



SANGFOR



NGAF

Pedoman terbaik untuk Skenario Dos Attack Prevention
Versi 8.0.17



Data Perubahan

Tanggal	Keterangan Perubahan
June 11, 2020	Rilis dokumen Versi 8.0.17
May 17, 2021	Pembaruan dokumen.

DAFTAR ISI

BAB 1 Penjelasan Fungsi	1
BAB 2 Rekomendasi Pedoman	1
BAB 3 Instal Hyenae.....	1
BAB 4 Konfigurasi Policy dari Serangan DoS.....	7

BAB 1 Penjelasan Fungsi

Denial-of-Service (DoS) adalah serangan yang dapat melumpuhkan perangkat atau jaringan, membuat tidak dapat diakses oleh pengguna. Serangan DoS dilakukan dengan membanjiri target dengan trafik atau mengirimkan informasi yang dapat memicu penyebab dari kerusakan.

Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. Dalam kedua kasus, serangan DoS menghilangkan pengguna yang sah (yaitu karyawan, anggota, atau pemegang akun) dari layanan atau sumber daya yang mereka harapkan. Anda dapat mengaktifkan anti-DOS pada fungsi NGAF.

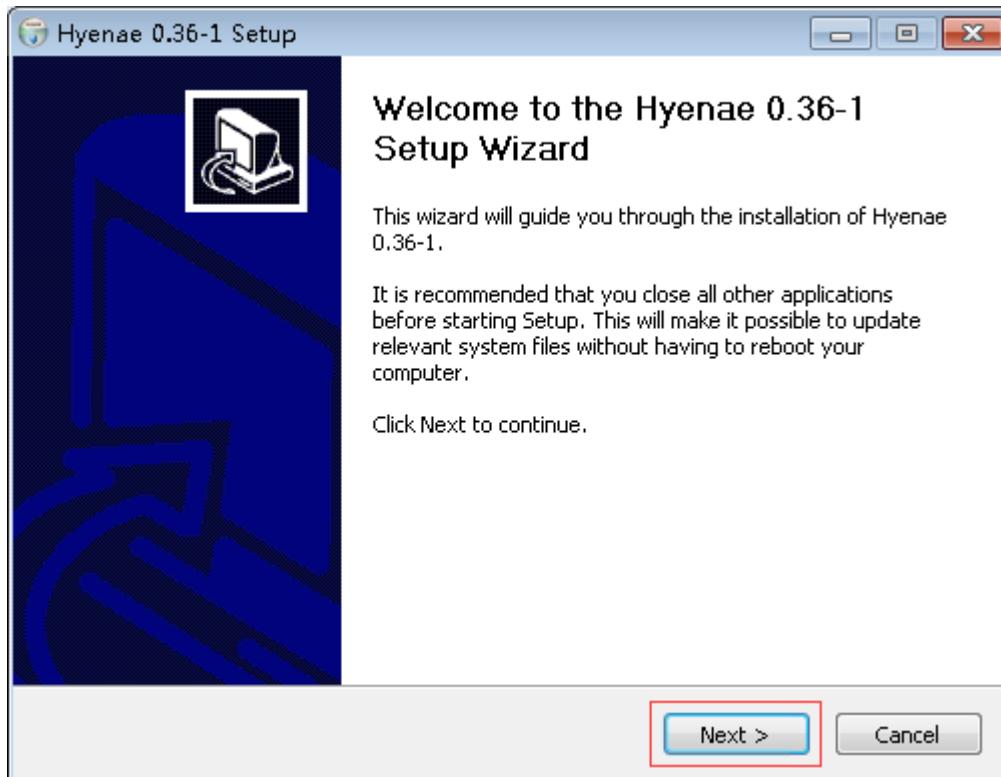
BAB 2 Rekomendasi Pedoman

Skenario:

