บทที่ 3 : การป้องกันการเจาะระบบ Part4

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

การป้องกันการถูกเจาะระบบ

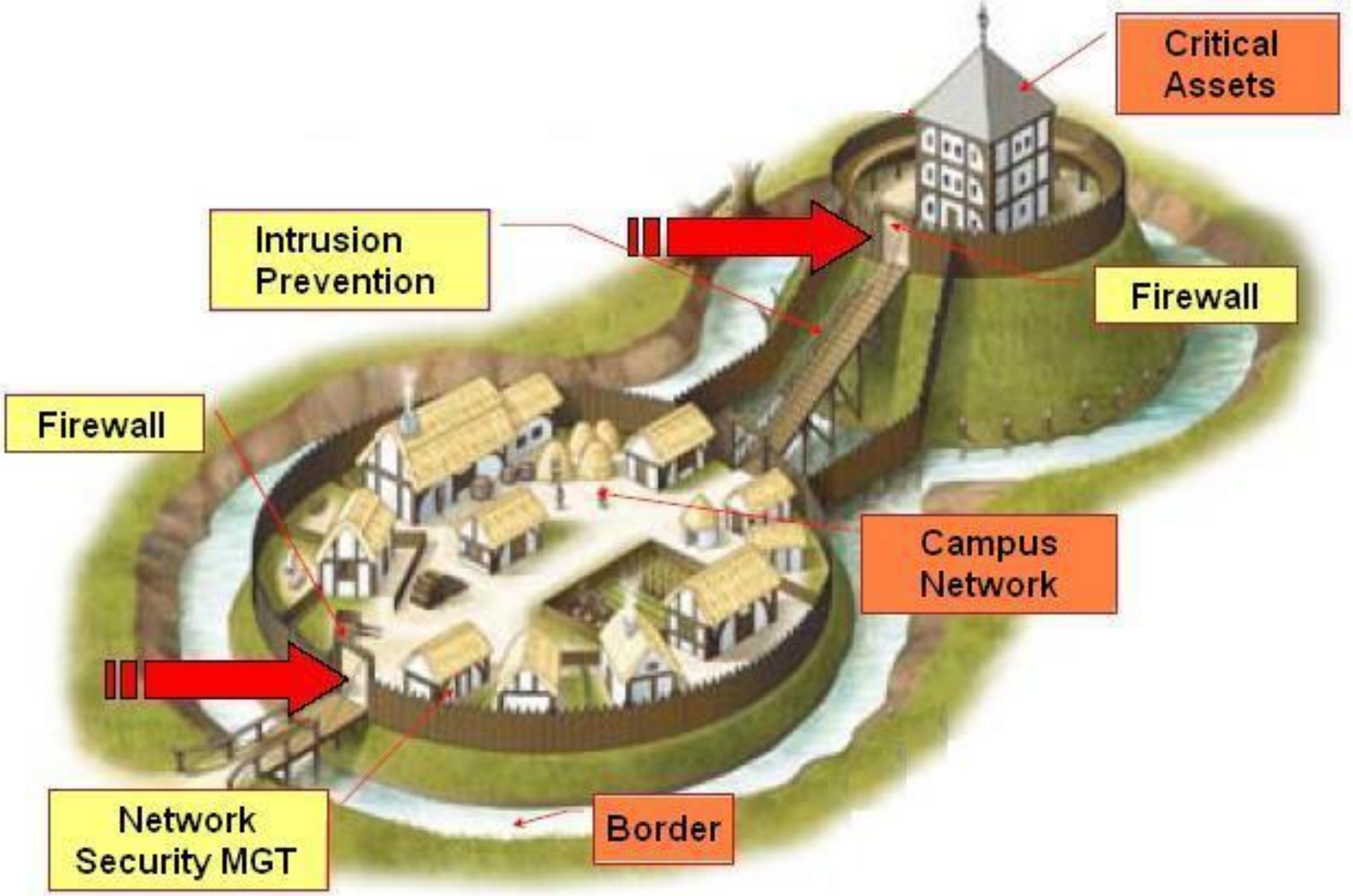
- IDS (Intrusion Detection System)
- IPS (Intrusion Prevention System)
- Firewall
- Antivirus
- เครื่องมือวิเคราะห์ระดับองค์กร
  - GFI LANguard N.S.S. (Network Security Scanner)
  - eEye Retina N.S.S.
  - Nessus Security Scanner

