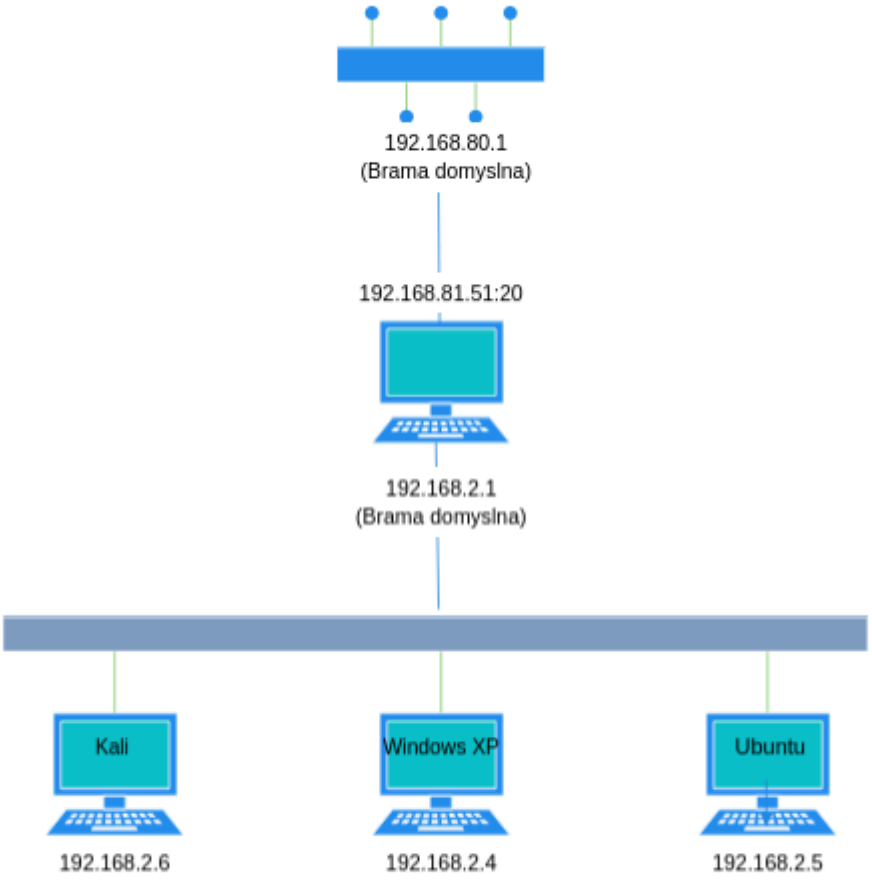
Testy Penetracyjne Lab 5

Julia Sadecka, Cyberbezpieczeństwo

1. Opis aktualnego środowiska sieciowego



2. Opis hosta z którego będzie przeprowadzona analiza sieciowa

Host znajduje się na maszynie Kali i ma adres IP 192.168.2.6 z maską 24.

3. Charakterystyka bibliotek użytych w programie
    - Biblioteka socket - służy ona do tworzenia i zarządzania gniazdami. Tutaj użyta aby umożliwić skanowanie otwartych portów w sieci.
    - Biblioteka ipaddress - służy do manipulacji i analizy adresów IPoraz sieci. Tutaj użyta aby zdobyć adres IP aktualnie podłączony do sieci i wyciągnąć z niego adres sieci i maskę

- Biblioteka threading - służy do obsługi wątków. Umożliwia to wykonywanie różnych operacji w jednym programie. Użyta aby przyśpieszyć działanie programu

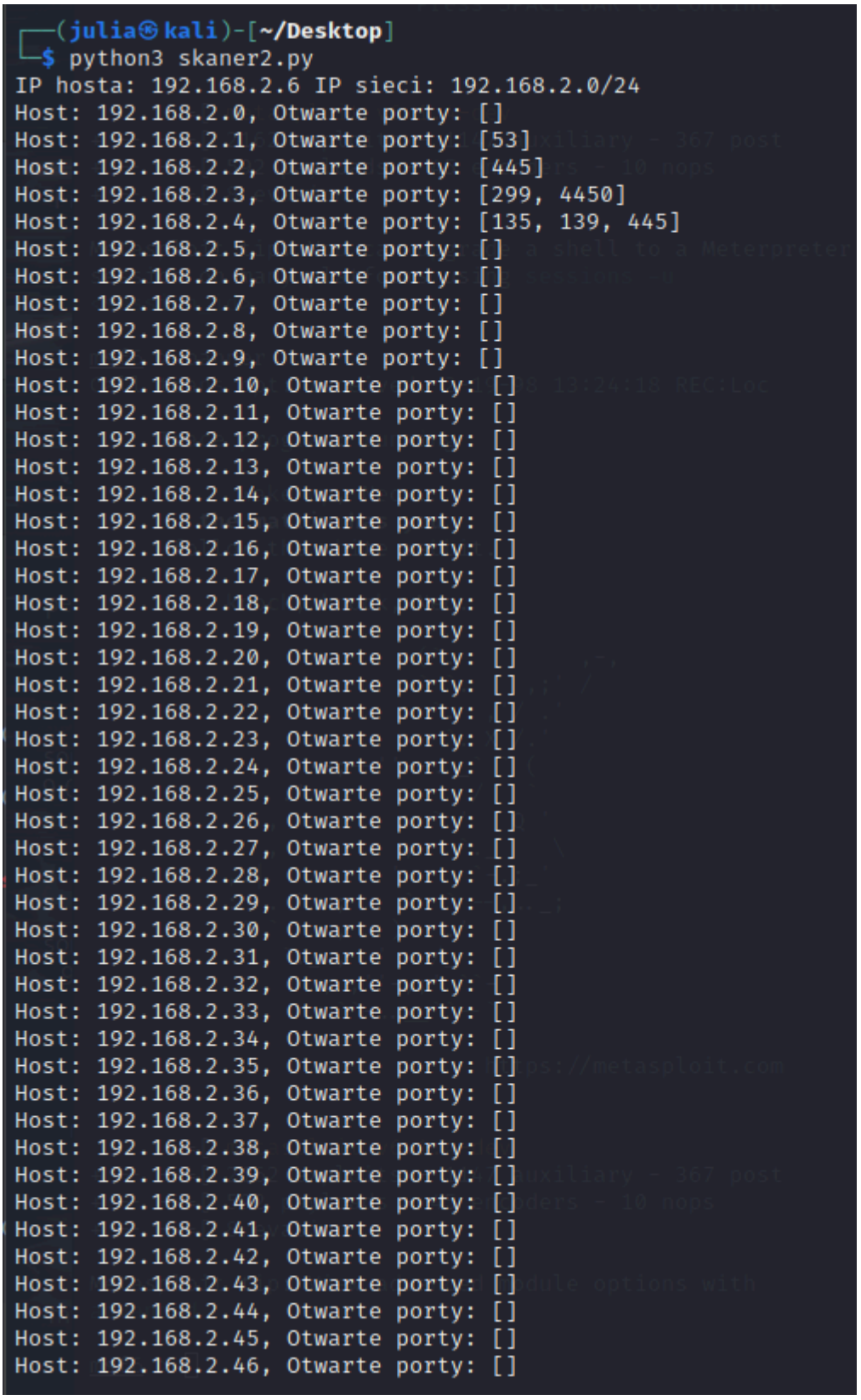
4. Kod

```
# Użyte biblioteki
import socket
import ipaddress
import threading

# Pozyskanie aktualnego adresu IP maszyny
def get_current_ip():
    try:
        sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
        sock.connect(("8.8.8.8", 80))
        current_ip = sock.getsockname()[0]
        sock.close()
        return current_ip
    except Exception as e:
        print(f"Wystąpił błąd: {e}")

# Stworzenie adresu sieci, potrzebnego aby następnie przebadać
wszystkie adresy IP w tej sieci
def get_network_address(ip, subnet_length):
    try:
        ip_obj = ipaddress.IPv4Address(ip)
        network_obj =
ipaddress.IPv4Network(f"{ip}/{subnet_length}", strict=False)
        return network_obj.network_address
    except ipaddress.AddressValueError as e:
        print(f"Błąd: {e}")
        return None

# Skanowanie jedenego portu w jednym adresie IP
def scan_port(ip, port):
        sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        sock.settimeout(0.2) # Ustawienie limitu czasu na 0.2sek
w celu przyśpieszenia procesu
        result = sock.connect_ex((str(ip), port))
        if result == 0:
            open_ports.append(port)
        sock.close()
```

```
        # print(f"Port {port} na hoście {ip} jest {'otwarty' if
result == 0 else 'zamknięty'}")

# Funkcja skanująca wszystkkie porty w jednym adresie IP
def scan_address(addr, start, amount):
    for port in range(0, amount):
        scan_port(addr, start + port)


if __name__ == "__main__":
    subnet_length = 24    # długość maski
    min_port = 1          # minimalna wartość portu
    max_port = 5002       # Maksymalna wartość portu
    threads = 900
    step = (max_port - min_port) // threads + 1
    current_ip = get_current_ip()
    subnet = str(get_network_address(current_ip, 24)) + '/24'
    open_ports = []
    threads = []
    # Wypisanie aktualnego adresu IP i adresu sieci i maski
    print("IP hosta: " + current_ip + ' IP sieci: ' + subnet)

    for host in ipaddress.IPv4Network(subnet, strict=False):
        open_ports.clear()
        threads.clear()
        st = min_port
        ip = str(host)
        # Obliczenie ilości potrzebnych portów do przeskanowania
na jednym adresie IP
        while True:
            if st + step >=max_port:
                t = threading.Thread(target=scan_address,
args=(ip, st, max_port - st, ))
                t.start()
                threads.append(t)
                break

            t = threading.Thread(target=scan_address, args=(ip,
st, step, ))
            t.start()
            threads.append(t)
            st = st + step
```

```
        while True:
            br = True

            for th in threads:
                if th.is_alive():
                    br = False
                    break
            if br:
                break
        open_ports.sort()
        # Wypisanie otwartych portów
        print(f"Host: {ip}, Otwarte porty: {open_ports}")

        # W przypadku portu 80 i 443 wypisanie stosownego
komunikatu
        if 80 in open_ports:
            print(f"Host {ip} - Otwarty port 80 (HTTP)")
        if 443 in open_ports:
            print(f"Host {ip} - Otwarty port 443 (HTTPS)")
```

5. Proces w strukturze sieciowej



Host z Windows XP wypisała otwarte porty: 135, 139 - Netbios, 445 - SMB/AD
Brama domyślna wyświetliła otwarty port 53 - DNS.