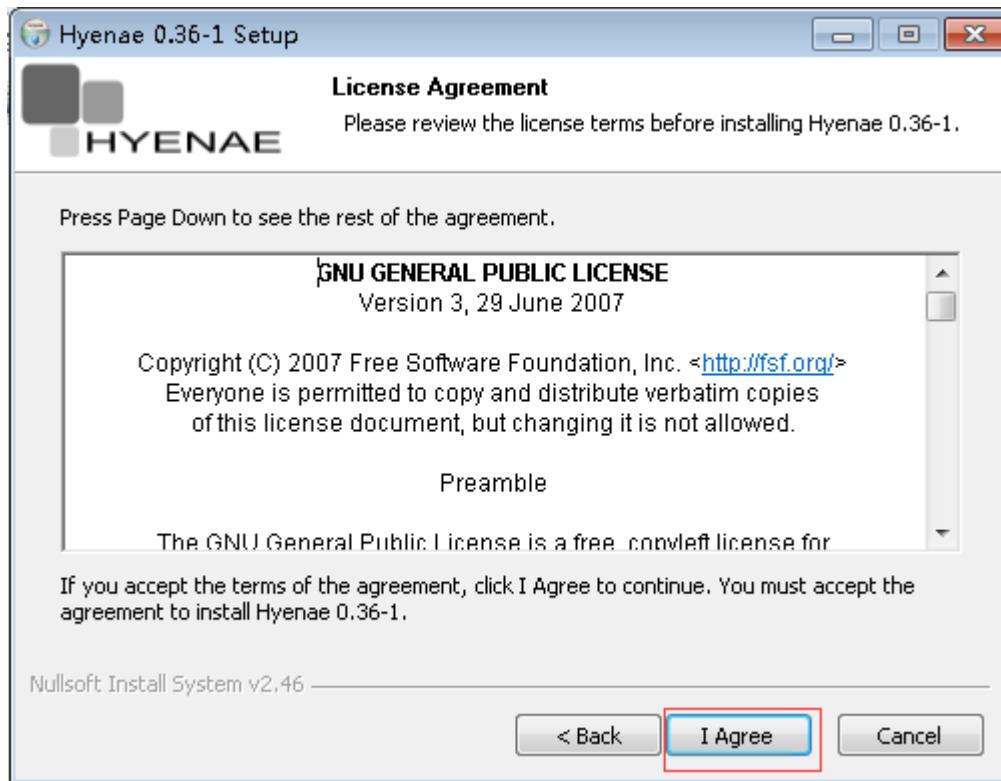
Contoh, Pelanggan UMKM dimana memiliki server web pada jaringan internal, dan sering sekali diserang DOS oleh kompetitor, dimana hasilnya adalah server web menggunakan sumber daya yang besar dan tidak dapat bekerja sesuai seperti biasanya. Diperlukan pertahanan terhadap serangan DOS dari jaringan eksternal.