การป้องกันการถูกเจาะระบบ

- วิธีพื้นฐานคือการสแกนหาจุดอ่อนในระบบ และอัพเดตแพตช์เพื่อปิดช่องโหว่นั้นๆ
- ผู้ดูแลระบบต้องรู้ว่าเครือข่ายมีช่องโหว่ตรงไหนบ้าง การใช้เครื่องมือด้านการรักษาความปลอดภัยเป็นวิธีที่ง่ายและได้ผลที่สุด
- การสแกนควรทำทั้งจากภายในและภายนอกเครือข่าย ทั้งในรูปแบบมีสิทธิ์และไม่มีสิทธิ์เข้าถึงระบบ
- หลังจากที่สแกนแล้วต้องทำการอัพเดตแพตช์ โดยปกติแล้วเครื่องมือสำหรับใช้สแกนช่องโหว่ส่วนใหญ่จะสามารถอัพเดตแพตช์ได้อยู่แล้ว
- ***การไม่อัพเดตแพตช์เป็นการเพิ่มความเสี่ยงให้สูงยิ่งขึ้น***

การป้องกันการถูกเจาะระบบ

- การติดตั้งแพตช์ หรือบางทีเรียกว่าฮ็อตฟิกส์ (Hot Fixes) เป็นสิ่งสำคัญมาก แต่ในระดับองค์กรควรมีการสำรองข้อมูลก่อนการติดตั้งแพตช์ เพื่อป้องกันผลกระทบที่อาจเกิดขึ้นกับระบบ
- ที่สำคัญควรมีการติดตามข่าวสารด้านความปลอดภัยอยู่เสมอ

