft Baseline Security Analyzer (MBSA)

GFI LANguard Network Security Scanner

GFI LanGuard™
Network security scanner and patch management

- พัฒนาโดยบริษัท GFI
- เป็นเครื่องมือที่ได้รับความนิยมมาก เป็นทั้งเครื่องมือสแกนหาช่องโหว่และสามารถติดตั้งแพตช์ได้ด้วย
- สามารถเช็คได้ทั้งระบบปฏิบัติการและแอปพลิเคชัน
- แลนการ์ดจะทำหน้าที่เหมือนแฮ็คเกอร์ และแจ้งเตือนจุดอ่อนให้กับผู้ดูแลระบบแก้ไข
- สามารถติดตั้งแพตช์ให้กับเครื่องไคลเอนต์จำนวนมากได้อย่างง่ายดาย

GFI LANguard Network Security Scanner

GFI LanGuard™

[Home](#)

[Benefits](#)

[Features](#)

[Statistics](#)

[Testimonials](#)

[Try it now](#)

IT and security administrators,
time is your enemy, don't worry,
we can help.

You don't have enough time or resources to meet compliance regulations and secure your network effectively. You struggle to cope with the growing list of essential but repetitive, time consuming tasks you must address daily.

[So what's the solution? GFI LanGuard](#)