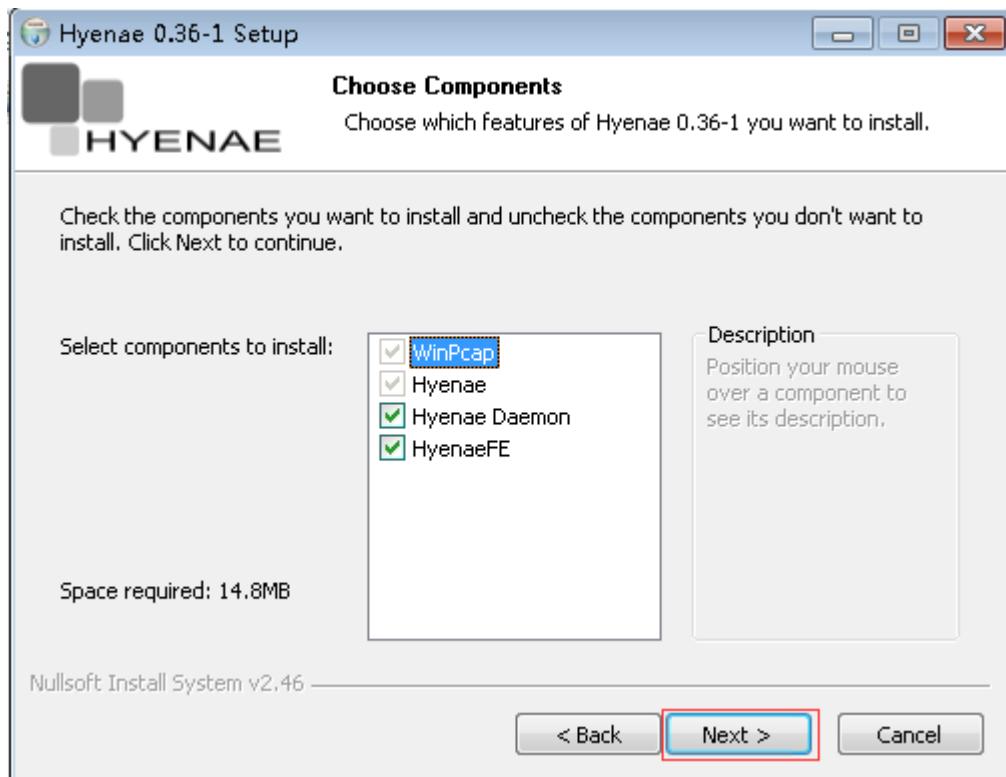
BAB 3 Instal Hyenae

1. Jalankan installer Hyenae, tekan tombol next untuk lakukan installasi.

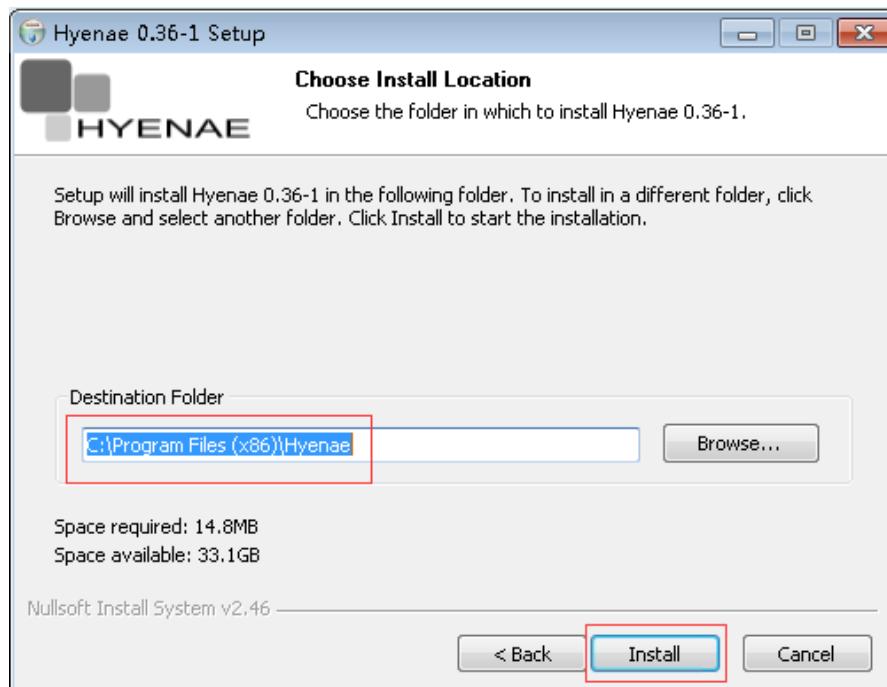


2. Klik "I Agree" pada halaman, lalu klik "Next" lagi.



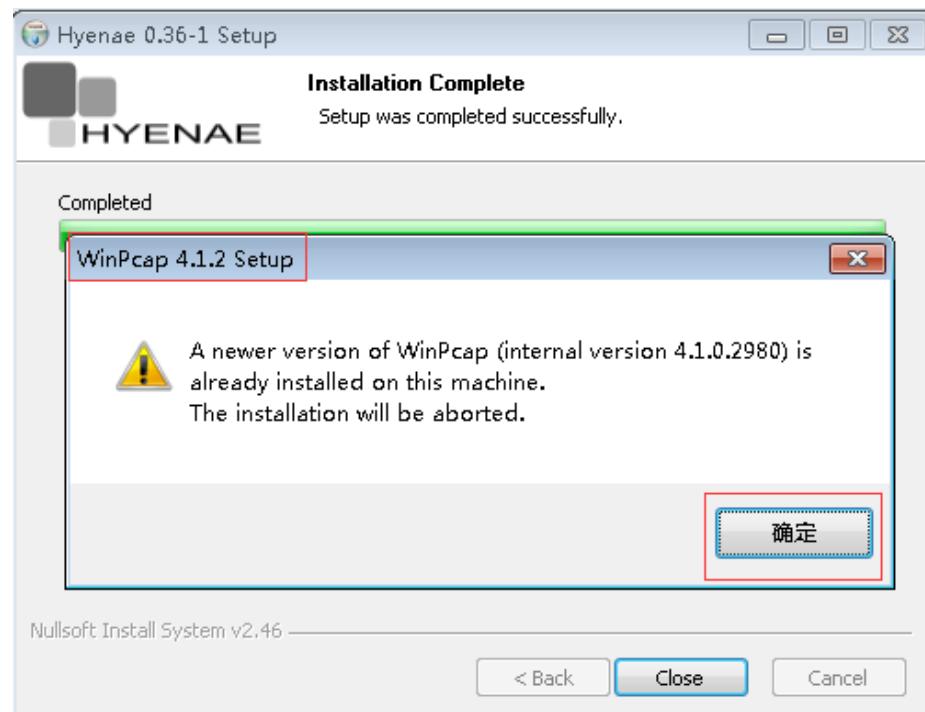


3. Setelah pilih posisi akan di install, klik install untuk menjalankan proses installasi.

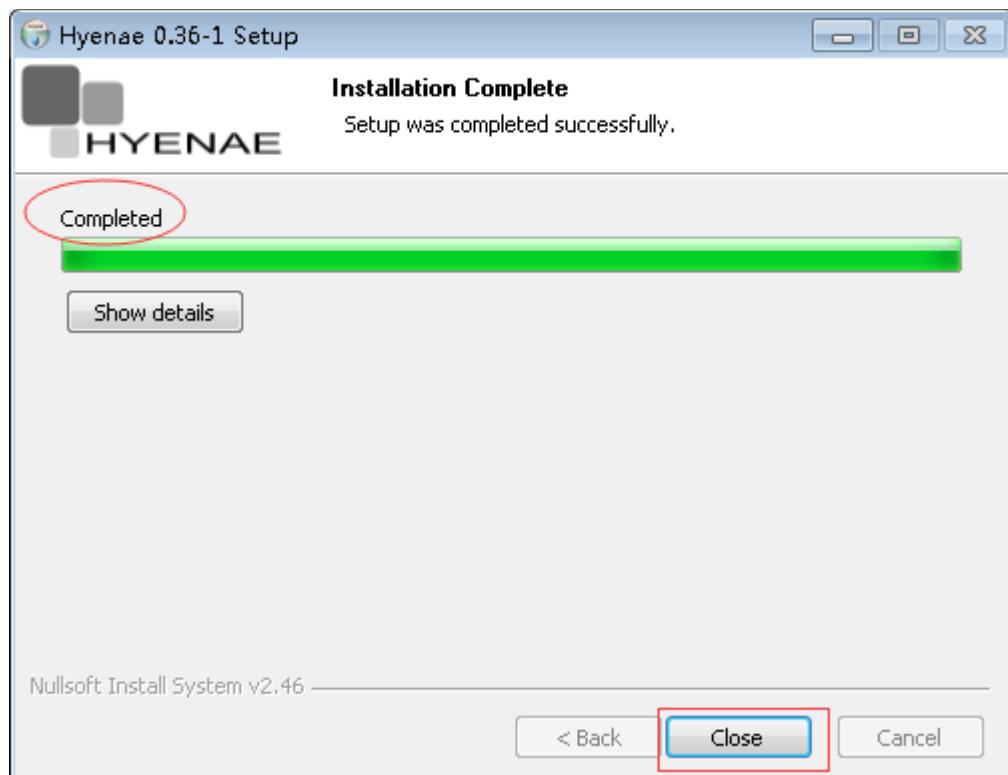


