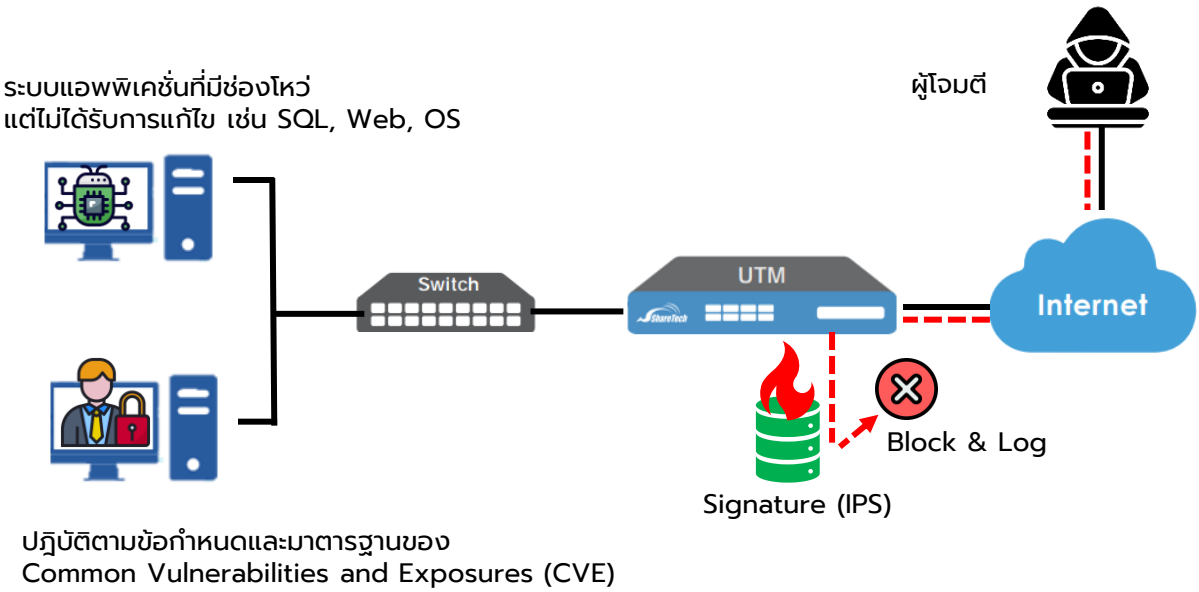
IPS (Intrusion Prevention System)
การป้องกันการโจมตีทางไซเบอร์

www.sharetechthai.com
rung@nit.co.th



IPS (Intrusion Prevention System) การป้องกันการโจมตีทางไซเบอร์

IPS คือเทคโนโลยีที่ป้องกันการการบุกรุก และตรวจสอบข้อมูลโดยเปรียบเทียบกับฐานข้อมูลทางด้านความเสี่ยง (Signature) อีกทั้งระบุช่องโหว่ที่อาจเกิดขึ้น , พฤติกรรมการโจมตีเครือข่าย รวมทั้งระบบแอพพิเคชั่นที่มีช่องโหว่ แต่ไม่ได้รับการแก้ไข ซึ่งผู้โจมตีอาจจะใช้ประโยชน์จาก ช่องโหว่ เพื่อขัดขวางการทำงานของ เครือข่าย และแอพพิเคชั่น

ดังนั้น บทบาทหลักของ IPS คือการเสริมความปลอดภัยไฟร์วอลล์ โดยปกกันช่องโหว่ที่ไฟร์วอลล์อาจไม่สามารถปิดกั้นได้อย่างสมบูรณ์ และช่วยให้มั่นใจในความปลอดภัยของระบบ จากผ่านการตรวจสอบแบบเรียลไทม์ และการสกัดสกัดกั้นความพยายามเข้าถึงที่เป็นอันตราย เช่น

- การโจมตีแบบ Brute-force
- การโจมตีแบบ SQL Injection
- การโจมตีแบบ XSS Attack
- การรับส่งข้อมูลที่เป็นอันตราย DOS, Trojan, Malware
- ป้องกันได้บนเลเยอร์ (OSI) ตั้งแต่เลเยอร์ 3 ถึงเลเยอร์ 7

High Risk (26303)
ET SHELLCODE Bindshell2 Decoder Shellcode (UDP)
ET SHELLCODE Rothenburg Shellcode
ET ATTACK_RESPONSE Hostile FTP Server Banner (StnyFtpd)
ET ATTACK_RESPONSE Hostile FTP Server Banner (Reptile)
ET ATTACK_RESPONSE Hostile FTP Server Banner (Bot Server)
ET ATTACK_RESPONSE Unusual FTP Server Banner (fuckFtpd)
ET ATTACK_RESPONSE Unusual FTP Server Banner (NzmxFtpd)
ET WEB_CLIENT Possible Microsoft Internet Explorer URI Validation Remote Code Execution Attempt
ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (1)
ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (2)