RANCANG BANGUN KEAMANAN VPS DAN ROUTER PT BPM DENGAN PEMANFAATAN HONEYPOT COWRIE DAN SNORT IPS

SKRIPSI

Ariel Muhammad Amri

2003421002

PROGRAM STUDI BROADBAND MULTIMEDIA

JURUSAN TEKNIK ELEKTRO

POLITEKNIK NEGERI JAKARTA

2024

RANCANG BANGUN KEAMANAN VPS DAN ROUTER PT BPM DENGAN PEMANFAATAN HONEYPOT COWRIE DAN SNORT IPS

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar

Sarjana Terapan

Ariel Muhammad Amri

2003421002

PROGRAM STUDI BROADBAND MULTIMEDIA

JURUSAN TEKNIK ELEKTRO

POLITEKNIK NEGERI JAKARTA

2024

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama	:	Ariel Muhammad Amri
NIM	:	2003421002
Tanda Tangan	:	Ariel
Tanggal	:	2 Agustus 2024

POLITEKNIK NEGERI JAKARTA

LEMBAR PENGESAHAN
SKRIPSI

Skripsi diajukan oleh:

Nama : Ariel Muhammad Amri
NIM : 2003421002
Program Studi : Broadband Multimedia
Judul Skripsi : Rancang Bangun Keamanan VPS dan Router PT BPM dengan Pemanfaatan Honeypot Cowrie dan Snort IPS

Telah diuji oleh tim penguji dalam Sidang Skripsi pada 9 Agustus 2024 dan dinyatakan (**Lulus/~~Tidak Lulus~~**).

Pembimbing 1: Dandun Widhiantoro, A.Md., S.T., M.T. ( )

NIP. 19701125 199503 1 001

Pembimbing 2: Budi Utami, S.Si., M.Si. ( )

NIP. 19880927 202203 2 009

Depok, … Agustus 2024

Disahkan Oleh

Ketua Jurusan Teknik Elektro

Dr. Murie Dwiyaniti, S.T., M.T.

NIP. 19780331 200312 2 002

KATA PENGANTAR

Puji dan syukur dipanjatkan kepada Allah Azza wa Jalla, karena atas berkat dan rahmat-Nya, skripsi ini dapat diselesaikan. Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Terapan Politeknik. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi penulis untuk menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Bapak Dandun Widhiantoro, A.Md., S.T., M.T. dan Ibu Budi Utami, S.Si., M.Si., selaku dosen pembimbing yang telah menyediakan waktu untuk mengarahkan penulis dalam penyusunan laporan ini;
2. Orang tua dan keluarga penulis yang telah memberikan do'a, motivasi, serta bantuan dukungan material dan moral selama menyelesaikan skripsi;
3. Sahabat dan orang terdekat penulis yang telah banyak membantu dan mendukung penulis dalam menyelesaikan laporan ini, terkhusus untuk Daniel, Andika, Dzakiyyudin, dan Ilhamsyah.
4. Pak Mayel selaku CTO dari PT Berdikari Prima Mandiri yang telah membimbing dan mengarahkan dalam menyelesaikan skripsi ini.
5. Bang Oktafiyan selaku NOC dari PT Berdikari Prima Mandiri yang telah banyak membantu dalam menyelesaikan skripsi ini.

Akhir kata, penulis berharap semoga Allah Azza wa Jalla berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga laporan skripsi ini membawa manfaat bagi pengembangan ilmu.

Jakarta, Agustus 2024

Ariel Muhammad Amri

Rancang Bangun Keamanan VPS dan Router PT BPM dengan Pemanfaatan Honeypot Cowrie dan Snort IPS

Abstrak

Dengan kemajuan teknologi informasi pada jaringan komputer, masalah serius terkait keamanan jaringan masih tetap menjadi tantangan dalam beberapa tahun terakhir. Honeypot Cowrie dan Snort dapat dimanfaatkan untuk meningkatkan keamanan server atau jaringan. Honeypot Cowrie adalah sistem deteksi intrusi yang dirancang khusus untuk menangani masalah terkait protokol SSH (Secure Shell). Sementara itu, Snort adalah sistem deteksi intrusi berbasis jaringan yang juga dapat berfungsi sebagai sistem pencegahan intrusi dengan pendekatan berbasis aturan dalam pendeteksiannya. Untuk mengukur efektivitas Honeypot Cowrie dan Snort IPS (Intrusion Prevention System), dilakukan serangkaian pengujian yang mencakup pengujian akurasi deteksi Honeypot Cowrie dalam melindungi layanan SSH, serta pengukuran jumlah paket yang di-drop oleh Snort dan penilaian efisiensinya dalam menangani serangan. Hasil pengujian menunjukkan bahwa Honeypot Cowrie mampu mendeteksi semua metode dan modul serangan yang menargetkan port 22 dengan akurasi 100%. Hasil Snort IPS menunjukkan Snort men-drop 4,96% dari total paket yang diterima selama serangan brute-force, yang merupakan persentase rendah, menunjukkan kemampuan sistem dalam menangani trafik jaringan tanpa mengorbankan kinerja. Tingkat efisiensi Snort dalam menangani serangan brute-force sebesar 95,04% menunjukkan keandalannya. Selain itu, Snort juga terbukti efektif dalam mendeteksi serangan penetrasi dari modul Metasploit yang menargetkan port 80. Namun, dalam pengujian serangan DoS (Denial of Service), Snort mengalami penurunan performa yang signifikan dengan persentase packet drop sebesar 90,81%, yang menunjukkan keterbatasan Snort dalam menghadapi serangan DoS yang intens. Hasil efisiensi Snort sebesar 9,1% menunjukkan bahwa Snort memiliki keterbatasan dalam menangani lalu lintas jaringan yang sangat tinggi.