4. Permintaan instalasi WinPcap muncul, indikasi WinPcap akan muncul jika sudah terinstall. Installasi dari WinPcap dapat dibatalkan dengan menekan tombol OK;

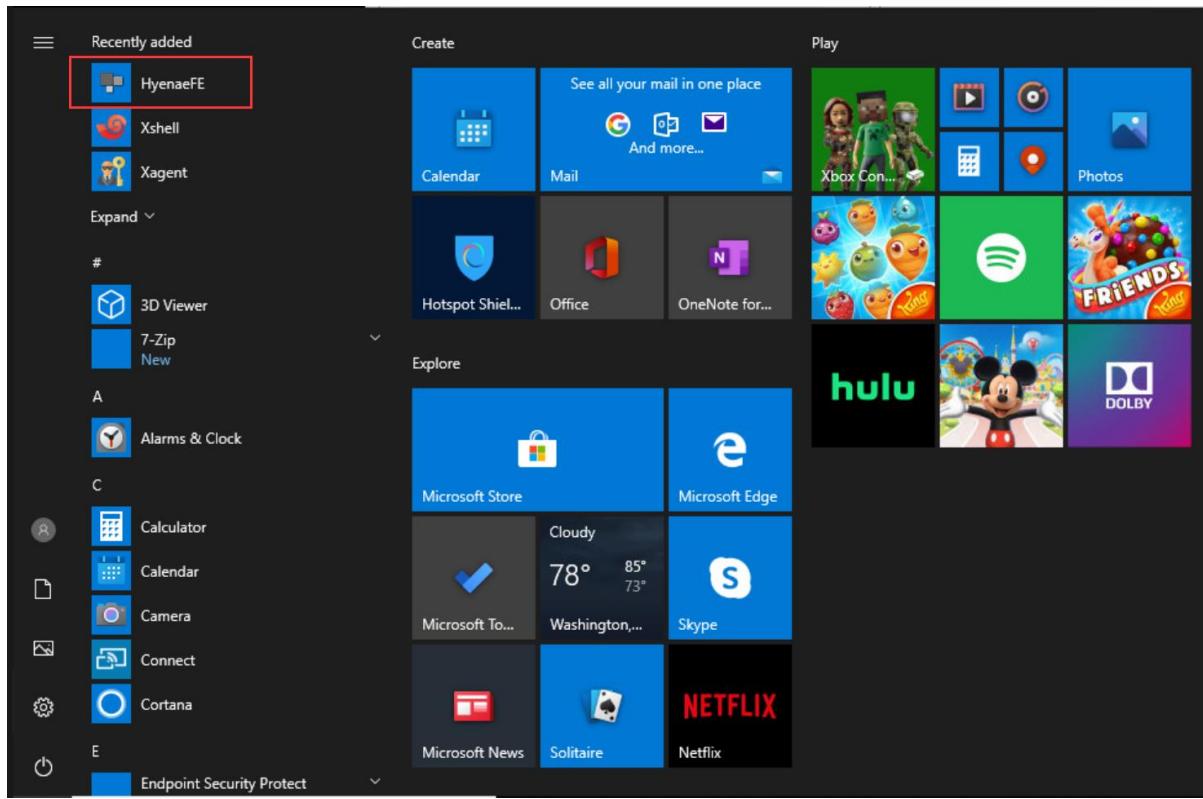
Catatan: Piranti Hyane memerlukan piranti WinPcap untuk di install, akan tetap jika piranti wireshark telah terinstall pada PC maka tidak perlu lagi mengulang installasi WinPcap. Jika belum terinstal ikuti langkah selanjutnya untuk menginstall WinPcap.