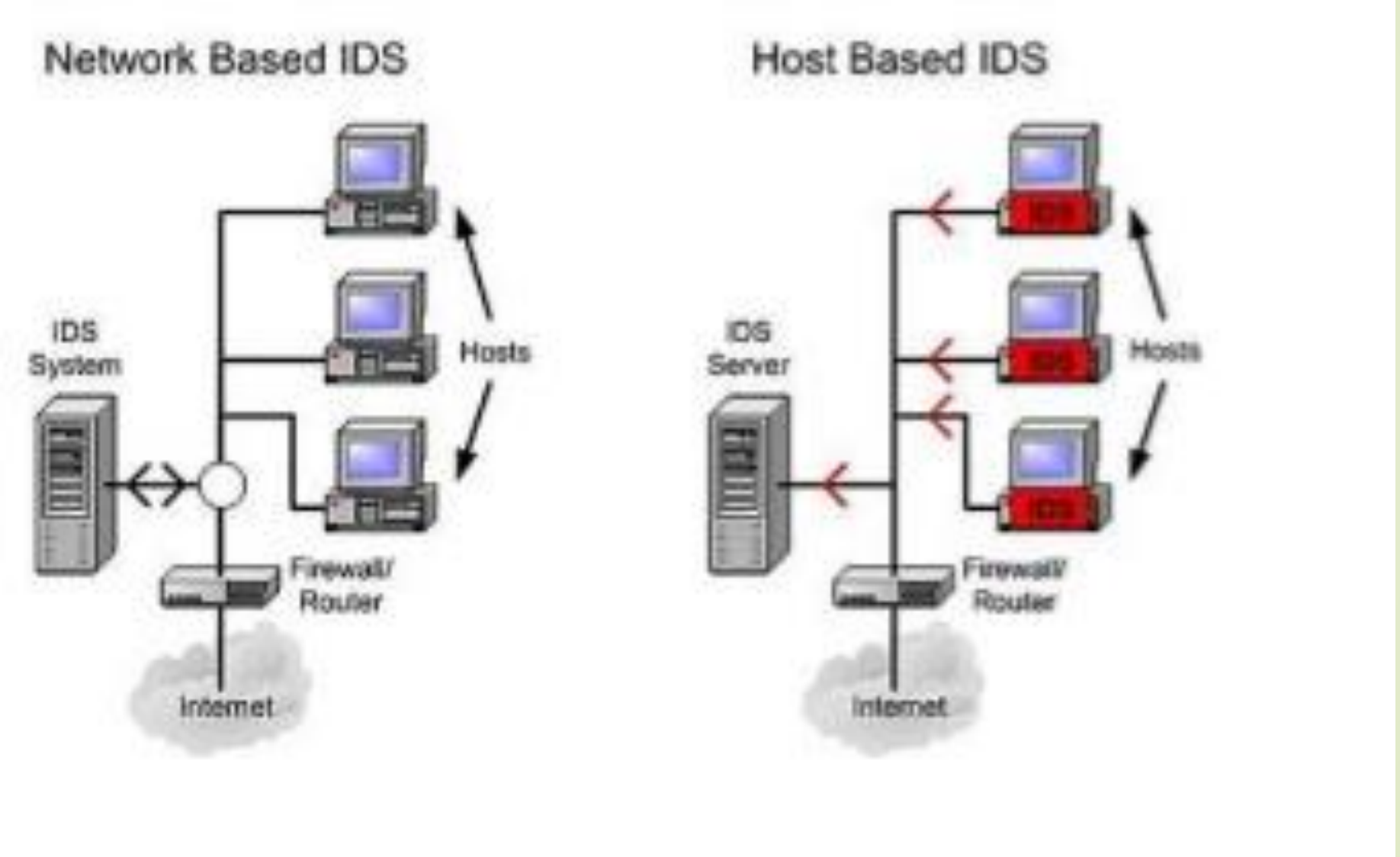

Critical Assets
Intrusion Prevention
Firewall
Firewall
Campus Network
Network Security MGT
Border

ระบบตรวจจับการบุกรุก

Intrusion Detection System (IDS)

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

ประเภทของ IDS



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 MxAfee, Trend Micro, Cisco
- * ปัจจุบันระบบนี้ได้ถูกรวมเข้ากับผลิตภัณฑ์ Next-Generation Firewall (NGFW) ทำให้มีความนิยมลดลงมาก

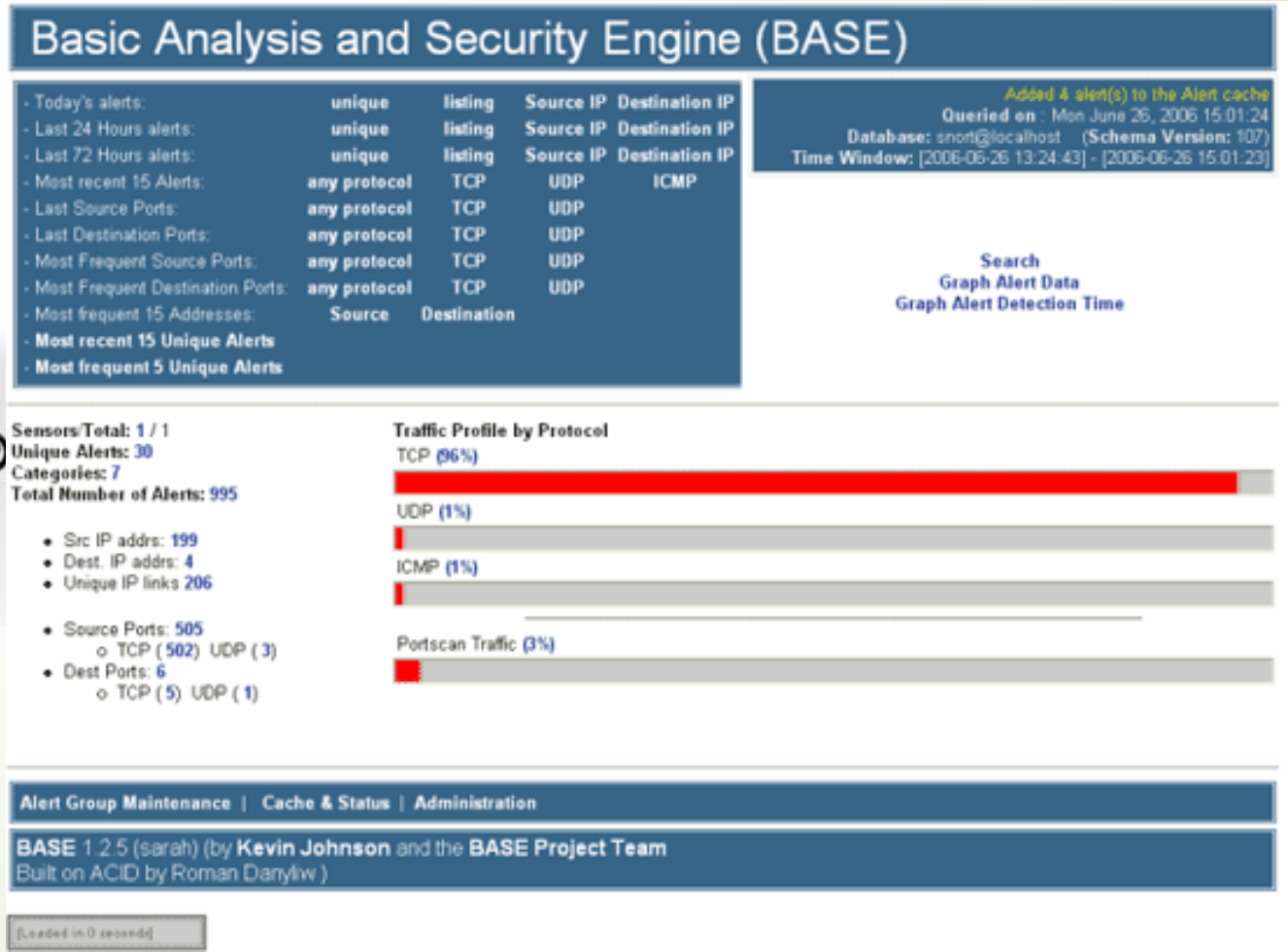
*(ข้อมูลจาก Gartner ปี 2018)