***Kata kunci**: honeypot cowrie, intrusi deteksi, keamanan jaringan, snort*

Design and Implementation of VPS and Router Security of PT BPM using Honeypot Cowrie and Snort IPS

Abstract

With advances in information technology on computer networks, serious issues related to network security remained a challenge in recent years. Cowrie's Honeypot and Snort can be used to enhance server or network security. Honeypot Cowrie is an intrusion detection system designed specifically to deal with issues related to the SSH (Secure Shell) protocol. Meanwhile, Snort is a network-based intrusion Detection system that can also serve as an intruder prevention system with a rule-based approach in its detection. To measure the effectiveness of Honeypot Cowrie and Snort IPS (Intrusion Prevention System), a series of tests were carried out that included testing the accuracy of Cowrie's Honypot detection in protecting SSH services, as well as measuring the number of packets dropped by Snort and assessing its effectivency in dealing with attacks. The test results showed that Honeypot Cowrie was able to detect all methods and modules of attack targeting port 22 with a 100% accuracy. Snort IPS results revealed that Snort dropped 4.96% of the total package received during a brute-force attack, which is a low percentage, showing the system's ability to handle network traffic without compromising performance. In addition, Snort also proved to be effective in detecting penetration attacks from Metasploit modules targeting port 80. However, in the DoS (Denial of Service) attack test Snort experienced a significant decline in performance with a package drop percentage of 90.81%, indicating Snort's limitation in the face of intense DoS attacks.

***Key words**: honeypot cowrie, intrusion detection, network security, snort*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Ancaman terhadap keamanan informasi digital, mencakup aspek kerahasiaan dan integritas, menjadi isu penting di era modern ini. Dengan semakin terhubungnya dunia melalui informasi digital yang mendukung layanan dan infrastruktur utama, risiko serangan siber juga meningkat (Perwej et al., 2021). Meskipun teknologi informasi telah mempermudah pencarian, pengumpulan, dan distribusi data, teknologi ini juga membuka peluang bagi terjadinya serangan siber, seperti pencurian dan pemalsuan data selama proses komunikasi data.

Sistem keamanan jaringan yang handal wajib dimiliki oleh setiap perusahaan, termasuk PT Berdikari Prima Mandiri. Perusahaan ini merupakan perusahaan penyedia layanan internet dan penyedia layanan *hosting website* pelanggan. Masalah keamanan jaringan yang dialami oleh perusahaan adalah penyerangan berupa *brute-force* yang diarahkan ke *Virtual Private Server* (VPS) sebagai *server hosting* dan ke *router* perusahaan. Meskipun perusahaan sudah menggunakan *firewall*, tetapi *firewall* yang digunakan masih bisa ditembus oleh penyerang. Hal ini dapat mempengaruhi layanan internet yang disediakan oleh perusahaan. Oleh karena itu, dibutuhkan sistem yang dapat meningkatkan keamanan jaringan untuk melindungi VPS dan *router* perusahaan.

Honeypot dan Snort dapat dimanfaatkan untuk sistem keamanan jaringan. Hasil studi terkait Snort oleh (Satria et al., 2021) digunakan Snort sebagai IPS (*Intrusion Prevention System*). Diperoleh hasil bahwa setiap paket yang berasal dari serangan *brute-force* dan melewati sistem Snort akan diawasi untuk menentukan jumlah paket yang diterimanya per detik. Jika paket yang tiba di sistem Snort tidak sesuai dengan aturan yang telah ditetapkan, maka sistem Snort akan menghentikan paket tersebut karena telah melewati batas maksimum paket yang diizinkan untuk lewat per detik. Studi lain terkait Honeypot yang dilakukan oleh (Mispriatin et al., 2022) menunjukkan hasil pengujian yang dilakukan bahwa Honeypot Dionaea memiliki tingkat keefektifan sebesar 92,8% dalam mendeteksi serangan port scanning, tetapi tidak efektif dalam mendeteksi serangan *brute-force* SSH.

Sebaliknya, Honeypot Cowrie memiliki tingkat keefektifan sebesar 7,2% dalam mendeteksi serangan *port scanning* dan 92,8% efektif dalam mendeteksi serangan *brute-force* SSH. Hasil pengujian dari studi tersebut menunjukkan bahwa Honeypot Cowrie lebih efektif dari Honeypot Dionaea untuk mendeteksi serangan *brute-force* SSH. Sementara itu, Snort dapat digunakan untuk mendeteksi dan memblokir akses jumlah paket yang tidak sesuai aturan sistem Snort.

Berdasarkan uraian tersebut, maka disusun skripsi yang berjudul "Rancang Bangun Keamanan VPS dan Router PT BPM dengan Pemanfaatan Honeypot Cowrie dan Snort IPS". Penelitian ini menggunakan Honeypot Cowrie untuk menjebak dan mendeteksi perilaku penyerang serta melacak alamat IP penyerang yang melakukan serangan siber terhadap SSH dan *router* perusahaan. Snort dipilih sebagai IPS untuk mendeteksi dan melakukan pemblokiran akses penyerang yang berhasil menyusup kedalam jaringan.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan permasalahan dalam skripsi ini, antara lain:

a. Bagaimana langkah untuk implementasi sistem keamanan Honeypot Cowrie dan Snort IPS di jaringan internal perusahaan?
b. Serangan siber apa saja yang dapat dideteksi dan diidentifikasi oleh Honeypot Cowrie dan Snort IPS?
c. Bagaimana hasil pengujian sistem keamanan Honeypot Cowrie dan Snort IPS?