5. Setelah instalasi selesai, klik tombol “Close”, sebaiknya lakukan restart PC supaya piranti Hyenae dapat mengenali PIC.



6. Klik menu start lalu jalankan piranti “HyenaeFE”.



7. Saat menjalankan interface dari piranti HyenaeFE, beberapa setingan dan tombol perlu diperkenalkan sebagai berikut:

Operation Mode: Mode operasi, biarkan pilihan pada "Attack from local machine";

Network Interface: Network card, digunakan untuk memilih perangkat jaringan untuk digunakan oleh piranti mengirim ke PC;

Network Protocol: Network protocol, IP-Version (IP version) ada IPv4 dan IPv6, umumnya pilih pilihan dasar "IPv4", Packet Type (tipe paket) ada TCP, UDP dan tipe lainnya, anda dapat memilih sesuai kebutuhan;

Send Parameters: parameter dikirimkan, set jumlah dari paket yang dikirim, interval waktu pengiriman dan durasi pengingiriman.

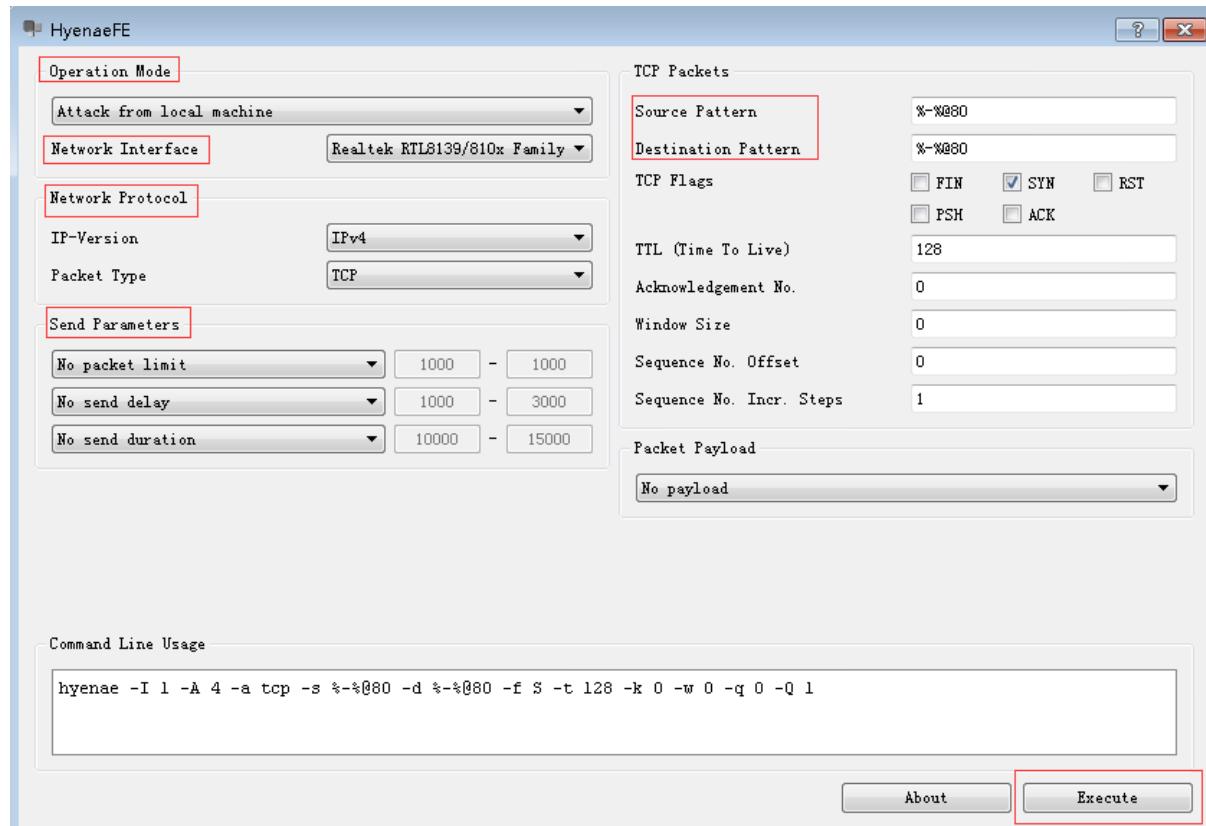
Source Pattern: pattern asal, digunakan untuk set MAC asal, IP asal dan asal port saat pengiriman paket data, format MAC-IP@port number, "%" artinya di buat secara acak;

Destination Pattern: pattern tujuan, digunakan untuk set MAC tujuan, IP tujuan dan port tujuan dari paket data yang dikirimkan, format MAC-IP@port number, "%" artinya di buat secara acak;

Execute: execute adalah tombol untuk memulai pengiriman paket

Catatan: Dalam process penggunaan Hyenae mengirim paket data, ada kemungkinan kejadian paket yang dikirimkan terlalu cepat membuat PC menjadi bermasalah. Kami sarankan untuk membatasi jumlah paket yang dikirimkan saat pengujian.