SNORT

The Opensource IDPS

Download

https://snort.org/



Firewall

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

Antivirus

- เป็นโปรแกรมสามัญประจำเครื่องและเครือข่ายที่ใช้ป้องกัน Malware ที่อาจจะถูกฝังลงสู่คอมพิวเตอร์
- Antivirus จะใช้งานได้เป็นอย่างดีหากผู้ใช้มีการอัพเดตอยู่เสมอๆ
- เป็นสิ่งพื้นฐานที่ช่วยลดความเสี่ยงจากการถูกโจมตีได้ไม่น้อย
- จะเรียนอย่างละเอียดอีกครั้งหลังสอบกลางภาค

tom's guide PRODUCT REVIEWS DEALS HOW TO FORUM

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

Ref : https://www.tomsguide.com/us/best-antivirus,review-2588.html

เครื่องมือวิเคราะห์ระดับองค์กร

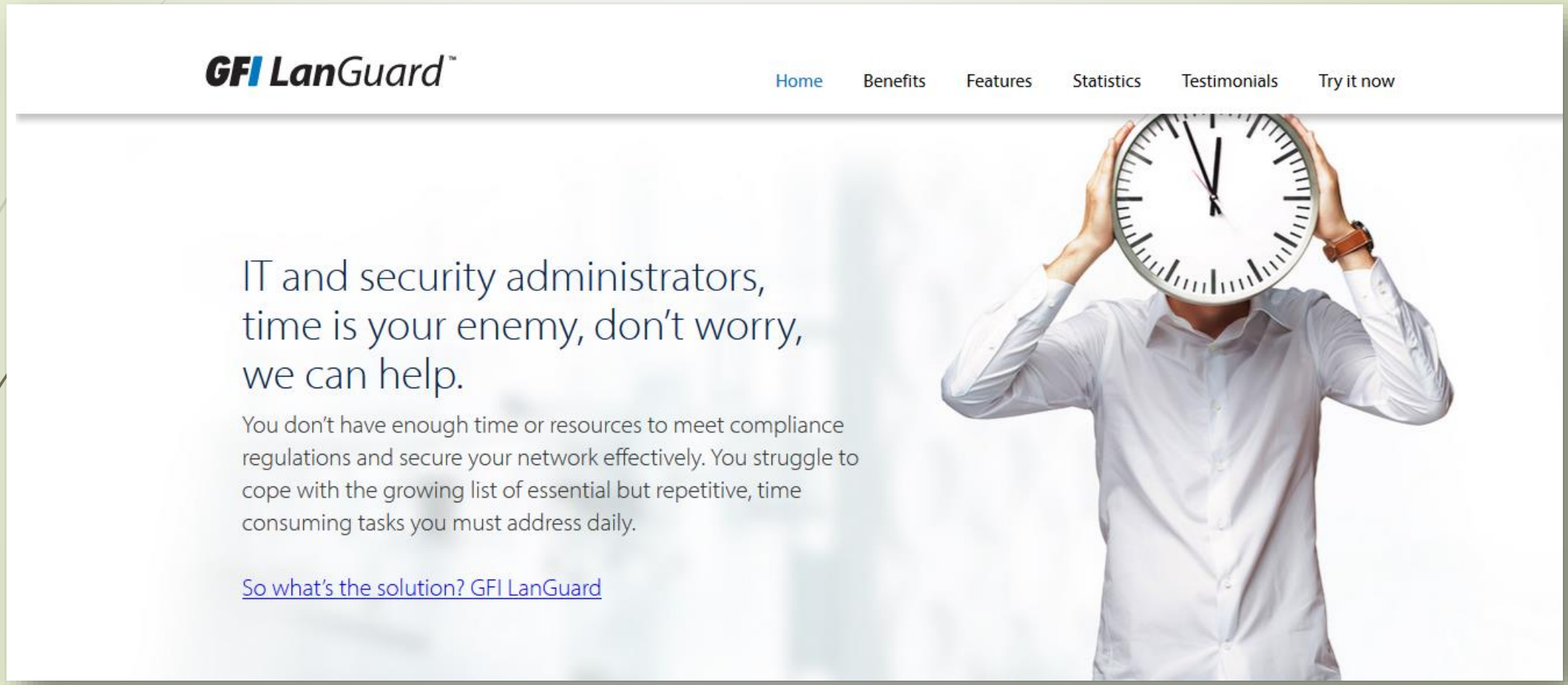
ซอฟต์แวร์สแกนเครือข่ายและติดตั้งแพตช์ระดับองค์กร เช่น