1.3 Batasan Masalah

Berdasarkan perumusan masalah yang dibuat, terdapat batasan masalah untuk membatasi ruang lingkup pengujian kinerja tools IPS dalam menangani kerentanan sistem keamanan jaringan, adalah:

a. Sistem keamanan yang diuji adalah Honeypot Cowrie 2.5 Snort 3.1.74 dengan menggunakan aturan (*rule*) yang sudah tersedia dari masing – masing sistem.
b. Metode IDS yang digunakan adalah *knowledge-based*.

c. Objek yang dilindungi adalah *Virtual Private Server* yang menggunakan OS linux Ubuntu *desktop* 22.04 dan *router* Mikrotik.
d. Pengujian terfokus pada penyerangan terhadap jaringan berupa serangan *brute-force* dan DoS.
e. Alamat IP *router* Mikrotik tidak dapat disertakan pada skripsi ini dikarenakan merupakan hal yang *confidential* bagi PT BPM.

1.4 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dari penelitian ini, yaitu:

a. Mengetahui implementasi Honeypot Cowrie dan Snort IPS untuk digunakan sebagai sistem keamanan jaringan di jaringan internal perusahaan.
b. Mengetahui dan mengidentifikasi serangan siber yang dideteksi oleh Honeypot Cowrie dan Snort IPS.
c. Melakukan pengujian sistem keamanan Honeypot Cowrie dan Snort IPS.

1.5 Luaran

Pada skripsi ini, luaran yang diharapkan antara lain:

a. Sistem keamanan jaringan terintegrasi Honeypot Cowrie dan Snort IPS di PT Berdikari Prima Mandiri.
b. Menghasilkan artikel ilmiah yang telah diseminarkan pada Seminar Nasional Teknik Elektro (SNTE) 2024, seminar tersebut dilaksanakan di Politeknik Negeri Jakarta tanggal 26 Juni 2024.
c. Laporan skripsi.
d. Menghasilkan artikel ilmiah terkait sistem keamanan VPS dan *router* menggunakan Honeypot Cowrie dan Snort IPS yang dibuat dan disertai data hasil pengujian sistem. Artikel akan di-*submit* pada Jurnal Nasional Informatika dan Teknologi Jaringan (INFOTEKJAR).

DAFTAR PUSTAKA

Alamsyah Pratama, M., Setiawan, H., & Mair, Z. R. (2023). Implementasi Honeypot Sebagai Pendeteksi Serangan Pada Virtual Private Server (VPS). *Journal of Software Engineering and and Computer Intelligence*, *1*(1), 26-39.

Amijoyo, T., Umar, R., & Yudhana, A. (2020). *Bruteforce In The Hydra Process And Telnet Service Using The Naïve Bayes Method*, *4*(36).

Army, W. L., Barovih, G., Seta, H. B., Margiutomo, S. A. S., Arifianto, T., Pujianto, D., Mutasar, Habibah, N., & Fajri, T. I. (2022). *Teknologi Jaringan Komputer* (A. Surahmat, Ed.; Pertama). Widina Bhakti Persada Bandung.

Balen, J., Vajak, D., & Salah, K. (2020). Comparative performance evaluation of popular virtual private servers. *Journal of Internet Technology*, *21*(2), 343–356.

Čhulālongkǭnmahāwitthayālai. Khana Witthayāsāt, Mahāwitthayālai Būraphā. Faculty of Informatics, Institute of Electrical and Electronics Engineers, IEEE Thailand Section, & Electrical Engineering/Electronics, C. (n.d.). *2019 JCSSE : the 16th International Joint Conference on Computer Science and Software Engineering : "Knowledge Evolution Towards Singularity of Man-Machine Intelligence" : July 10-12, 2019, Amari Pattaya, Chonburi, Thailand*.

Gupta, A., & Sen Sharma, L. (2020). Performance Analysis and Comparison of Snort on Various Platforms. In *International Journal of Computer Information Systems and Industrial Management Applications. 10*.

Mispriatin, M., Gusti, J., Ginting, A., Arifwidodo, B., & Kunci, K. (2021). *Analisis Kinerja Honeypot Dionaea Dan Cowrie Dalam Mendeteksi Serangan*. *6*, 2021.

M.R., A., & P., V. (2022). Review of Cyber Attack Detection: Honeypot System. *Webology*, *19*(1), 5497–5514.

Natanegara, T., Muhdiyin, Y. & Singsasatia, D. (2023). Implementasi Honeypot Cowrie dan SNORT sebagai Alat Deteksi Serangan pada Server. *Jurnal Mahasiswa Teknik Informatika*, *7*(3), 1871-1877.

Nursetyo, A., Rosal, D., Setiadi, I. M., Sari, C. A., & Rachmawanto, E. H. (2019). Website and Network Security Techniques against Brute Force Attacks using Honeypot. *2019 Fourth International Conference on Informatics and Computing (ICIC)*, 1-6.

Park, J., Kim, J., Gupta, B. B., & Park, N. (2021). Network Log-Based SSH Brute-Force Attack Detection Model. *Computers, Materials and Continua*, *68*(1), 887–901.

Perwej, D., Qamar Abbas, S., Pratap Dixit, J., Akhtar, N., & Kumar Jaiswal, A. (n.d.). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*, *2021*(12), 669–710.

Putri, D. A. P., & Rachmawati, A. (2019). Honeypot cowrie implementation to protect ssh protocol in ubuntu server with visualisation using kippo-graph. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(6), 3200–3207.

