Botnet Simulation and Detection System

CP422031 Introduction to Cybersecurity
สาขา ความมั่นคงปลอดภัยไซเบอร์ SECTION 3

ปัญหา

ปัจจุบันภัยคุกคามประเภท Botnet และ DDoS Attack มีจำนวนเพิ่มขึ้นอย่างต่อเนื่อง โดยผู้โจมตีผ่าน Command & Control (C2) Server เพื่อโจมตีเป้าหมายพร้อมกันองค์กรจำนวนมากยังขาดความเข้าใจ จึงจำเป็นต้องมีระบบจำลองเพื่อศึกษากระบวนการโจมตีและแนวทางป้องกันอย่างปลอดภัยในสภาพแวดล้อมปิด

วัตถุประสงค์

จำลองวงจรการทำงานของเครือข่ายบอทเน็ต (Botnet Lifecycle) ตั้งแต่การแพร่กระจาย การควบคุม ไปจนถึงการโจมตีแบบ DDoS และศึกษาแนวทางการตั้งรับด้วยระบบตรวจจับการบุกรุกเครือข่าย (Network IDS)

ขอบเขตการศึกษา

โครงการดำเนินการภายในเครือข่ายเสมือนแบบปิด (Virtual Lab) ใช้เครื่องจำลองทั้งหมด 6 เครื่อง ครอบคลุมฝั่งผู้โจมตี เหยื่อ และระบบป้องกัน โดยจำกัดการทดสอบเฉพาะการโจมตีแบบ HTTP Flood ภายในแลปเท่านั้น

EXAMPLE

วิธีการดำเนินงาน

Weaponization Phase
- ใช้ msfvenom สร้างไฟล์ reverse meterpreter payload (.exe)

Delivery Phase
- สร้างเว็บไซต์ Phishing หลอกดาวน์โหลดไฟล์

Execution Phase
- เหยื่อรันไฟล์
- สร้าง Reverse TCP กลับไป C2
- ได้ Meterpreter Session

Botnet Control
- ผู้โจมตีสั่ง Bot ทั้ง 2 เครื่องทำ HTTP Flood ไปยัง Target

Detection Phase
- Snort IDS ตรวจจับทราฟฟิกผิดปกติ
- แสดง Alert แบบ Real-time

เครื่องมือ / ซอฟแวร์

- ฝั่งโจมตี

Kali Linux,MetasploitFramework, msfvenom,Meterpreter
- ฝั่งแพร่กระจาย

Ubuntu Server,Docker,Nginx (Phishing Web Server)
- ฝั่งเหยื่อ

Windows 10 Pro (2 เครื่อง)
- ฝั่งป้องกัน

Ubuntu Server,Snort IDS,Nginx (Target Web Server)
- Virtualization

VirtualBox / VMware (ขึ้นอยู่กับที่ใช้)

อ้างอิง

Mirai เป็นมัลแวร์ Botnet ที่มีชื่อเสียงซึ่งใช้โจมตี DDoS โดยเปลี่ยนอุปกรณ์ IoT ให้กลายเป็น Bot ภายใต้การควบคุมของ C2 Server โครงการนี้นำ แนวคิดโครงสร้าง Botnet ของ Mirai มาใช้เป็นต้นแบบ ในการจำลองระบบภายใน Lab

ฟังก์ชัน

- สร้างและแจกจ่าย Payload
- รับ Reverse Connection จากเหยื่อ
- ควบคุมเครื่องเหยื่อหลายเครื่องพร้อมกัน (Botnet Behavior)
- สั่งโจมตีแบบ HTTP Flood
- วิเคราะห์แพ็กเกตเครือข่าย
- แจ้งเตือนเมื่อพบพฤติกรรมผิดปกติ

สรุปผล

- จากการทดลองพบว่า:
- สามารถจำลองโครงสร้าง Botnet ได้สำเร็จ
- เครื่องเหยื่อสามารถเชื่อมต่อกลับ C2 ได้พร้อมกันหลายเครื่อง
- สามารถสั่งโจมตีแบบ HTTP Flood พร้อมกันได้
- ระบบ Snort IDS สามารถตรวจจับทราฟฟิกผิดปกติและแจ้งเตือนได้แบบ Real-time
- แสดงให้เห็นความสำคัญของ Network Monitoring ในการป้องกัน DDoS
- โปรเจคนี้ช่วยให้เข้าใจโครงสร้าง Botnet และกระบวนการตรวจจับเชิงเครือข่ายได้อย่างเป็นรูปธรรมในสภาพแวดล้อมที่ปลอดภัย

GROUP 6
นายคงกระพัน ลือชา รหัสนักศึกษา 673380366-2
นายจีราวัฒน์ วงษ์คำจันทร์ รหัสนักศึกษา 673380367-0
นายสหพล พรหมศร รหัสนักศึกษา 673380383-2
นายสิริภัทร พิมทอง รหัสนักศึกษา 673380384-0
นายชิษณุพงศ์ จิตมาลย์ รหัสนักศึกษา 673380541-0
นายนันทสิทธิ์ ศรีลับแล รหัสนักศึกษา 673380547-8
นายเสฏฐวุฒิ บุญสถาพร รหัสนักศึกษา 673380570-3

เสนอ
ศ.ดร.จักรชัย โสอินทร์
ผศ.ดร.สาธิต กระเวนกิจ
อ.ชาติชาย ปุณริบูรณ์

COLLEGE OF COMPUTING
KHON KAEN UNIVERSITY