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

GFI LANguard Network Security Scanner

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

GFI LANguard Network Security Scanner



https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard

GFI LANguard Network Security Scanner

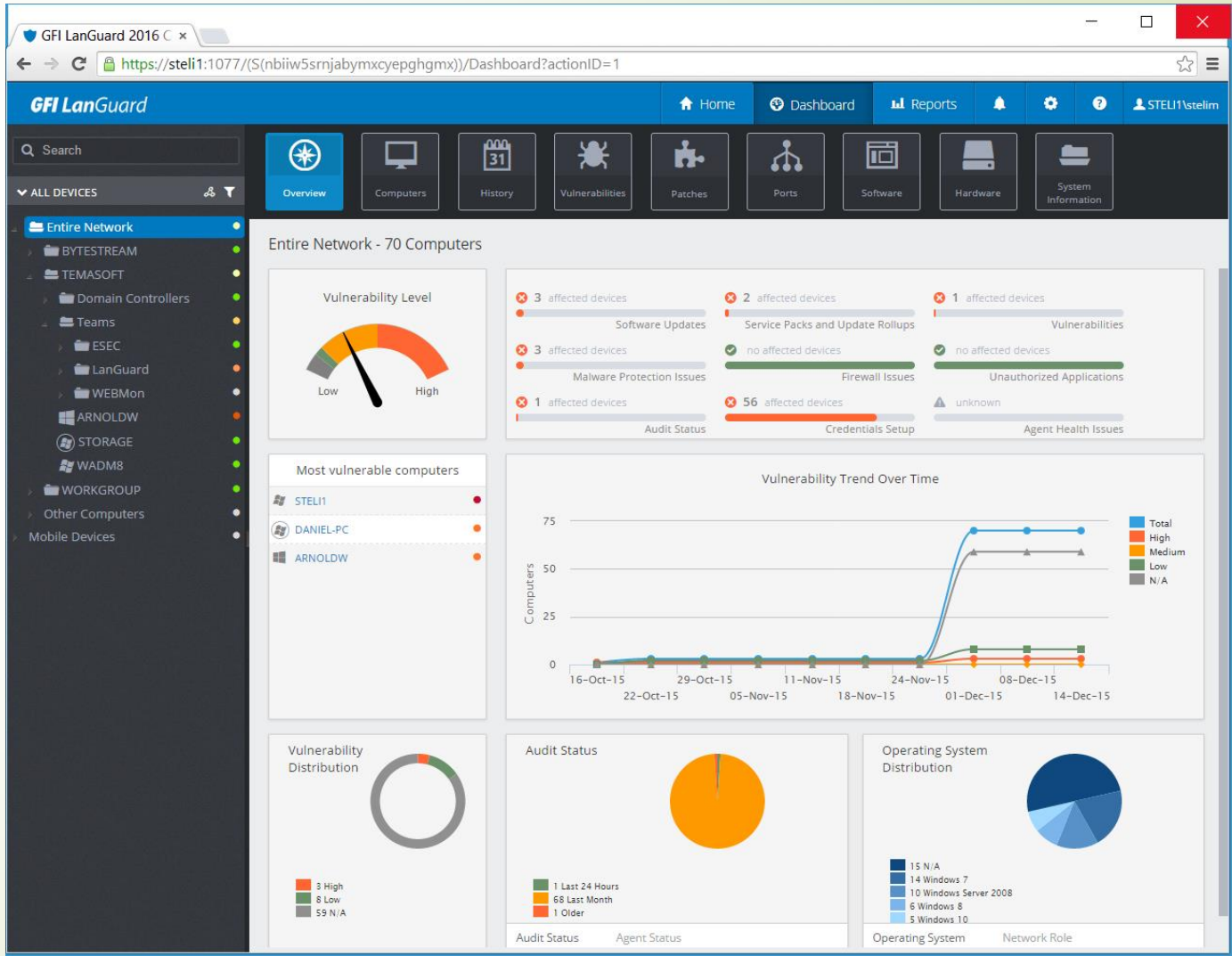
GFI LanGuard™

Home Ben

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

GFI LanGuard helps you with:

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

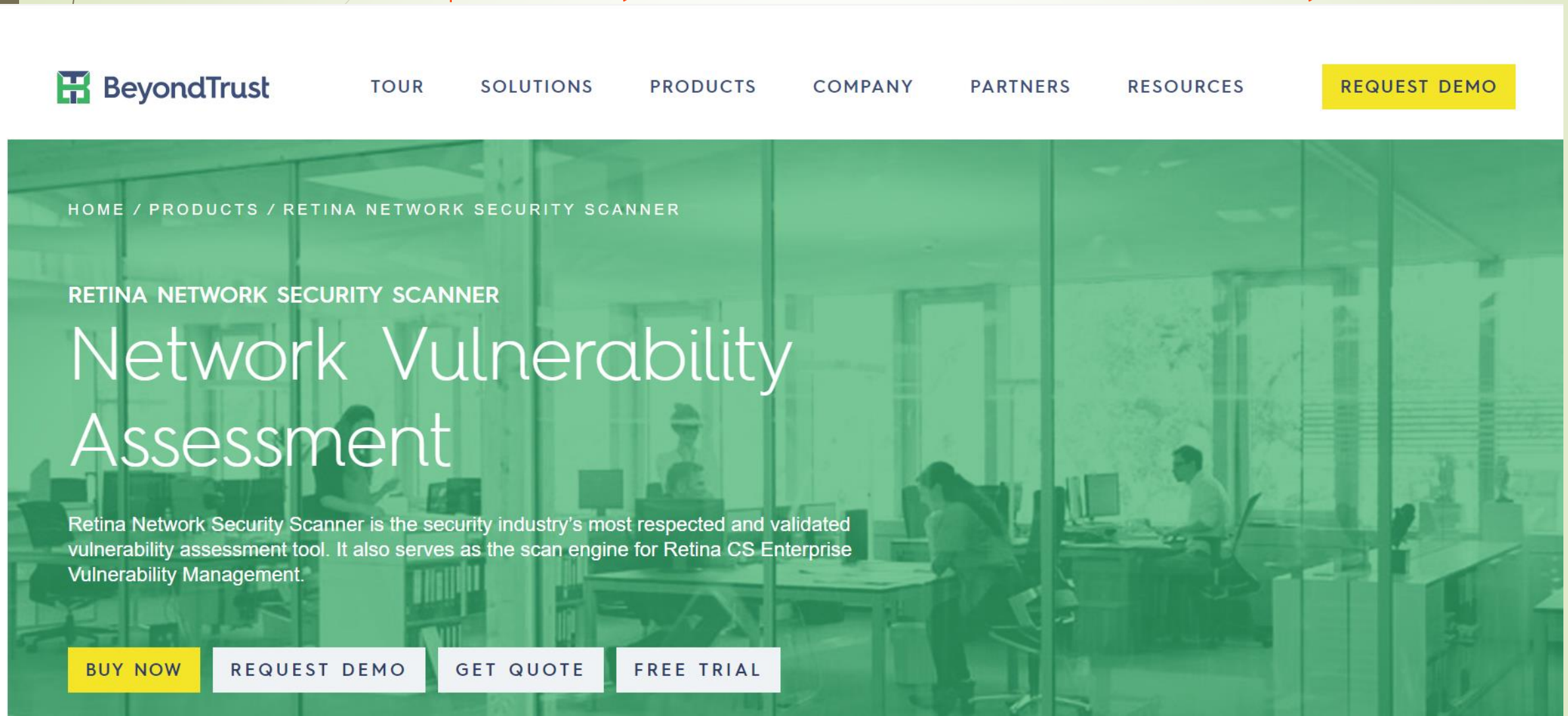


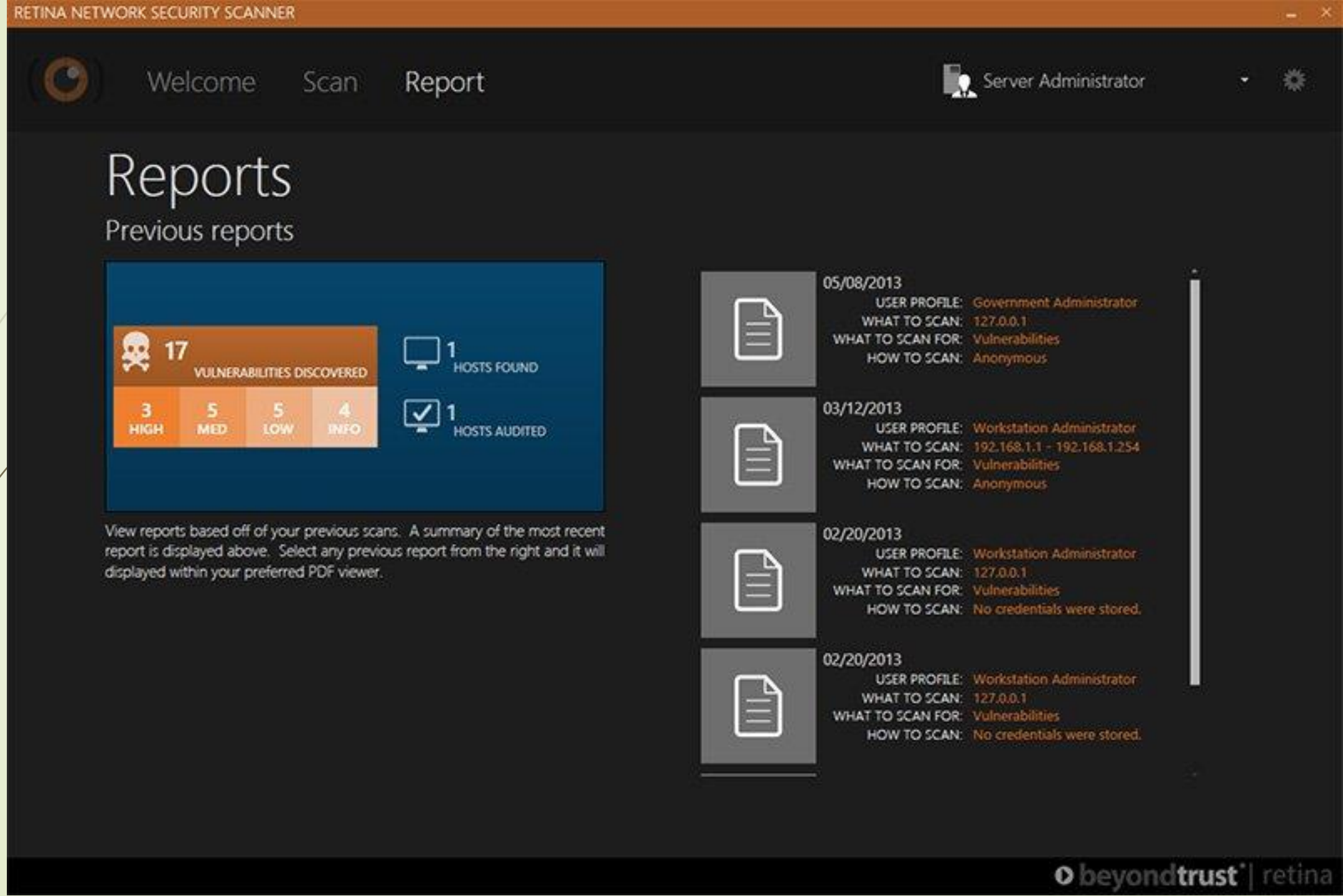
Retina Network Security Scanner

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

Retina Network Security Scanner

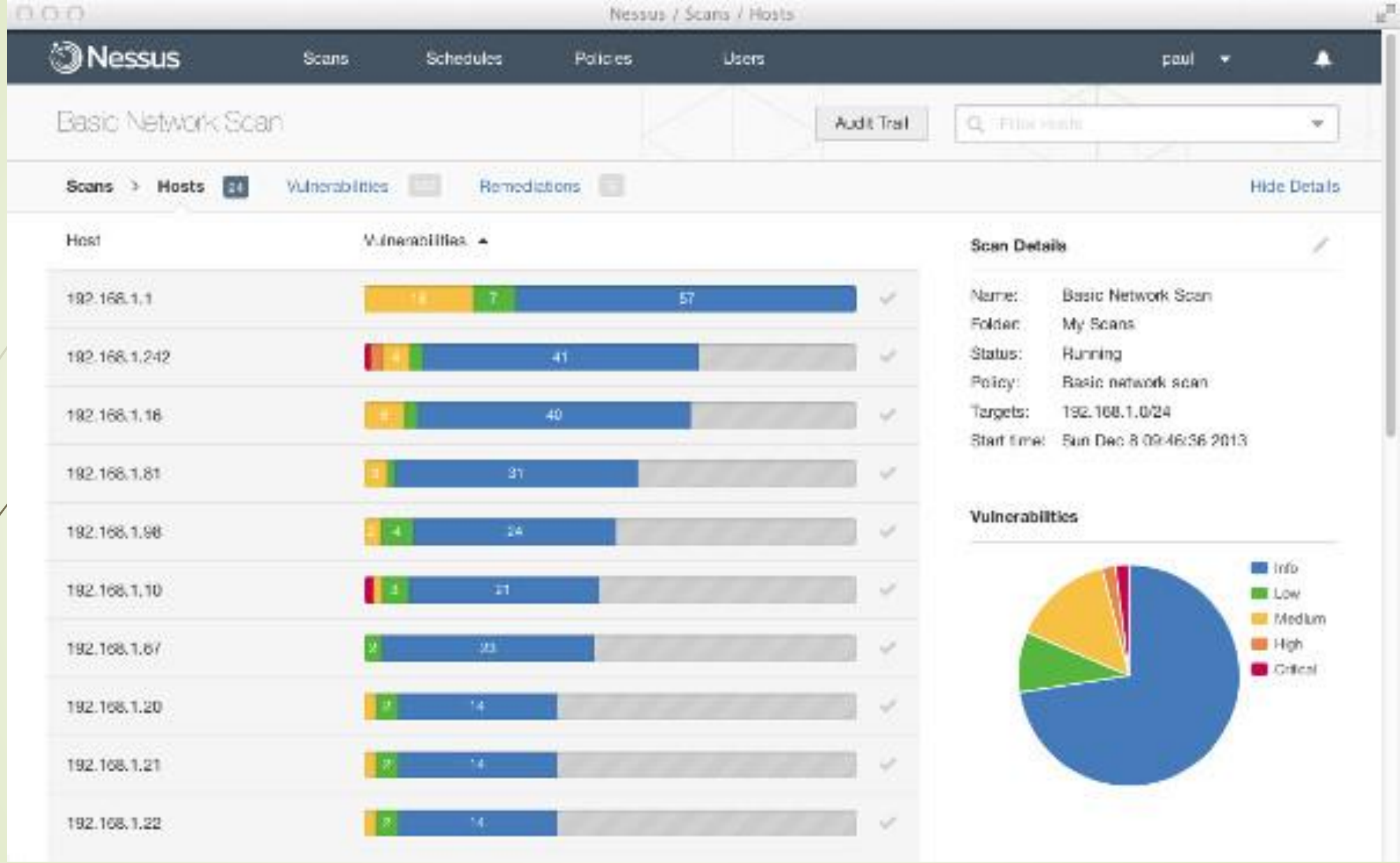
http://www.beyondtrust.com/Products/RetinaNetworkSecurityScanner/