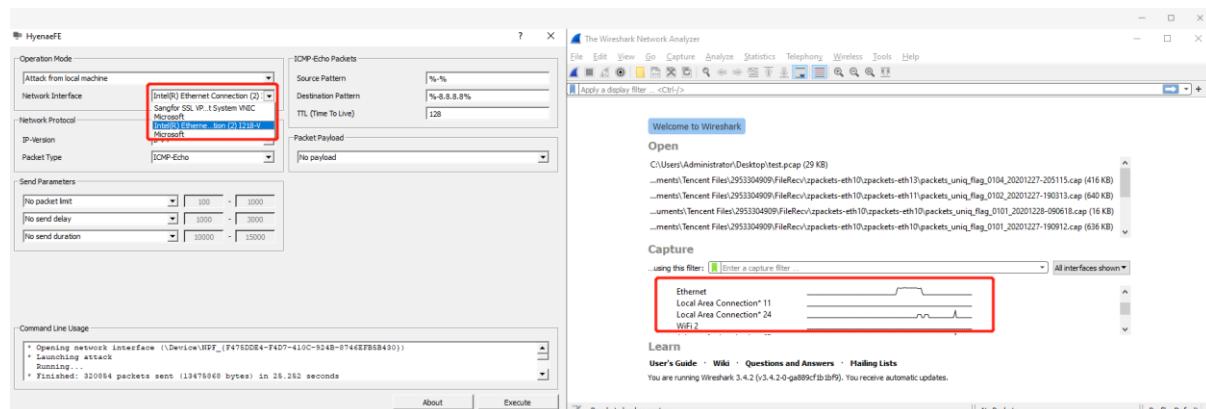
Best Practice_Dos Attack Prevention



Catatan:

Hyenae menggunakan komponen WinPcap, jadi pembacaan list dari NIC, akan muncul beberapa nama NIC sebagai "Microsoft", seperti halnya pada wireshark. Ketika jumlah dari NIX terlalu besar.

Anda dapat mengirimkan paket melalui NIC yang berbeda dalam Hyenae untuk melihat apakah trafik tertinggi dalam wireshark. Biasanya multiple NIC dalam Wireshark dan pada beberapa NIC tersebut tidak memiliki trafik. Sangat mudah untuk melakukan pengujian list NIC pada Hyenae dan list NIC dalam Wireshark. Maka dari itu temukan NIC dari jaringan dalam Hyenae.



BAB 4 Konfigurasi Policy dari Serangan DoS

Perangkat hanya memiliki "Outbound Attack Protection". Jika anda mengaktifkan "Inbound Attack Protection", anda perlu mengaktifkannya dalam sistem konfigurasi.

The top screenshot shows the 'Anti-DoS/DDoS' configuration page. The left navigation menu is expanded to show 'Policies' under 'Network Security'. The main table header includes columns for 'Section', 'Description', 'Type', 'Attack Source Zone', and 'Status'. A note at the bottom states 'No data available'.

The bottom screenshot shows the 'System' configuration page with the 'Network' tab selected. The left navigation menu is identical to the top one. The main area contains various network-related settings, including RAS and Q931 ports, SIP configuration, and a large section for 'Gratuitous ARP' settings. Under 'Gratuitous ARP', there is a checkbox for 'Enable protection against outside DoS attacks' which is checked and highlighted with a red rectangle. Other options in this section include 'ARP Broadcast Interval' set to 30 seconds, and several other checkboxes for packet detection, Base64 decoding, and MAC address change response.

1. Pada menu, pilih proteksi DoS/DDoS, klik tombil Add, dan pilih jaringan external untuk strategi proteksi serangan jaringan internal.

Best Practice_Dos Attack Prevention

The screenshot shows the Sangfor management interface under the 'System' section. The 'Anti-DoS/DDoS' configuration page is displayed. The 'Inbound Attack Protection' tab is active. A single policy entry is shown:

No.	Name	Protection	Description	Type
1	Dos	Inbound	Anti-DoS/DDoS: Enable Packet-Based Attack and Abnormal Message: Enable	

2. Masukan policy Input dan pilih asal yang tepat dan Area Tujuan. Jika anda memilih Asal dan Tujuan Area, policy tidak akan berpengaruh.