Rahmatillah, A., Firdaus, A., Laila, E., Komputer, J. T., Sriwijaya, N., Negara, J. S., & Selatan, S. (2021). Implementasi Intrusion Prevention System (IPS) Pada Keamanan Jaringan Dengan Notifikasi Berbasis Telegram di Jurusan Teknik Komputer. In *Jurnal Laporan Akhir Teknik Komputer*, *1*(1).

Satria, E., Huda, T. P. S., Iqbal, M., & Sarjana, F. W. (2021). The investigation on cowrie honeypot logs in establishing rule signature snort. *IOP Conference Series: Earth and Environmental Science*, *644*(1).

Syed, N. F., Baig, Z., Ibrahim, A., & Valli, C. (2020). Denial of service attack detection through machine learning for the IoT. *Journal of Information and Telecommunication*, *4*(4), 482–503.

Widodo Purbo, O., Widodo Purbo Institut Teknologi Tangerang Selatan, O., Komplek Komersial BSD, I., & Raya Serpong Jl Komp Bsd No Kav, J. (2019).

Ubuntu Linux Server Security Analysis and Simulation With Port Knocking & Iptable. *International Journal of Basic and Applied Science*, *8*(2).

Wiryadinata, R., Bangun Keamanan, R., & Kunci, K. (2022). Rancang Bangun Keamanan Port Secure Shell (SSH) Menggunakan Metode Port Knocking, *JIKOMSI [Jurnal Ilmu Komputer dan Sistem Informasi]*, *5*, 28–33.

Yang, Y. Y. (2020). Network attack and Countermeasures Based on telnet connection in the era of Internet of Things. *Proceedings - 2020 International Conference on Urban Engineering and Management Science, ICUEMS 2020*, 707–710.

Yeboah-Boateng, E. O., & Kwabena-Adade, G. D. (2020). Remote Access Communications Security: Analysis of User Authentication Roles in Organizations. *Journal of Information Security*, *11*(03), 161–175.

DAFTAR RIWAYAT HIDUP

Ariel Muhammad Amri

Lahir di Bekasi pada tanggal 9 Januari 2002. Lulus dari SDN Jatiluhur 04 pada tahun 2014, lulus dari SMPN 24 Bekasi pada tahun 2017, dan lulus dari SMK Prestasi Prima pada tahun 2020.

LAMPIRAN

Dokumentasi Pengujian *Brute-Force* Honeypot Cowrie

```
cowrie@security: ~/cowrie/var/log/cowrie
2024-07-15T09:42:50.680497Z [HoneyPotSSHTransport,5,192.168.92.1] Initialized em
ulated server as architecture: linux-x64-lsb
2024-07-15T09:42:50.681092Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug
] b'admin' authenticated with b'password'
2024-07-15T09:42:50.681298Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] st
arting service b'ssh-connection'
2024-07-15T09:42:50.682028Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug
] b'admin' trying auth b'password'
2024-07-15T09:42:50.682475Z [HoneyPotSSHTransport,6,192.168.92.1] login attempt
[b'admin'/b'123456789'] succeeded
2024-07-15T09:42:50.683749Z [HoneyPotSSHTransport,6,192.168.92.1] Initialized em
ulated server as architecture: linux-x64-lsb
2024-07-15T09:42:50.684272Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug
] b'admin' authenticated with b'password'
2024-07-15T09:42:50.684576Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] st
arting service b'ssh-connection'
2024-07-15T09:42:50.684924Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug
] b'admin' trying auth b'password'
2024-07-15T09:42:50.685336Z [HoneyPotSSHTransport,7,192.168.92.1] login attempt
[b'admin'/b'password'] succeeded
2024-07-15T09:42:50.686458Z [HoneyPotSSHTransport,7,192.168.92.1] Initialized em
ulated server as architecture: linux-x64-lsb
2024-07-15T09:42:50.687117Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug
] b'admin' authenticated with b'password'
```

Dokumentasi Pengujian *Login* SSH dan Telnet Honeypot Cowrie

Berikut ini adalah dokumentasi hasil pengujian *login* SSH Honeypot Cowrie.

```
2024-07-26T07:23:11.725917Z [twisted.conch.ssh.session#info] Getting shell
2024-07-26T07:24:48.502232Z [HoneyPotSSHTransport,1,192.168.92.1] CMD: whoami
2024-07-26T07:24:48.508655Z [HoneyPotSSHTransport,1,192.168.92.1] Command found:
 whoami
2024-07-26T07:24:52.343182Z [HoneyPotSSHTransport,1,192.168.92.1] CMD: id
2024-07-26T07:24:52.347334Z [HoneyPotSSHTransport,1,192.168.92.1] Command found:
 id
2024-07-26T07:24:57.828670Z [HoneyPotSSHTransport,1,192.168.92.1] CMD: cd /
2024-07-26T07:24:57.832323Z [HoneyPotSSHTransport,1,192.168.92.1] Command found:
 cd /
2024-07-26T07:25:00.091650Z [HoneyPotSSHTransport,1,192.168.92.1] CMD: ls
2024-07-26T07:25:00.095189Z [HoneyPotSSHTransport,1,192.168.92.1] Command found:
 ls
2024-07-26T07:25:38.171677Z [HoneyPotSSHTransport,1,192.168.92.1] CMD: cd sbin
2024-07-26T07:25:38.176225Z [HoneyPotSSHTransport,1,192.168.92.1] Command found:
 cd sbin
2024-07-26T07:25:39.182677Z [HoneyPotSSHTransport,1,192.168.92.1] CMD: ls
2024-07-26T07:25:39.185693Z [HoneyPotSSHTransport,1,192.168.92.1] Command found:
 ls
2024-07-26T07:25:40.677078Z [HoneyPotSSHTransport,1,192.168.92.1] CMD: exit
2024-07-26T07:25:40.680573Z [HoneyPotSSHTransport,1,192.168.92.1] Command found:
 exit
2024-07-26T07:25:40.682792Z [twisted.conch.ssh.session#info] exitCode: 0
2024-07-26T07:25:40.683914Z [cowrie.ssh.connection.CowrieSSHConnection#debug] se
```

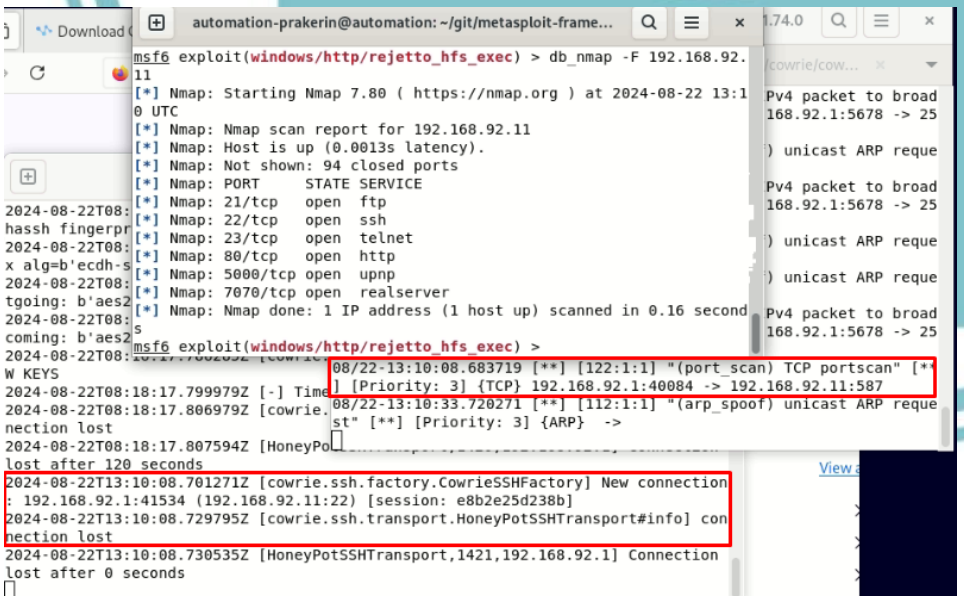
Berikut ini adalah dokumentasi hasil pengujian *login* Telnet Honeypot Cowrie.

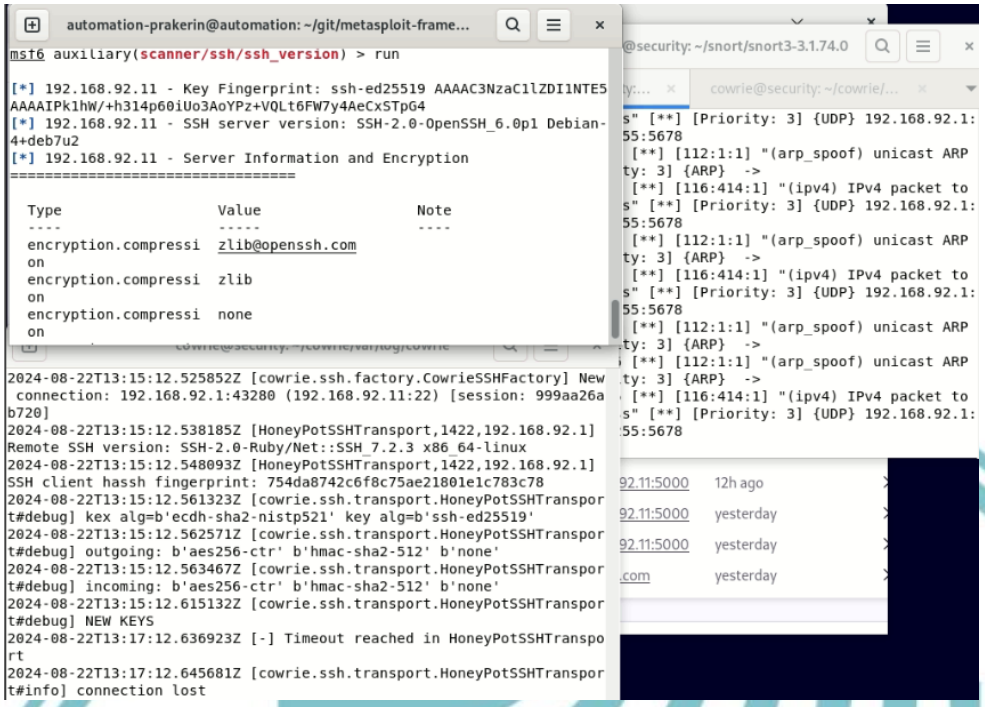
```
automation-prakerin@automation:~$ telnet 192.168.92.11
Trying 192.168.92.11...
Connected to 192.168.92.11.
Escape character is '^]'.
login: security
Password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
security@ssh_server:~$ id
uid=1001(security) gid=1001(security) groups=1001(security)
security@ssh_server:~$ whoami
security
security@ssh_server:~$ ls
phil
security@ssh_server:~$ exit
```

Dokumentasi Pemindaian Port Honeypot Cowrie

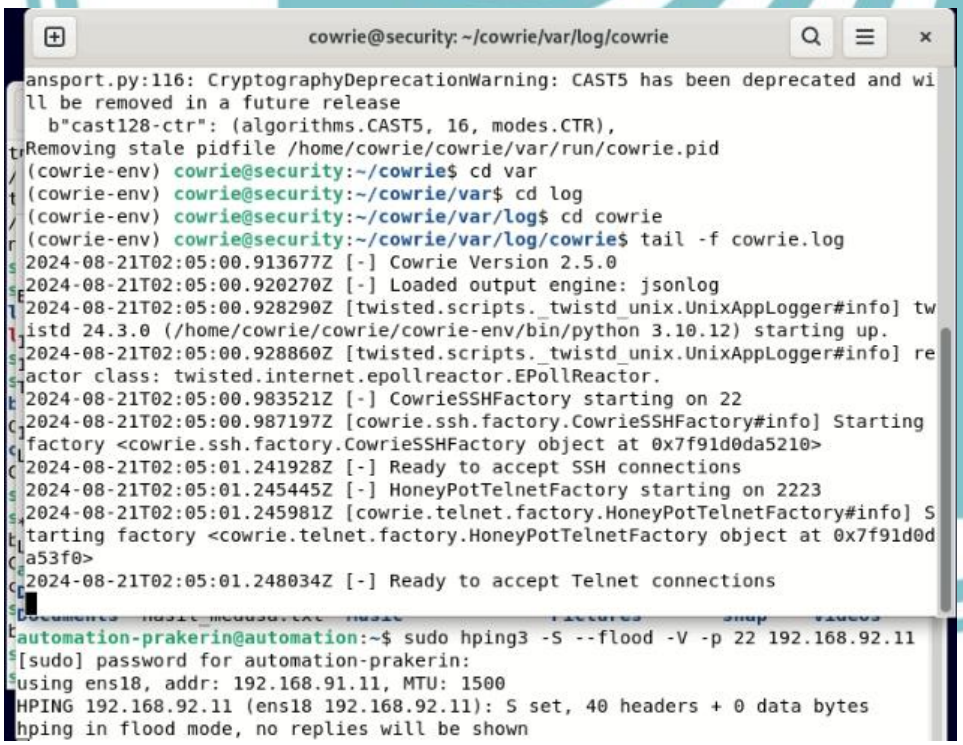
```
2024-07-15T10:35:30.015863Z [cowrie.ssh.factory.CowrieSSHFactory] New connection
: 192.168.92.1:35740 (192.168.92.253:22) [session: 27c124fa67e6]
2024-07-15T10:35:30.025759Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] con
nection lost
2024-07-15T10:35:30.026289Z [HoneyPotSSHTransport,0,192.168.92.1] Connection los
t after 0 seconds
```

Dokumentasi Pengujian Penetrasi Honeypot Cowrie





Dokumentasi Pengujian DoS Honeypot Cowrie



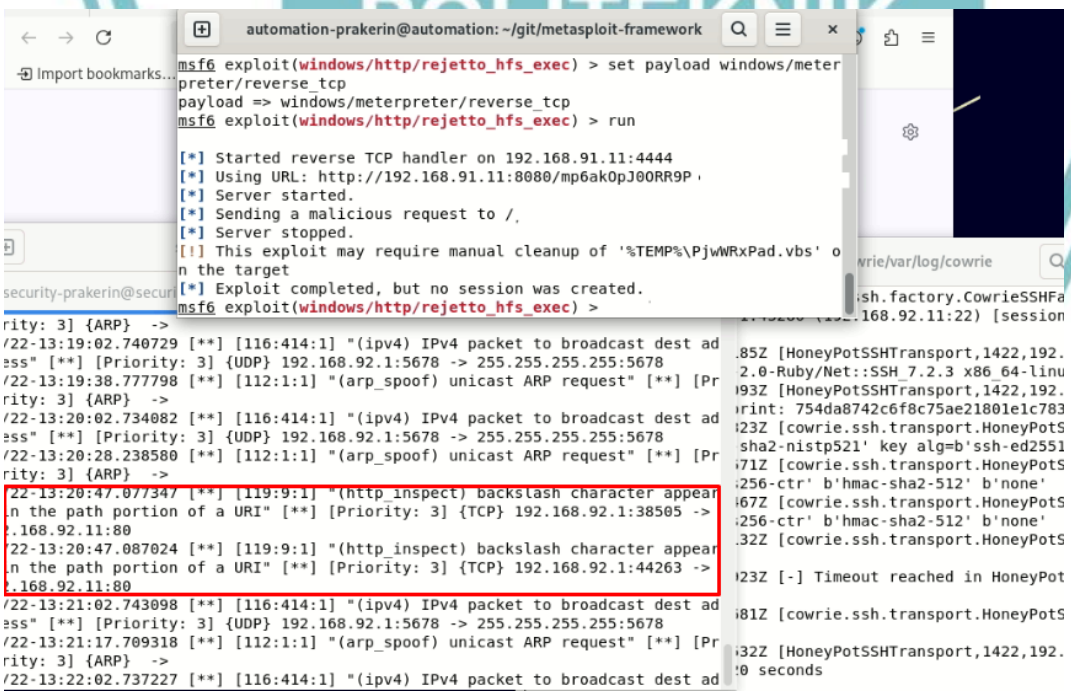
Dokumentasi Pengujian Brute-Force Snort IPS

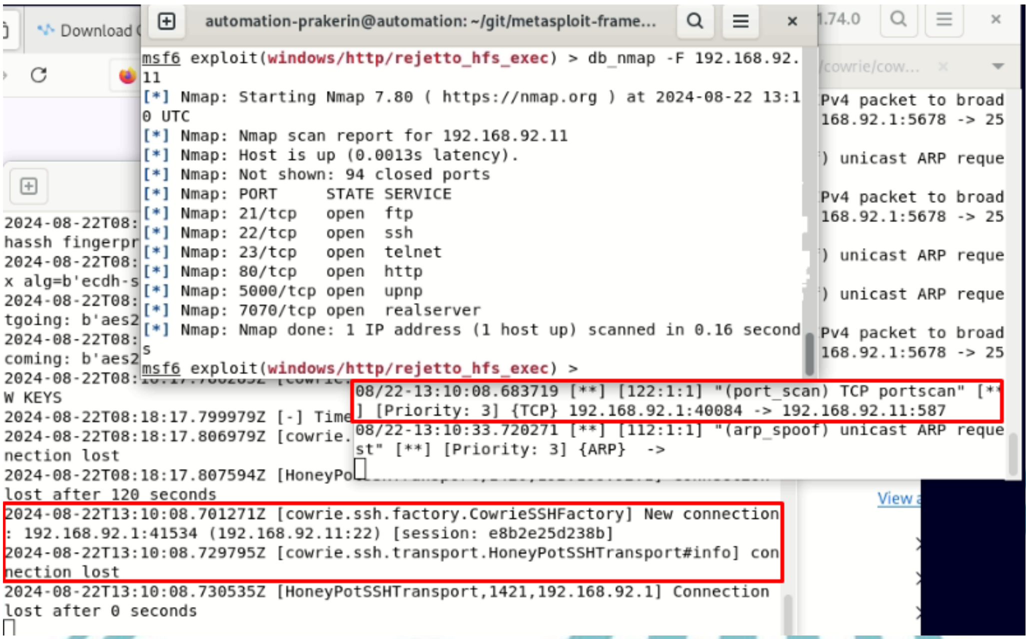
```
07/17-08:10:13.798478 [**] [129:1:1] "(stream_tcp) SYN on established session" [
**] [Priority: 3] {TCP} 192.168.92.1:33868 -> 192.168.92.253:22
07/17-08:10:13.799284 [**] [129:1:1] "(stream_tcp) SYN on established session" [
**] [Priority: 3] {TCP} 192.168.92.1:33944 -> 192.168.92.253:22
07/17-08:10:14.222767 [**] [129:3:1] "(stream_tcp) data sent on stream not accep
ting data" [**] [Priority: 3] {TCP} 192.168.92.1:33646 -> 192.168.92.253:22
07/17-08:10:14.222931 [**] [129:1:1] "(stream_tcp) SYN on established session" [
**] [Priority: 3] {TCP} 192.168.92.1:34296 -> 192.168.92.253:22
07/17-08:02:43.352466 [**] [128:6:1] "(ssh) payload size incorrect for the given
 payload" [**] [Priority: 3] {TCP} 192.168.92.253:22 -> 192.168.92.1:34374
07/17-08:10:14.418109 [**] [129:3:1] "(stream_tcp) data sent on stream not accep
ting data" [**] [Priority: 3] {TCP} 192.168.92.1:34130 -> 192.168.92.253:22
07/17-08:10:14.418591 [**] [129:3:1] "(stream_tcp) data sent on stream not accep
ting data" [**] [Priority: 3] {TCP} 192.168.92.1:34130 -> 192.168.92.253:22
07/17-08:06:22.878481 [**] [128:6:1] "(ssh) payload size incorrect for the given
 payload" [**] [Priority: 3] {TCP} 192.168.92.253:22 -> 192.168.92.1:34174
07/17-08:10:14.418879 [**] [129:3:1] "(stream_tcp) data sent on stream not accep
ting data" [**] [Priority: 3] {TCP} 192.168.92.1:34130 -> 192.168.92.253:22
07/17-08:10:14.751960 [**] [129:3:1] "(stream_tcp) data sent on stream not accep
ting data" [**] [Priority: 3] {TCP} 192.168.92.1:33646 -> 192.168.92.253:22
07/17-08:10:15.040870 [**] [129:3:1] "(stream_tcp) data sent on stream not accep
ting data" [**] [Priority: 3] {TCP} 192.168.92.1:34130 -> 192.168.92.253:22
07/17-08:05:37.331023 [**] [128:6:1] "(ssh) payload size incorrect for the given
 payload" [**] [Priority: 3] {TCP} 192.168.92.1:34402 -> 192.168.92.253:22
```

Dokumentasi Pemindaian Port Snort IPS

```
07/22-02:58:33.270531 [**] [129:1:1] "(stream_tcp) SYN on established session" [
**] [Priority: 3] {TCP} 192.168.92.1:41534 -> 192.168.92.253:22
07/22-02:58:33.272971 [**] [122:4:1] "(port_scan) TCP distributed portscan" [**]
 [Priority: 3] {TCP} 192.168.92.1:55038 -> 192.168.92.253:1025
```

Dokumentasi Pengujian Penetrasi Snort IPS





Dokumentasi Pengujian DoS Snort IPS

ICMP Flood

```
07/18-07:20:09.372622 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority:
3] {ICMP} 192.168.92.1 -> 192.168.92.253
07/18-07:20:09.372622 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority:
3] {ICMP} 192.168.92.1 -> 192.168.92.253
07/18-07:20:09.372622 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority:
3] {ICMP} 192.168.92.1 -> 192.168.92.253
07/18-07:20:09.372666 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority:
3] {ICMP} 192.168.92.1 -> 192.168.92.253
07/18-07:20:09.372666 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority:
3] {ICMP} 192.168.92.1 -> 192.168.92.253
07/18-07:20:09.372666 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority:
3] {ICMP} 192.168.92.1 -> 192.168.92.253
07/18-07:20:09.372666 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority:
3] {ICMP} 192.168.92.1 -> 192.168.92.253
07/18-07:20:09.372666 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority:
3] {ICMP} 192.168.92.1 -> 192.168.92.253
07/18-07:20:09.372719 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority:
3] {ICMP} 192.168.92.1 -> 192.168.92.253
07/18-07:20:09.372719 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority:
3] {ICMP} 192.168.92.1 -> 192.168.92.253
07/18-07:20:09.372719 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority:
3] {ICMP} 192.168.92.1 -> 192.168.92.253
07/18-07:20:09.372719 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority:
3] {ICMP} 192.168.92.1 -> 192.168.92.253
```

SYN TCP Flood Port 22

```
07/18-06:39:40.576207 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:20932 -> 192.168.92.253:22
07/18-06:39:40.576207 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:20423 -> 192.168.92.253:22
07/18-06:39:40.636383 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:24033 -> 192.168.92.253:22
07/18-06:39:40.668330 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:26216 -> 192.168.92.253:22
07/18-06:39:40.668330 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:26075 -> 192.168.92.253:22
07/18-06:39:40.732307 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:29113 -> 192.168.92.253:22
07/18-06:39:40.832474 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:56831 -> 192.168.92.253:22
07/18-06:39:40.832474 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:33749 -> 192.168.92.253:22
07/18-06:39:40.956407 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:62975 -> 192.168.92.253:22
07/18-06:39:40.956407 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:62259 -> 192.168.92.253:22
07/18-06:39:40.992315 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:42560 -> 192.168.92.253:22
07/18-06:39:40.992315 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:42431 -> 192.168.92.253:22
```

SYN TCP Flood Port 80

```
07/18-06:51:50.460473 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:38378 -> 192.168.92.253:80
07/18-06:51:50.556569 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:41755 -> 192.168.92.253:80
07/18-06:51:50.556569 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:42807 -> 192.168.92.253:80
07/18-06:51:50.556570 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:42241 -> 192.168.92.253:80
07/18-06:51:50.556570 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:41903 -> 192.168.92.253:80
07/18-06:51:50.556570 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:42809 -> 192.168.92.253:80
07/18-06:51:50.588251 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:43626 -> 192.168.92.253:80
07/18-06:51:50.588251 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:43966 -> 192.168.92.253:80
07/18-06:51:50.684349 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:47943 -> 192.168.92.253:80
07/18-06:51:50.876427 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:53896 -> 192.168.92.253:80
07/18-06:51:50.876427 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:53898 -> 192.168.92.253:80
07/18-06:51:50.944258 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [
Priority: 3] {TCP} 192.168.92.1:56133 -> 192.168.92.253:80
```

SYN TCP Flood Port 0

```
07/18-06:36:11.015427 [**] [116:446:1] "(tcp) TCP port 0 traffic" [**] [Priority
: 3] {TCP} 192.168.92.253:0 -> 192.168.92.1:48493
07/18-06:36:11.015456 [**] [116:446:1] "(tcp) TCP port 0 traffic" [**] [Priority
: 3] {TCP} 192.168.92.1:48514 -> 192.168.92.253:0
07/18-06:36:11.015456 [**] [116:446:1] "(tcp) TCP port 0 traffic" [**] [Priority
: 3] {TCP} 192.168.91.11:48495 -> 192.168.92.253:0
07/18-06:36:11.015463 [**] [116:446:1] "(tcp) TCP port 0 traffic" [**] [Priority
: 3] {TCP} 192.168.92.253:0 -> 192.168.92.1:48514
07/18-06:36:11.015471 [**] [116:446:1] "(tcp) TCP port 0 traffic" [**] [Priority
: 3] {TCP} 192.168.92.253:0 -> 192.168.91.11:48495
07/18-06:36:11.015481 [**] [116:446:1] "(tcp) TCP port 0 traffic" [**] [Priority
: 3] {TCP} 192.168.92.1:48516 -> 192.168.92.253:0
07/18-06:36:11.015481 [**] [116:446:1] "(tcp) TCP port 0 traffic" [**] [Priority
: 3] {TCP} 192.168.92.1:48497 -> 192.168.92.253:0
07/18-06:36:11.015486 [**] [116:446:1] "(tcp) TCP port 0 traffic" [**] [Priority
: 3] {TCP} 192.168.92.253:0 -> 192.168.92.1:48516
07/18-06:36:11.015494 [**] [116:446:1] "(tcp) TCP port 0 traffic" [**] [Priority
: 3] {TCP} 192.168.92.253:0 -> 192.168.92.1:48497
07/18-06:36:11.015514 [**] [116:446:1] "(tcp) TCP port 0 traffic" [**] [Priority
: 3] {TCP} 192.168.91.11:48499 -> 192.168.92.253:0
07/18-06:36:11.015514 [**] [116:446:1] "(tcp) TCP port 0 traffic" [**] [Priority
: 3] {TCP} 192.168.91.11:48518 -> 192.168.92.253:0
07/18-06:36:11.015521 [**] [116:446:1] "(tcp) TCP port 0 traffic" [**] [Priority
: 3] {TCP} 192.168.92.253:0 -> 192.168.91.11:48499
```

Statistik Paket Log Snort Brute-Force

Packet Statistics

---

ssh

packets: 131463

allowed: 397088

dropped: 20695

Statistik Paket Log Snort DoS

DoS TCP SYN TCP Flood

Packet Statistics

---

daq

packets: 37494550

allowed: 344804

dropped: 34049709

DoS TCP ICMP Flood

Packet Statistics

---

daq

packets: 35999358

allowed: 3353711

dropped: 32645646
