Cyber Attack Pattern Analysis By Tshark

หลักการและเหตุผล

ปัจจุบันเครือข่ายคอมพิวเตอร์ถูกใช้งานอย่างแพร่หลาย ทั้งในการศึกษา การทำงาน และบริการออนไลน์ ทำให้เกิดความเสี่ยงจากภัยคุกคามไซเบอร์ เช่น Port Scanning , ICMP Flood , SYN Flood , UDP Flood

การโจมตีเหล่านี้ส่งผลให้เครือข่ายล่ม ข้อมูลรั่วไหล หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต จึงจำเป็นต้องมี ระบบตรวจจับการบุกรุก (IDS) เพื่อตรวจจับพฤติกรรมผิดปกติและแจ้งเตือนผู้ดูแลระบบ

โครงงานนี้จึงจัดทำขึ้นเพื่อพัฒนา IDS แบบง่ายด้วย Tshark + Python บน Linux เพื่อวิเคราะห์ packet และตรวจจับการโจมตีพื้นฐานในเครือข่ายจำลอง

วัตถุประสงค์ของโครงงาน

1. เพื่อศึกษาแนวคิดและการทำงานของ Intrusion Detection System (IDS)
2. เพื่อพัฒนาระบบตรวจจับการโจมตีเครือข่ายโดยใช้ Tshark และ Python
3. เพื่อจำลองการโจมตีเครือข่ายในสภาพแวดล้อมทดลอง
4. เพื่อทดสอบประสิทธิภาพของระบบ IDS ที่พัฒนา

ขอบเขต

1. ระบบ IDS จะทำงานบนระบบปฏิบัติการ Linux
2. ใช้ Tshark ในการดักจับ packet ในเครือข่าย
3. ใช้ Python ในการวิเคราะห์ข้อมูล packet
4. การโจมตีที่ใช้ในการทดสอบประกอบด้วย
   - ICMP Flood Attack
   - SYN Flood Attack
   - UDP Flood Attack
   - Port Scanning Attack
5. ใช้เครือข่ายจำลองใน Virtual Machine

เครื่องมือที่ใช้

- Kali Linux
- Python
- hping3
- Ubuntu Linux
- Tshark
- nmap

วิธีการใช้งาน

1. ติดตั้งระบบ IDS บนเครื่อง Kali Linux
2. ใช้เครื่องมือ Tshark เพื่อดักจับ packet จาก network interface
3. โปรแกรม Python จะทำการวิเคราะห์ packet ที่ถูกจับมา
4. หากพบพฤติกรรมที่เข้าข่ายการโจมตี เช่น
   - จำนวน packet สูงผิดปกติ
   - การสแกนหลาย port

ระบบจะทำการแจ้งเตือนผู้ใช้งาน

อ้างอิง

Wireshark Foundation. (2024). Wireshark user guide. Retrieved from https://www.wireshark.org/docs/

Wireshark Foundation. (2024). TShark documentation. Retrieved from https://www.wireshark.org/docs/man-pages/tshark.html

สรุปผลการดำ เนินงาน

ระบบ IDS ที่พัฒนาขึ้นสามารถตรวจจับการโจมตีเบื้องต้นได้อย่างมีประสิทธิภาพในสภาพแวดล้อมจำลอง แต่ยังไม่รองรับการโจมตีขั้นสูง เช่น APT หรือ Zero-day และยังไม่สามารถป้องกันการโจมตี (ไม่มีระบบ IPS)

Group10

นายกนก รัตตสนธิกุล 673380200-6

นายจิรภัทร โตรักษา 673380207-2

นายวัชระ ประสาทซัย 673380242-0

นางสาวโศภิสรา ศาลางาม 67338026I-6

นางสาวธนัชพร สีสุทะ 673380219-5

นายธีรภัทร เสริมศรี 673380220-0

นายอภิรักษ์ สุริยะศรี 663380637-6

เสนอ ศ. ดร.จักรชัย โสอินทร์

ผศ. ดร.สาธิต กระเวนกิจ

อ. ดร.ชาติชาย ปุณริบูรณ์

Information and Communication Technology Security

หลักสูตร เทคโนโลยีสารสนเทศ

คณะ วิทยาลัยการคอมพิวเตอร์

พ.ศ.2569


```
═══ Traffic Analysis ═══
No attack detected

Traffic Summary
192.168.56.1 | Total:1 ICMP:0 SYN:0 UDP:1 Ports:0

═══ Traffic Analysis ═══
⚠ ICMP Flood detected from 192.168.56.102
⚠ ICMP Flood detected from 192.168.56.1

Traffic Summary
192.168.56.102 | Total:34023 ICMP:34022 SYN:0 UDP:0 Ports:0
192.168.56.100 | Total:1 ICMP:0 SYN:0 UDP:0 Ports:0
192.168.56.1 | Total:34024 ICMP:34024 SYN:0 UDP:0 Ports:0

═══ Traffic Analysis ═══
⚠ ICMP Flood detected from 192.168.56.102
⚠ ICMP Flood detected from 192.168.56.1

Traffic Summary
192.168.56.102 | Total:47216 ICMP:47216 SYN:0 UDP:0 Ports:0
192.168.56.1 | Total:47213 ICMP:47212 SYN:0 UDP:0 Ports:0

═══ Traffic Analysis ═══
⚠ UDP Flood detected from 192.168.56.1

Traffic Summary
192.168.56.1 | Total:14404 ICMP:0 SYN:0 UDP:14400 Ports:0
192.168.56.102,192.168.56.1 | Total:6 ICMP:6 SYN:0 UDP:0 Ports:0

═══ Traffic Analysis ═══
No attack detected

Traffic Summary
```