RETINA NETWORK SECURITY SCANNER
Welcome
Scan
Report
Server Administrator
Reports
Previous reports
17
VULNERABILITIES DISCOVERED
3
HIGH
5
MED
5
LOW
4
INFO
1
HOSTS FOUND
1
HOSTS AUDITED
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.
beyondtrust | retina

Nessus Security Scanner

- เป็นเครื่องมือที่ช่วยในการค้นหาช่องโหว่ และแนะนำวิธีแก้ปัญหาของระบบก่อนที่แฮคเกอร์จะเข้ามาเจาะโดยใช้ช่องโหว่ดังกล่าว
- เนสสัสเป็นเครื่องมือที่มีความสามารถค่อนข้างมาก แต่ข้อเสียคือมีความซับซ้อนและยากต่อการใช้งานในบางฟีเจอร์ ดังนั้นผู้ใช้เครื่องมือนี้จำเป็นต้องมีความรู้ความสามารถมากพอสมควร
- เป็นซอฟต์แวร์แบบไคลเอนต์เซิร์ฟเวอร์ ซึ่งเป็นระบบรวมศูนย์ทำให้ผู้ดูแลระบบบริหารจัดการได้ง่ายขึ้น



https://www.tenable.com/products/nessus-vulnerability-scanner

The Nessus Scan Sequence