GFI LANguard Network Security Scanner

16

GFI LanGuard™

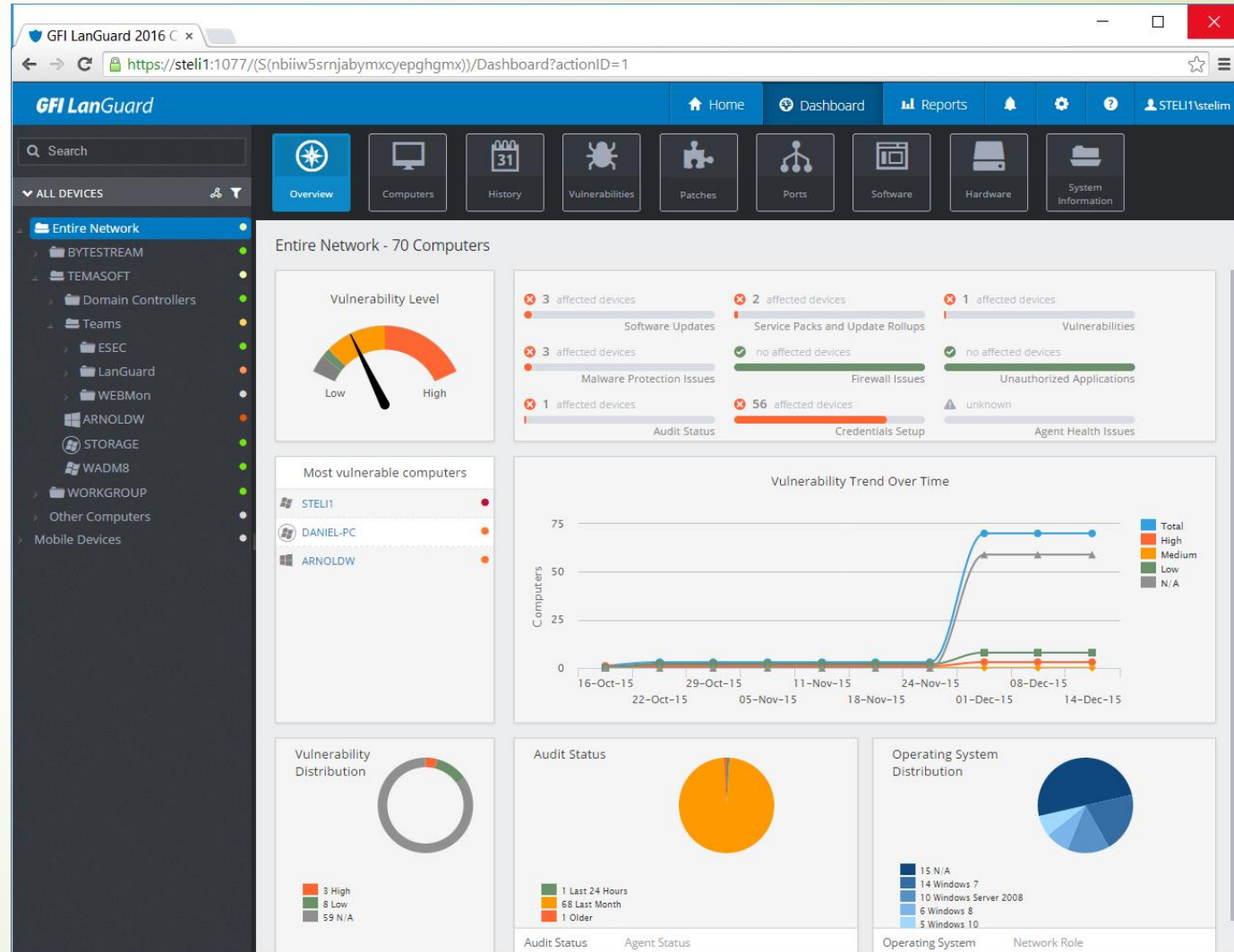
Home Ben



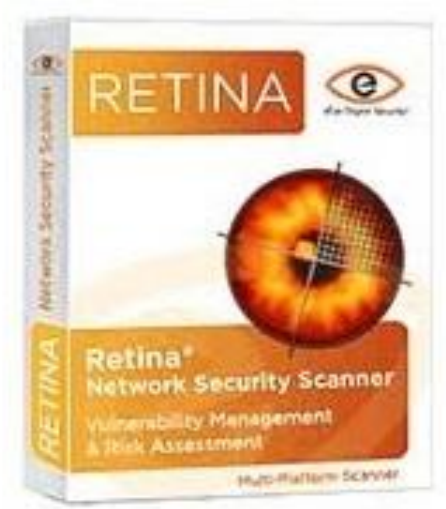
Manage, secure and troubleshoot systems with greater efficiency on more platforms.

GFI LanGuard helps you with:

- ✓ Patch management
- ✓ Vulnerability assessment
- ✓ Network auditing management
- ✓ Compliance
- ✓ BYOD reporting
- ✓ Network discovery
- ✓ Third-party software rollout
- ✓ Port scanning



Retina Network Security Scanner



- เดิมทีพัฒนาโดยบริษัท eEye แต่ในปี 2012 Retina ได้ถูกซื้อโดยบริษัท BeyondTrust
- เป็นเครื่องมือที่ใช้สำหรับสแกนและรายงานผลเท่านั้น ไม่ได้จัดการแพตช์ หากต้องการอัปเดตแพตช์ต้องใช้เครื่องมือเสริม คือ UpdateExpert
- จุดเด่นของ Retina คือสามารถสแกนเครือข่ายได้อย่างรวดเร็ว และ Retina ไม่ได้ทดลองโจมตีจริง ผู้ดูแลระบบจึงมั่นใจได้ว่าการสแกนจะไม่มีผลกระทบต่อระบบ

Retina Network Security Scanner

18

<http://www.beyondtrust.com/Products/RetinaNetworkSecurityScanner/>



TOUR

SOLUTIONS

PRODUCTS

COMPANY

PARTNERS

RESOURCES

REQUEST DEMO

HOME / PRODUCTS / RETINA NETWORK SECURITY SCANNER

RETINA NETWORK SECURITY SCANNER

Network Vulnerability Assessment

Retina Network Security Scanner is the security industry's most respected and validated vulnerability assessment tool. It also serves as the scan engine for Retina CS Enterprise Vulnerability Management.

BUY NOW

REQUEST DEMO

GET QUOTE

FREE TRIAL



Welcome

Scan

Report



Server Administrator



19

Reports

Previous reports



View reports based off of your previous scans. A summary of the most recent report is displayed above. Select any previous report from the right and it will displayed within your preferred PDF viewer.



05/08/2013

USER PROFILE: Government Administrator

WHAT TO SCAN: 127.0.0.1

WHAT TO SCAN FOR: Vulnerabilities

HOW TO SCAN: Anonymous



03/12/2013

USER PROFILE: Workstation Administrator

WHAT TO SCAN: 192.168.1.1 - 192.168.1.254

WHAT TO SCAN FOR: Vulnerabilities

HOW TO SCAN: Anonymous



02/20/2013

USER PROFILE: Workstation Administrator

WHAT TO SCAN: 127.0.0.1

WHAT TO SCAN FOR: Vulnerabilities

HOW TO SCAN: No credentials were stored.



02/20/2013

USER PROFILE: Workstation Administrator

WHAT TO SCAN: 127.0.0.1

WHAT TO SCAN FOR: Vulnerabilities

HOW TO SCAN: No credentials were stored.

Nessus Security Scanner



tenable
network security

- เป็นเครื่องมือที่ช่วยในการค้นหาช่องโหว่ และแนะนำวิธีแก้ปัญหาของระบบก่อนที่แฮคเกอร์จะเข้ามาเจาะโดยใช้ช่องโหว่ดังกล่าว
- เนสส์สเป็นเครื่องมือที่มีความสามารถค่อนข้างมาก แต่ข้อเสียคือมีความซับซ้อนและยากต่อการใช้งานในบางฟีเจอร์ ดังนั้นผู้ใช้เครื่องมือนี้จำเป็นต้องมีความรู้ความสามารถมากพอสมควร
- เป็นซอฟต์แวร์แบบไคลเอนต์เซิร์ฟเวอร์ ซึ่งเป็นระบบรวมศูนย์ ทำให้ผู้ดูแลระบบบริหารจัดการได้ง่ายขึ้น

Nessus





The Nessus Scan Sequence