The screenshot shows the 'Edit Inbound Attack Prevention' dialog box. The 'Source' field is set to 'External Zone: DMZasWAN'. The 'Network Objects' field is set to 'LAN'. The 'Action' section has both 'Log event' and 'Deny' checkboxes checked.

Anda dapat mengkonfigurasi parameter untuk setiap tipe serangan, Contoh: anda dapat mengatur threshold ke angkat yang lebih kecil untuk melihat pengaruh yang lebih baik, jika dibutuhkan pengesetan pada trafik jaringan.

Best Practice_Dos Attack Prevention

Navigation

- Status
- Network
- Objects
- Policies
- System**
 - General
 - System
 - Logging Options
 - Alarm Options
 - Central Management
 - Security Capability Update
 - Administrator
 - Maintenance
 - Troubleshooting
 - Tools
 - Logs
 - High Availability
- Authentication System
- Security Solution

Anti-DoS/DDoS

No.	Name	Protection	Description	Type
1	Dos	Inbound	Anti-DoS/DDoS: Enable Packet-Based Attack and Abnormal Message: Enable	

Edit Inbound Attack Prevention

Defense Against DoS/DDoS Attack

- ICMP Flood** (selected)
- SYN Flood
- UDP Flood
- DNS Flood
- ICMPv6 Flood

Defense against ICMP flooding attack

Per-Dst-IP Packet Loss Threshold(packets/sec): 400

Per-Src-IP Packet Loss Threshold(packets/sec): 200

Address Block Period(sec): 300

Network Objects: LAN

Attack Type: Selected: Defense against SYN ...

Action: Log event Deny

Advanced

Advanced Protection

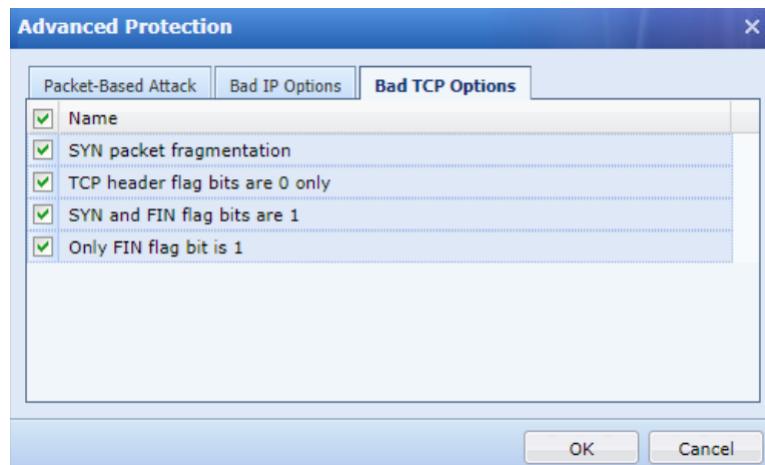
Packet-Based Attack

- Name
- Unknown protocol
- TearDrop attack
- Sending IP fragment
- LAND attack
- WinNuke attack
- Smurf attack
- Large size ICMP packet(>1024B) #Ping of death

Advanced Protection

Bad IP Options

- Name
- Wrong IP message
- IP timestamp message
- IP security option message
- IP stream option message
- IP record route option message
- IP loose src route option msg
- IP strict src route option msg



3. Didalam proses penggunaan Hyenae dalam pengiriman paket data, akan ada beberapa kejadian seperti pengiriman terlalu cepat dan PC menjadi tidak dapat berkerja. **Saran kami untuk membatasi jumlah paket yang dikirimkan pada saat pengujian.**

Format alamat dari asal dan tujuan adalah sebagai berikut:

