Hacker Port Scan Detection System

CP422031 INTRODUCTION TO CYBERSECURITY

อาจารยทีปรึกษา ศ.ดร.จักรชัย โสอินทร และ ผศ.ดร.สาธิต กระเวนกิจ
อ.ดร.ชาติชาย ปุณริบูรณ์

หลักการและเหตุผล

- การโจมตีระบบเครือข่ายมักเริ่มต้นด้วยการสแกนพอร์ต (Port Scanning)
- ผู้โจมตีใช้เครื่องมือ เช่น Nmap เพื่อค้นหา Port
- ที่เปิดอยู่ในระบบ
- หากไม่มีระบบตรวจจับผู้ดูแลระบบจะไม่ทราบว่ากำลังถูกสแกน
- การสแกนพอร์ตอาจนำไปสู่การค้นหาช่องโหว่และการโจมตีระบบ
- ดังนั้นจึงพัฒนาระบบ Detectorและ Auto Block IP เพื่อป้องกันภัยคุกคาม

วัตถุประสงค์

- พัฒนาระบบตรวจจับการ Port Scanning
- แสดงผลผ่าน Web Dashboard
- แจ้งเตือนผู้ดูแลระบบผ่าน Email
- บล็อก IP ของผู้โจมตีแบบ Automatic
- เก็บข้อมูลการโจมตีไว้เป็น Log

ขอบเขตการศึกษา

- สามารถตรวจจับการสแกนพอร์ตจากเครื่องโจมตีได้
- แสดงผลการโจมตีผ่านหน้า Web Application
- แจ้งเตือนผ่าน Email
- บล็อก IP Address อัตโนมัติ

แนวทางที่ใช้

1. ระบบทำงานโดย
2. ดักจับ Network Traffic
3. วิเคราะห์ Packet ที่เข้ามาในระบบ
4. ตรวจสอบจำนวน Port ที่ถูก Scan
5. หากมีการ Scan หลาย Port จาก IP เดียว
6. ระบบจะทำการ
   - แจ้งเตือนผ่านหน้าเว็บ
   - ส่ง Email แจ้งเตือน
   - บล็อก IP ของผู้โจมตีทันที

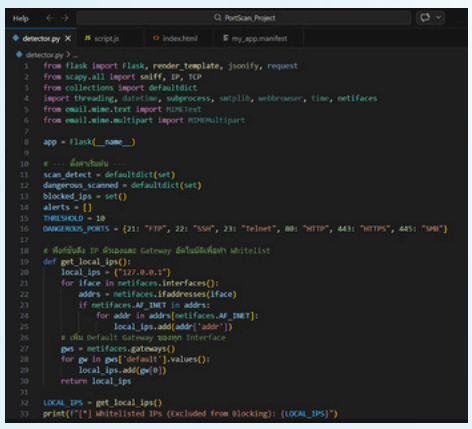
สรุปผล

ระบบสามารถตรวจจับพฤติกรรมการ Port Scan ได้แบบ Real-Time
เมื่อมีผู้โจมตีทำการ Scan ระบบจะ

1. ตรวจจับการ Scan
2. แสดงผลบน Web Dashboard
3. บล็อก IP ของผู้โจมตี
4. ส่ง Email แจ้งเตือนผู้ดูแลระบบ

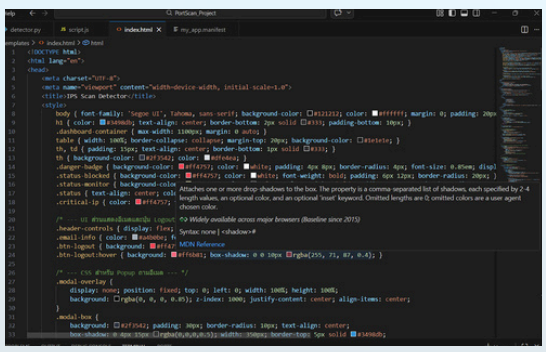
เครื่องมือที่ใช้

1. Python
2. Flask (Web Application)
3. Scapy (Packet Sniffing)
4. SMTP (Email Notification)
5. Linux / Windows Environment
6. เครื่องมือทดสอบการโจมตี
   - Kali Linux
   - Nmap



```python
from flask import Flask, render_template, jsonify, request
from scapy.all import sniff, IP, TCP
from collections import defaultdict
import threading, datetime, subprocess, smtplib, webbrowser, time, netifaces
from email.mime.text import MIMEText
from email.mime.multipart import MIMEMultipart

app = Flask(__name__)

# --- ตั้งค่าเริ่มต้น ---
scan_detect = defaultdict(set)
dangerous_scanned = defaultdict(set)
blocked_ips = set()
alerts = []
THRESHOLD = 10
DANGEROUS_PORTS = {21: "FTP", 22: "SSH", 23: "Telnet", 80: "HTTP", 443: "HTTPS", 445: "SMB"}

# ที่อยู่ที่ไม่ถือว่าเป็นผู้โจมตี (เพิ่มได้ตามต้องการ)
def get_local_ips():
    local_ips = {"127.0.0.1"}
    for iface in netifaces.interfaces():
        addrs = netifaces.ifaddresses(iface)
        if netifaces.AF_INET in addrs:
            for addr in addrs[netifaces.AF_INET]:
                local_ips.add(addr['addr'])
    # เพิ่ม Default Gateway ของทุก Interface
    gws = netifaces.gateways()
    for gw in gws['default'].values():
        local_ips.add(gw[0])
    return local_ips

LOCAL_IPS = get_local_ips()
print(f"[*] Whitelisted IPs (Excluded from Blocking): {LOCAL_IPS}")
```

```javascript
// ฟังก์ชันสำหรับส่งคำสั่ง Logout ไปยัง Server
function logout() {
    const email = localStorage.getItem('admin_email');

    if (!email) {
        alert("ไม่พบอีเมลที่เข้าสู่ระบบไว้");
        return;
    }

    fetch('/api/logout_email', {
        method: 'POST',
        headers: { 'Content-Type': 'application/json' },
        body: JSON.stringify({ email: email })
    })
    .then(response => response.json())
    .then(data => {
        if (data.status === 'success') {
            // ลบข้อมูลอีเมลออกจาก Browser ของผู้ใช้
            localStorage.removeItem('admin_email');
            alert('Logout เรียบร้อยแล้ว!');
            // รีโหลดหน้าเพื่อให้ UI กลับไปแสดงแบบเริ่มต้น
            location.reload();
        } else {
            alert('เกิดข้อผิดพลาด: ' + data.message);
        }
    })
    .catch(error => console.error('Error:', error));
}
```



สมาชิก
นายปริณ ปริบุญณะ 673380548-6
นายกิจภานันท์ นามโยธา 673380365-4
นายพร้อมพงศ์ ศรีสวาสดิ์ 673380552-5
นายภูมิพัฒน์ วรรณชัย 673380560-6
นายฉันทวัฒน์ ชานนท์ 673380538-9
นายปองพล หอระตะ 673380549-4