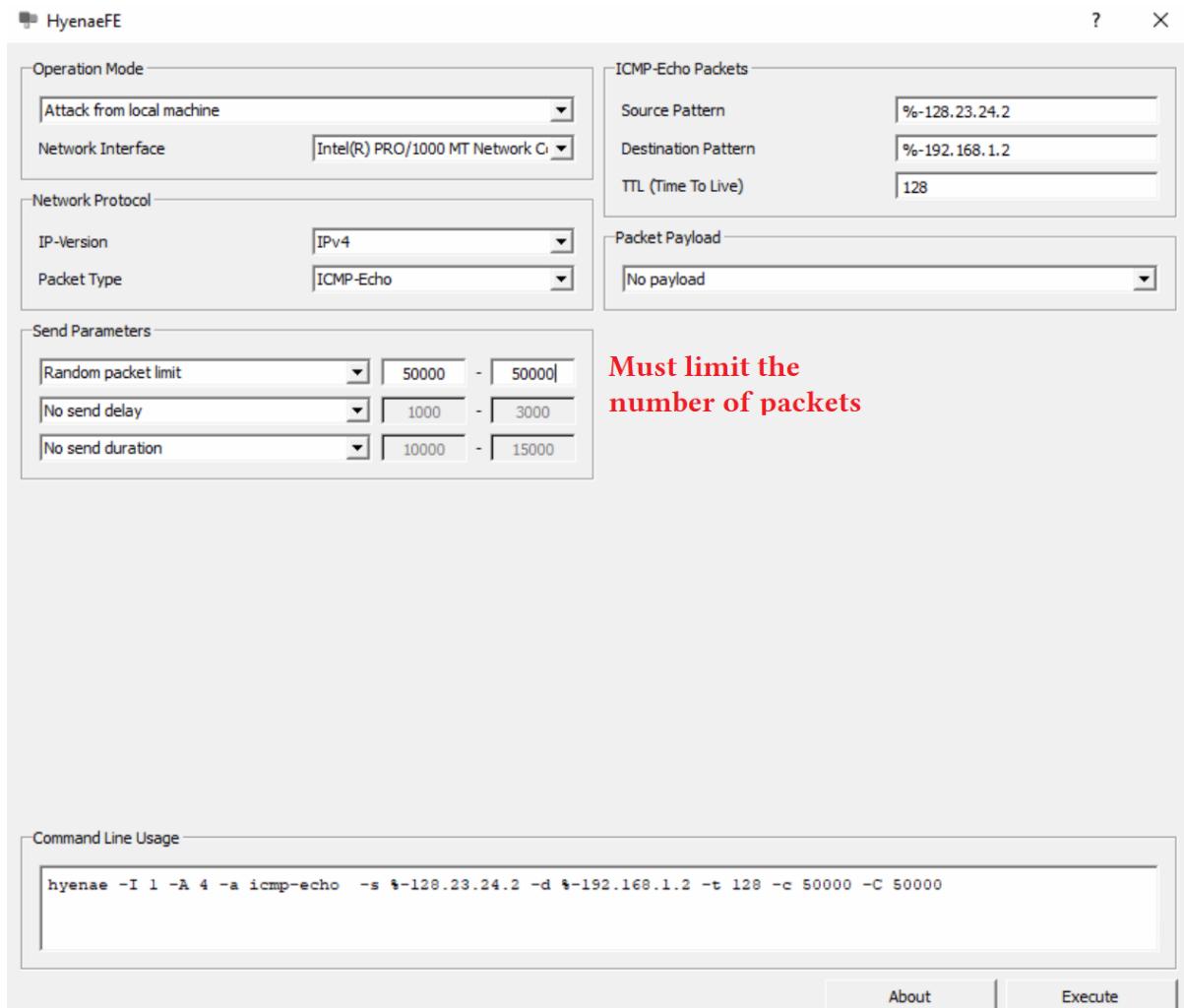
Source Pattern: Source pattern, digunakan untuk set Asal MAC, Asal IP dan asal port dari paket data yang dikirimkan, format adalah MAC-IP@port number, "%" artinya di buat secara acak.

Destination Pattern: pattern tujuan, digunakan untuk set MAC tujuan, IP tujuan dan port tujuan dari paket data yang dikirimkan, format MAC-IP@port number, "%" artinya di buat secara acak;

Pada saat anda memilih protokol yang berbeda, format dari contoh akan berbeda. **Jika anda perlu mengganti % dengan alamat yang berhubungan**, anda hanya perlu merubah IP-nya saja.

Contoh, ketika protokol icmp-echo telah dipilih, format adalah %-%, % pertama mengidentifikasi sebagai alamat MAC, dan % kedua mengidentifikasi sebagai alamat IP. Anda tidak perlu MAC yang spesifik, **jadi tidak perlu merubah % awal, tapi jangan menghapusnya**. Contohnya, Pattern tujuan: %-192.168.1.2 identifikasi bahwa alamat tujuan dari data paket 192.168.1.2 dan alamat MAC tidak diperlukan.

Best Practice_Dos Attack Prevention



4. Anda dapat menyaring sejarah dari serangan DOS melalui log center.

DoS Attack												
Filter Export Logs												
Filter: Period (2020-06-12 00:00~2020-06-12 23:59) Direction(Outbound,Inbound) Attacker Zone(All) Attacker IP(All) Target IP(All) Type (All) Threat level (High,Medium,Low) Action (Allow,Deny)												
No.	Date	Type	Direction	Attacker IP	Attacker MAC	Target IP	Threat Level	Act...	Description	Det... Whitelist		
1	2020-06-12 10:44:56	ICMP flooding ...	Inbound	128.23.24.2	No. 1	Date: 2020-06-12 10:44:56 Type: ICMP flooding attack Direction: Inbound Attacker Zone: DMZasWAN Attacker IP: 128.23.24.2 Attacker MAC: cf:dd:33:ad:06:82 Target IP: 192.168.1.2 Policy Name: Dos Threat Level: High Action: Deny Blocked Period: 300 second Description: Number of packets sent on an IP address exceeds the threshold (200 packets/second)						View Add



SANGFOR

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc