Rancang Bangun Sistem Keamanan Jaringan *Digital Signage* Menggunakan *Honeypot*

Maulidi[1], Atthariq[2*], Novira Dwina[3]

[1,2,3] *Jurusan Tekniknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe*
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA
[1]dmauli413@gmail.com
[2*]atthariq@pnl.ac.id
[3]noviradwina@pnl.ac.id

Abstrak—Di era digital saat ini, keamanan informasi menjadi prioritas utama, terutama mengingat meningkatnya ancaman terhadap jaringan dan server, termasuk pada jaringan *Digital Signage* PT. PLN Nusantara Power Up Arun Lhokseumawe. Insiden baru-baru ini melibatkan upaya seorang oknum yang berhasil mengakses server Xibo dan mengunggah konten yang tidak seharusnya, menunjukkan perlunya strategi keamanan yang lebih canggih. Penelitian ini meneliti penerapan *Honeypot Cowrie,* perangkat lunak *Honeypot* dengan interaksi tingkat menengah, yang bertujuan untuk menyamarkan layanan pada server dan mendeteksi serangan terhadap SSH, *Telne*t, dan *Open*SSH. Melalui metode studi literatur, sistem dirancang, diuji, dan dianalisis. *Honeypot Cowrie* terbukti efektif dalam mendeteksi serangan pada jaringan *Digital Signage*, dengan tingkat keberhasilan 100% untuk serangan *Port Scanning attack*, 90% untuk *Brute force attack*, 100% untuk *Remote Login Attack* dan 90% untuk *Denial of Service* (DoS) *Attack*. Meskipun penyerang berhasil menemukan *port* SSH, teknik *Honeypot Cowrie* dan konfigurasi *port* yang tidak standar berhasil mengelabui penyerang dan menjaga keamanan server.
Kata kunci : Keamanan Jaringan, Digital Signage, Honeypot Cowrie.

Abstract—In today's digital era, information security is a top priority, especially given the increasing threats to networks and servers, including PT PLN Nusantara Power Up Arun Lhokseumawe's Digital Signage network. A recent incident involving the efforts of an unscrupulous individual who successfully accessed the Xibo server and uploaded inappropriate content, demonstrates the need for a more sophisticated security strategy. This research examines the implementation of Cowrie's Honeypot, a Honeypot software with mid-level interaction, which aims to disguise services on the server and detect attacks against SSH, Telnet, and OpenSSH. Through the literature study method, the system was designed, tested, and analyzed. Cowrie's honeypot proved effective in detecting attacks on Digital Signage networks, with 100% success rate for Port Scanning attack, 90% for Brute force attack, 100% for Remote Login Attack and 90% for Denial of Service (DoS) Attack. Although the attacker managed to find the SSH port, Cowrie's Honeypot technique and non-standard port configuration managed to trick the attacker and maintain server security.
Keywords: Network Security, Digital Signage, Honeypot Cowrie.

I. Pendahuluan

Dalam era digital yang terus berkembang, penggunaan jaringan *Digital Signage* menjadi semakin meluas, termasuk pada perusahaan-perusahaan besar seperti PT PLN Nusantara Power Up Arun Lhokseumawe. *Digital Signage* menyajikan platform yang efektif untuk menyampaikan informasi visual secara dinamis kepada karyawan, pengunjung dan mitra usaha. Meskipun memberikan keuntungan dalam penyampaian informasi, keamanan jaringan *Digital Signage* menjadi aspek penting yang harus diperhatikan.

PT. PLN Nusantara Power Up Arun Lhokseumawe, sebagai perusahaan energi terkemuka, mengandalkan infrastruktur *Digital Signage* untuk menyampaikan informasi operasional, keamanan, dan lainnya. Dalam konteks ini, keamanan jaringan *Digital Signage* sebagai prioritas utama untuk melindungi integritas data, menjaga kontinuitas operasional, dan menghindari potensi kerugian akibat serangan ciber.

Tetapi, sampai saat ini, tantangan keamanan jaringan *Digital Signage* masih menjadi fokus perhatian di banyak organisasi, termasuk perusahaan energi seperti PT. PLN Nusantara Power Up Arun Lhokseumawe. Ancaman ciber seperti serangan p*ort scanning* SSH*, brute force, malware,* perusakan data, atau gangguan operasional lainnya, bisa mengancam keandalan sistem serta kepercayaan *stakeholder.*

Perkembangan pesat teknologi informasi dan perangkat lunak menuntut peningkatan keamanan sistem informasi untuk mencegah akses ilegal oleh perangkat yang tidak sah. Keamanan sistem informasi bertujuan untuk melindungi efisiensi, kerahasiaan, integritas, dan keandalan sistem dari berbagai ancaman, baik dari manusia maupun perangkat lunak berbahaya seperti virus dan trojan. Untuk menjamin keamanan, beberapa domain penting seperti kontrol akses, telekomunikasi, dan pengembangan sistem harus dipertimbangkan. Strategi pengamanan mencakup langkah preventif, seperti penggunaan *firewall* dan SSL, serta upaya *recovery* untuk memperbaiki kerusakan yang telah terjadi [1].

Namun, untuk mengevaluasi efektivitas *Honeypot Cowrie* dalam implementasi di jaringan *Digital Signage* PT. PLN Nusantara Power Up Arun. Apakah *Honeypot Cowrie* mampu memberikan perlindungan yang memadai dan mendeteksi ancaman dengan akurat dan apakah notifikasi yang dikirim melalui telegram dapat memberikan informasi secara *real-time* untuk respons yang cepat terhadap serangan.

Honeypot adalah mekanisme pertahanan jaringan yang berfungsi sebagai duplikasi layanan palsu dari server asli dan

tersedia secara *open source* tanpa biaya. *Honeypo*t bisa menjadi alternatif *firewall* jika biaya menjadi pertimbangan dalam mengamankan server. Terdapat tiga jenis *Honeypot* yang dapat dipilih sesuai kebutuhan, *Low Interaction Honeypot* (LIH) yang berinteraksi minimal dan mudah dikonfigurasikan, *Medium Interaction Honeypot* (MIH) yang meniru layanan server utama pada server virtual dengan kemampuan mengumpulkan informasi lebih banyak, dan *High Interaction Honeypot* (HIH) yang menawarkan interaksi tertinggi dengan sistem operasi asli, meskipun konfigurasi lebih rumit dan risiko lebih tinggi jika penyusup berhasil membongkar jebakannya [2].

Cowrie adalah perangkat lunak *Honeypot Medium Interaction* yang dirancang untuk menyamarkan layanan di server *openSSH* dan mendeteksi serta mencatat serangan *brute force* pada server SSH, *Telnet*, dan *OpenSSH*. Dengan menggunakan konsep *redirection*, *Cowrie* mengalihkan penyerang ke layanan *Honeypot* palsu setelah serangan *openSSH* berhasil, sehingga penyerang percaya bahwa mereka telah sukses, padahal sebenarnya mereka terperangkap dalam sistem palsu. Fitur utama *Cowrie* adalah kemampuannya dalam melakukan *logging*, yang memungkinkan administrator jaringan untuk memantau dan menganalisis aktivitas penyerang secara mendetail dalam sistem tersebut [3].

Digital Signage adalah sistem tampilan yang menampilkan informasi dan konten multimedia seperti gambar, video, dan teks melalui layar datar seperti LCD, LED, atau plasma. Berbeda dengan media televisi yang menggunakan penyampaian pesan secara luas (broadcast), *Digital Signage* menggunakan pendekatan *narrowcast* yang lebih terarah. Keuntungan menggunakan *Digital Signage* meliputi kemampuan untuk menarik perhatian audiens dengan konten dinamis, memperbarui pesan sesuai waktu dan situasi, menghemat biaya dan waktu dengan menggabungkan berbagai media konvensional dalam satu *platform*, memaksimalkan return on *investment* melalui penjualan ruang iklan, dan meningkatkan citra perusahaan dengan teknologi modern. Digital Signage memungkinkan pengeditan dan penjadwalan konten secara terintegrasi, serta mendukung berbagai jenis media digital seperti teks, gambar, audio, animasi, dan video [4].

XIBO adalah aplikasi *open source* untuk *Digital Signage* yang dikelola oleh *Spring Signage*. Dikembangkan sebagai proyek universitas oleh James Packer dan diperkenalkan ke publik pada tahun 2006 dengan lisensi AGPLv3, *XIBO* mengelola konten dan penjadwalan melalui web administration panel berbasis PHP/MySQL. (.NET) dan Ubuntu (Python), serta perangkat display seperti TV dan proyektor. *Xibo* Server berfungsi untuk mengelola konten dan penjadwalan, sedangkan *Xibo Client* menampilkan konten pada monitor LCD. *Xibo Client* dapat diinstal pada sistem operasi Windows dan Unix, dengan kebutuhan aplikasi pendukung seperti .NET *Framework* v3.5 SP1, *Flash Player*, Windows *Media Player*, *Microsoft PowerPoint*, dan Internet Explorer [5]. *Kippo-graph* adalah skrip berfitur lengkap untuk memvisualisasikan statistik dari *Honeypot Kippo*. *Kippo-graph* merupakan suatu program pendukung untuk *kippo*-SSH *Honeypot* yang digunakan untuk menggambarkan aktivitas atau kegiatan pada *port* SSH yang ditampilkan dalam bentuk diagram atau grafik [6]. Telegram adalah *platform* olah pesan seluler yang menawarkan layanan pesan yang terenkripsi sehingga pengguna dapat mengirim pesan, foto, dan video ke kontak yang dipilih secara pribadi. Telegram dapat digunakan secara gratis, dan menawarkan sebuah layanan yang memungkinkan pengembang *website* untuk mengintegrasikan *website* yang dibangun dengan aplikasi mobile Telegram. Untuk mengintegrasikan website dengan aplikasi mobile Telegram, digunakan sebuah fitur dari Telegram yaitu bot API dan chat Bot [7].

SSH adalah protokol jaringan yang memungkinkan pertukaran data melalui saluran aman antara dua perangkat jaringan, terutama banyak digunakan pada sistem berbasis Linux dan Unix untuk mengakses shell SSH dirancang sebagai pengganti telnet dan shell remote tidak lainnya yang mengirim informasi, terutama kata sandi, dalam bentuk plain text yang membuatnya mudah untuk disadap. Akan tetapi seringkali masalah keamanan jaringan dipandang sebelah mata. Selama ini para administrator jaringan hanya berusaha untuk membuat pertahanan sebaik-baiknya seperti menggunakan *firewall* dan *Intrusion Detection System* (IDS) agar jaringan lebih aman [8].

Efektivitas adalah tingkat keberhasilan dalam mencapai tujuan yang telah ditetapkan, diukur dengan membandingkan *input* dan *output*. Efektivitas merupakan faktor kunci dalam keberhasilan organisasi atau program. Sementara itu, untuk mengukur keefektifan *honeypot,* pada penelitian ini menggunakan rumus *Attack Detection Rate* (ADR). ADR adalah metrik yang digunakan untuk menilai efektivitas sistem keamanan, seperti IDS atau IPS, dalam mendeteksi serangan. ADR menunjukkan persentase serangan yang terdeteksi dibandingkan dengan total serangan yang terjadi [9].

$$\textit{Attack Detection Rate}\ (\textbf{ADR}) \quad \frac{\textit{Jumlah Serangan Terdeteksi}}{\textit{Jumlah Total Serangan}} \times 100\%$$

ADR yang tinggi menunjukkan bahwa sistem keamanan mampu mendeteksi sebagian besar serangan yang terjadi, sementara ADR yang rendah mengindikasikan bahwa banyak serangan tidak terdeteksi, yang dapat menyebabkan risiko keamanan yang lebih besar [10].

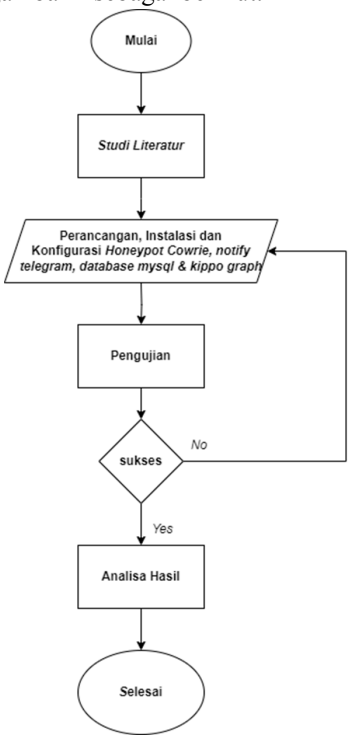
TABEL I
KLASIFIKASI KRITERIA PERSENTASE KEEFEKTIFAN

Persentase	Kriteria
>100%	Sangat Efektif
100%	Efektif
90%-99%	Cukup Efektif
75%-89%	Kurang Efektif
>75%	Tidak Efektif

II. METODOLOGI PENELITIAN

A. *Alur Penelitian*

Alur penelitian ini dilakukan melalui beberapa tahapan, ditunjukkan pada gambar 1 sebagai berikut.

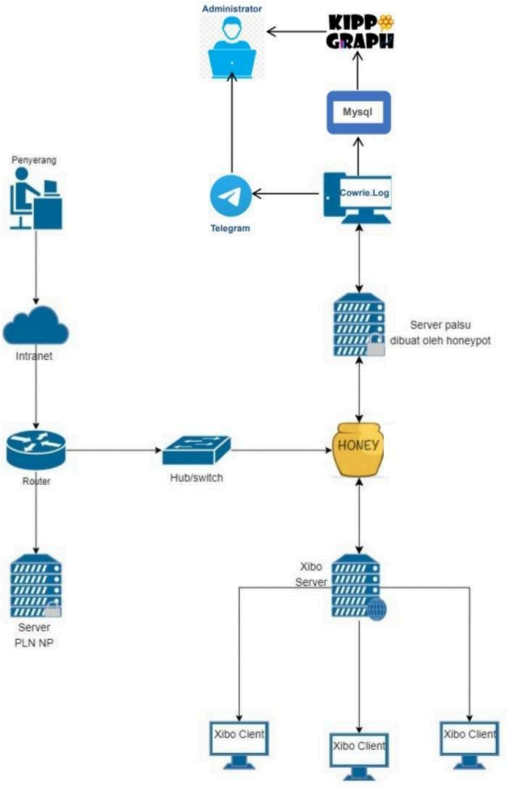


Gambar 1. Diagram Alur Penelitian

1) *Studi Literatur:* Tahap ini melibatkan pengumpulan, pembacaan, dan pemahaman jurnal ilmiah, skripsi, artikel, serta informasi dari forum dan komunitas terpercaya secara online untuk memperoleh data yang mendukung penelitian.
2) *Perancangan Sistem:* Pada tahap ini, dilakukan perancangan *Digital Signage* dan *Honeypot* untuk memudahkan implementasi. Tujuannya adalah untuk menentukan model perangkat lunak yang jelas dan memenuhi kebutuhan analisis data yang diperlukan.
3) *Pengujian Sistem:* Setelah perancangan selesai, dilakukan pengujian sistem, terutama pada aspek keamanan *Honeypot* yang telah dibangun, untuk memastikan sistem berfungsi dengan baik.
4) *Analisa Hasil Pengujian:* Tahap ini bertujuan untuk mengevaluasi apakah sistem keamanan jaringan berbasis *Honeypot* berjalan sesuai rencana, serta untuk mengidentifikasi kelebihan dan kekurangan dari sistem tersebut.

B. *Rancangan Sistem*

Adapun rancangan sistem yang digunakan untuk membangun sistem keamanan jaringan *digital signage* menggunakan *Honeypot* pada PT. PLN Nusantara Power UP Arun ditunujukkan pada gambar 2 berikut.



Gambar 2. Rancangan Sistem

Sistem *Honeypot* bekerja dengan cara menarik perhatian penyerang atau pembobol keamanan dengan membuat target yang tampaknya rentan. Ketika penyerang mencoba melakukan serangan terhadap server asli maka *Honeypot* mengalihkan penyerang ke server palsu yang telah dibuat pada *port* 2222, selanjutnya *Cowrie.log* akan merekam informasi mengenai serangan tersebut, seperti teknik penyerangan, metode penyerangan, tujuan penyerangan dan Notifikasi akan dikirim ke telegram setiap penyerang berhasil masuk ke server palsu yang telah dibuat. Dengan informasi ini perusahaan dapat meningkatkan sistem keamanan mereka dengan memperbarui sistem keamanan mereka, melacak dan mengidentifikasi ancaman, serta memahami lebih dalam mengenai serangan yang terjadi.

III. HASIL DAN PEMBAHASAN

A. *Hasil Pengujian Port Scanning Attack*

Teknik *port scanning* adalah proses pemindaian (scanning) *port* pada suatu sistem atau jaringan untuk mengidentifikasi *port-port* yang terbuka dan dapat diakses. Pengujian *Honeypot Cowrie* menggunakan teknik *port scanning* bertujuan untuk menguji keefektifan sistem *Cowrie* dalam mendeteksi aktivitas mencurigakan yang terkait dengan pemindaian *port*, pada pengujian ini penulis menggunakan Nmap sebagai *tools* untuk menjalankan serangan *port scanning*.

```
maulidi@maulidi-linux:~$ nmap 10.7.60.233
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-12 14:14 WIB
Nmap scan report for 10.7.60.233
Host is up (0.0080s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE
80/tcp   open  http
2222/tcp open  EtherNetIP-1
```

Gambar 3. Proses *Port scanning Attack*

Gambar 3 merupakan proses *port scanning Attacker* ke server *Xibo* dengan IP yang di serang 10.7.60.233, *port scanning* yang dilakukan adalah melakukan *scan* ke semua *port* pada perangkat target. Terlihat *port* yang terbuka ada dua yaitu *port* 80/tcp http dan *port* 2222/tcp milik server tiruan yang dibuat *honeypot,* yang dimana *attacker* tidak mengetahuinya.

```
2024-08-12T21:13:27.434176Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.7.60.167:55868 (10.7.60.233:2222) [session: bdd18c50c810]
2024-08-12T21:13:27.437255Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2024-08-12T21:13:27.437347Z [HoneyPotSSHTransport,0,10.7.60.167] Connection lost after 0 seconds
2024-08-12T21:13:36.495740Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.7.60.167:36474 (10.7.60.233:2222) [session: ac53bed9640c]
2024-08-12T21:13:36.498220Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2024-08-12T21:13:36.498513Z [HoneyPotSSHTransport,1,10.7.60.167] Connection lost after 0 seconds
2024-08-12T21:14:06.180162Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.7.60.167:35362 (10.7.60.233:2222) [session: 3619e8e007f7]
2024-08-12T21:14:06.182707Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2024-08-12T21:14:06.183040Z [HoneyPotSSHTransport,2,10.7.60.167] Connection lost after 0 seconds
2024-08-12T21:14:18.123821Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 10.7.60.167:44344 (10.7.60.233:2222) [session: b0c40f5e733a]
2024-08-12T21:14:18.126323Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2024-08-12T21:14:18.126637Z [HoneyPotSSHTransport,3,10.7.60.167] Connection lost after 0 seconds
```

Gambar 4. *Log* yang Dihasilkan dari *Port Scanning Attack*

Log Cowrie pada Gambar 4 mencatat serangan pemindaian *port* yang dilakukan menggunakan Nmap dari IP `10.7.60.233` ke *honeypot* dengan IP `10.7.60.167`. Serangan ini menghasilkan banyak koneksi baru ke berbagai *port*, namun semua koneksi langsung terputus setelah 0 detik, menunjukkan penggunaan teknik pemindaian cepat seperti SYN scan atau *Null* scan. Setiap koneksi memiliki ID sesi unik, tetapi berlangsung sangat singkat. Pola koneksi berulang dan cepat ini mencerminkan karakteristik pemindaian *port* agresif, di mana penyerang mencoba mengidentifikasi *port* terbuka dan layanan di server target tanpa melakukan eksploitasi lebih lanjut.

B. Hasil Pengujian Brute Force Attack

Pengujian *Brute force* adalah metode pengujian keamanan di mana berbagai kombinasi *username* dan *password* dicoba secara sistematis untuk menemukan kredensial yang benar. Pada pengujian ini penulis menggunakan *Hydra* sebagai *tools*. Alat seperti *Hydra* sering digunakan untuk melakukan serangan *Brute force* terhadap berbagai layanan jaringan ataupun suatu sistem.

```
maulidi@maulidi-linux: ~
maulidi@maulidi-linux:~$ hydra -L wordlist.txt -P wordlist.txt ssh://10.7.60.233:2222
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-12 14:44:41
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 225 login tries (l:15/p:15), ~15 tries per task
[DATA] attacking ssh://10.7.60.233:2222/
[2222][ssh] host: 10.7.60.233   login: root   password: admin
[2222][ssh] host: 10.7.60.233   login: root   password: password
[2222][ssh] host: 10.7.60.233   login: root   password: letmein
[2222][ssh] host: 10.7.60.233   login: root   password: qwerty
1 of 1 target successfully completed, 4 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-12 14:44:58
```

Gambar 5. Proses *Brute force Attacker*

Gambar 5 menunjukkan proses *Brute Force Attack* yang dilakukan terhadap server dengan IP `10.7.60.233` melalui port `2222`. Penyerang mencoba menebak kombinasi *username* dan *password* yang benar untuk masuk ke server. Beberapa kombinasi berhasil *login* ke *honeypot* yang telah disiapkan, menggunakan username "root" dan berbagai variasi password seperti "123", "qwert", "qwe123", dan "1324567890". Namun, penyerang sebenarnya bisa masuk hanya dengan username "root", tanpa harus memasukkan password atau dengan password apa saja, karena server ini sengaja dibuat rentan untuk memantau aktivitas penyerang.

```
cowrie@sinfo1: ~/cowrie/var/log/cowrie
2024-07-16T12:39:12.702257Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'maulidi' failed a
uth b'password'
2024-07-16T12:39:12.702466Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login:
()
2024-07-16T12:39:12.704459Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2024-07-16T12:39:12.704616Z [HoneyPotSSHTransport,764,10.7.60.138] Connection lost after 3 seconds
2024-07-16T12:39:12.712791Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'maulidi' failed a
uth b'password'
2024-07-16T12:39:12.713027Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login:
()
2024-07-16T12:39:12.715169Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2024-07-16T12:39:12.715383Z [HoneyPotSSHTransport,765,10.7.60.138] Connection lost after 3 seconds
2024-07-16T12:39:12.723312Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'maulidi' failed a
uth b'password'
2024-07-16T12:39:12.723546Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login:
()
2024-07-16T12:39:12.725503Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2024-07-16T12:39:12.725662Z [HoneyPotSSHTransport,767,10.7.60.138] Connection lost after 3 seconds
2024-07-16T12:39:12.732533Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'maulidi' failed a
uth b'password'
2024-07-16T12:39:12.732771Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login:
()
2024-07-16T12:39:12.735059Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2024-07-16T12:39:12.735239Z [HoneyPotSSHTransport,766,10.7.60.138] Connection lost after 3 seconds
2024-07-16T12:39:12.743094Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'maulidi' failed a
uth b'password'
2024-07-16T12:39:12.743330Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login:
()
2024-07-16T12:39:12.745284Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2024-07-16T12:39:12.745492Z [HoneyPotSSHTransport,768,10.7.60.138] Connection lost after 3 seconds
2024-07-16T12:39:12.754456Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'maulidi' failed a
uth b'password'
2024-07-16T12:39:12.754767Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login:
()
2024-07-16T12:39:12.756688Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2024-07-16T12:39:12.756871Z [HoneyPotSSHTransport,769,10.7.60.138] Connection lost after 3 seconds
2024-07-16T12:39:12.763623Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'maulidi' failed a
uth b'password'
2024-07-16T12:39:12.763793Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login:
()
```

Gambar 6. *Log* yang Dihasilkan dari *Brute force Attack*

Alert/log yang dihasilkan dalam *file* `*Cowrie.json*` menunjukkan bahwa *Cowrie* telah mendeteksi adanya serangan *Brute Force* yang berasal dari perangkat dengan IP *Address* `10.7.60.138`, yang merupakan IP *Address* dari penyerang *(Attacker)*. *Log* ini mencatat secara rinci aktivitas yang mencurigakan, di mana penyerang berusaha untuk mencoba berbagai kombinasi *username* dan *password* dengan tujuan mendapatkan akses tidak sah ke server. Deteksi ini merupakan salah satu fungsi utama *Cowrie* sebagai *honeypot,* yang dirancang untuk memantau, mencatat, dan menganalisis upaya serangan terhadap sistem, termasuk serangan *brute force* seperti yang terdeteksi dalam *log* ini

C. Hasil Pengujian Remote Login

Pengujian ini bertujuan untuk mengevaluasi efektivitas serangan *Brute Force* dengan mencoba *login* jarak jauh melalui *port* SSH yang telah disiapkan pada server *honeypot*. Kombinasi *username* dan *password* yang didapat dari pengujian *Brute Force* sebelumnya digunakan untuk *login* melalui port `2222` di SSH palsu yang disediakan oleh *Honeypot Cowrie*. Hasil pengujian ditampilkan pada Gambar 7, yang menunjukkan apakah kombinasi tersebut berhasil memberikan akses *login* ke server *honeypot* melalui port SSH yang ditargetkan.

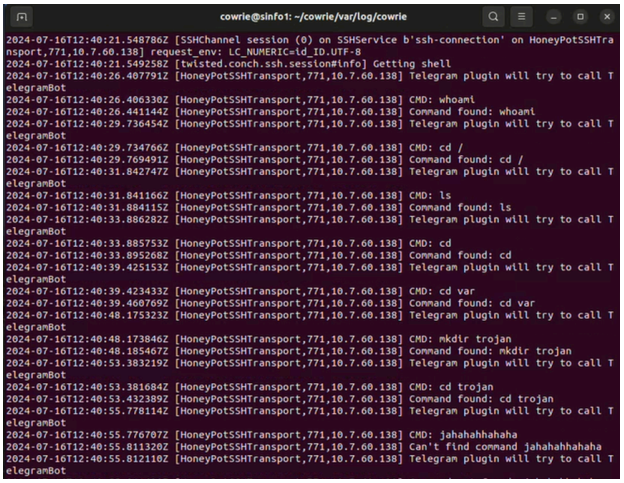
```
maulidi@maulidi-linux:~$ ssh root@10.7.60.233 -p 2222
root@10.7.60.233's password:

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.
root@Xibo:~#
```

Gambar 7. *Attacker* berhasil *login* ke server *Honeypot*

Percobaan *login* dilakukan oleh *Attacker* ke server *Honeypot* berhasil dengan *username* `root` dan *password* `123`, seolah-olah *Attacker login* ke server asli padahal *Attacker* hanya *login* ke server palsu yang dibuat oleh *Honeypot* dengan nama server "xibo".

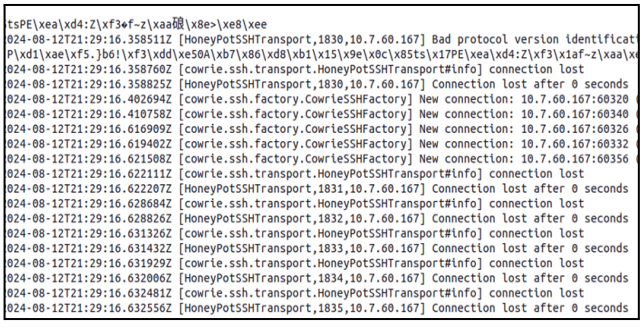


Gambar 8. Log yang Dihasilkan dari *Remote Login*

Gambar 8 menampilkan *log* deteksi yang dihasilkan oleh *Cowrie* selama upaya *remote login* yang dilakukan oleh penyerang. Penyerang mencoba menyabotase server dengan mengetikkan perintah acak. *Log* ini mencatat berbagai upaya eksploitasi, memberikan informasi penting tentang pola serangan dan niat jahat penyerang. Analisis lebih lanjut dari data *log* ini dapat membantu mengidentifikasi jenis perintah dan teknik yang sering digunakan, memungkinkan tim keamanan untuk mengembangkan aturan deteksi yang lebih efektif dan memperkuat kebijakan keamanan jaringan.

D. *Hasil Pengujian DoS Attack*

Pengujian DoS (*Denial of Service*) bertujuan untuk mengevaluasi kemampuan sistem *Honeypot* dalam mendeteksi dan menangani serangan yang mengganggu ketersediaan layanan. Dalam pengujian ini, penulis menggunakan MHDDoS sebagai alat untuk melaksanakan serangan, yang efektif dalam menghasilkan *traffic* tinggi untuk menguji ketahanan sistem. Dengan melakukan simulasi serangan ini, penulis berharap dapat mengamati sejauh mana *Honeypot* dapat mendeteksi pola serangan dan menilai respons serta mitigasi yang diterapkan, sehingga memperoleh wawasan yang lebih dalam mengenai efektivitas sistem *Honeypot.*

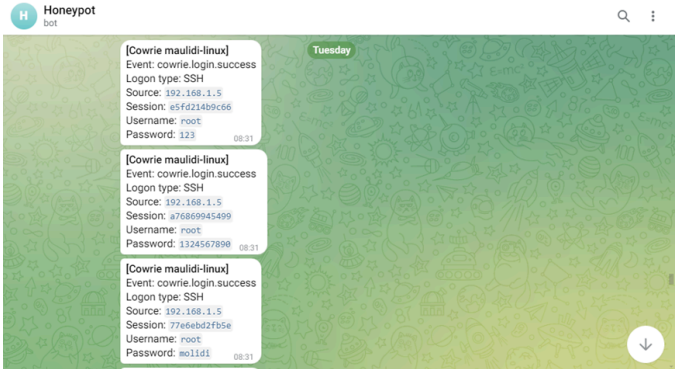


Gambar 9. *Log* yang dihasilkan *Cowrie* dari DDoS *Attack*

Gambar 9 merupakan *alert/log* deteksi yang dihasilkan oleh *Cowrie* pada perangkat server yang diserang menggunakan metode serangan *denial of service attack* menggunakan *tools* MHDDoS yang dilakukan oleh perangkat dengan IP *Address* 10.7.60.167 yang merupakan IP *Address Attacker. Honeypot Cowrie* berhasil mendeteksi serangan DDoS dan tidak membuat server SSH asli terganggu atau terpenuhi oleh serangan DDoS.

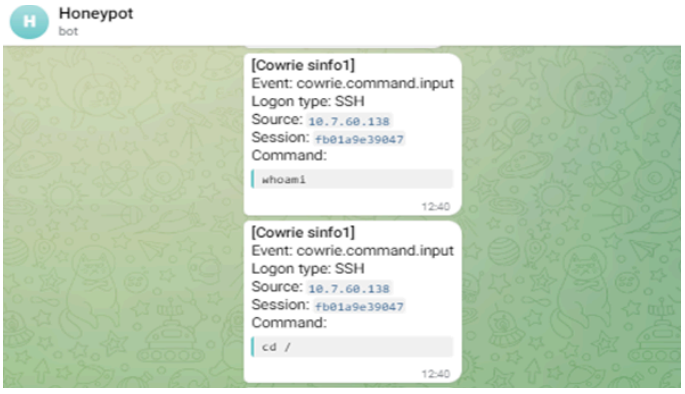
E. *Hasil Notifikasi Telegram*

Notifikasi akan dikirim ke bot Telegram saat serangan *Brute Force* berhasil menemukan kombinasi *username* dan *password* yang sah, yang memungkinkan akses ke server SSH *Honeypot.* Notifikasi ini bertujuan untuk memberi peringatan dini dan membantu dalam pemantauan aktivitas berbahaya pada server.



Gambar 10. Notifikasi Telegram dari *Brute force Attack*

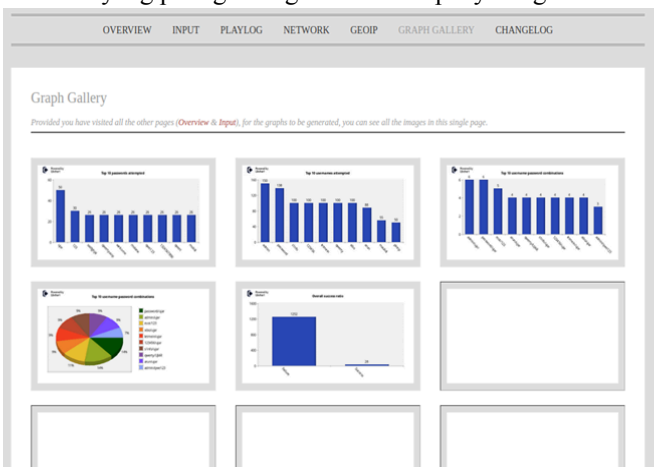
Gambar 11 menunjukkan notifikasi yang dikirim ke bot Telegram saat *attacker* berhasil login ke server *Honeypot* dengan metode *remote login* dan mengetikkan perintah-perintah yang dilakukan oleh penyerang. Semua aktivitas ini terdeteksi dan tercatat di bot Telegram. Notifikasi ini memberikan pemantauan *real-time* kepada administrator jaringan, memungkinkan mereka untuk segera mengetahui dan merespons upaya intrusi. Dengan demikian, penggunaan bot Telegram sebagaialat notifikasi meningkatkan kemampuan deteksi dini dan respons terhadap serangan, sehingga membantu dalam mengurangi potensi kerusakan pada sistem secara efektif.



Gambar 11. Notifikasi Telegram dari serangan *Remote Login*

F. *Hasil Kippo Graph*

Gambar 12 menunjukkan grafik dari *Kippo Graph,* antarmuka web yang digunakan untuk menampilkan data dari *Kippo, honeypot* yang mensimulasikan server SSH rentan. *Kippo* memantau aktivitas penyerang, khususnya serangan brute force pada layanan SSH. *Kippo Graph* memproses *log Kippo* dan menyajikannya secara visual. Fitur utamanya meliputi grafik serangan *brute force* yang menampilkan upaya *login* gagal berdasarkan waktu, serta daftar *username* dan *password* yang paling sering dicoba oleh penyerang.



Gambar 12. *Kippo Graph*

G. *Keefektifan*

Penelitian ini mengevaluasi efektivitas *Honeypot Cowrie* dalam mendeteksi serangan menggunakan metrik *Attack Detection Rate* (ADR). Pada serangan *Port Scanning*, *Honeypot* mendeteksi seluruh serangan yaitu dari 10 kali percobaan serangan, menghasilkan ADR 100%. Untuk *Brute Force*, *Honeypot* mendeteksi 9 dari 10 serangan, dengan ADR 90%, karena serangan ke *port default* SSH (port 22) tidak terdeteksi. Dalam percobaan *Remote Login*, *Honeypot* mendeteksi semua serangan, memberikan ADR 100%. Pada serangan *Denial of Service* (DoS), *Honeypot* mendeteksi 9 dari 10 serangan dengan ADR 90%, mirip dengan *Brute Force*, karena *port* 22 tidak aktif. *Honeypot Cowrie* menunjukkan deteksi yang efektif pada berbagai serangan.

TABEL II
KEEFEKTIFAN *HONYEPOT COWRIE*

Metode Serangan	Persentase	Kriteria
Port Scanning Attack	100%	Efektif
Brute Force Attack	90%	Cukup Efektif
Remote Login	100%	Efektif
DoS *Attack*	90%	Cukup Efektif

IV. KESIMPULAN

Honeypot Cowrie menunjukkan keefektifan yang tinggi dalam mendeteksi berbagai jenis serangan pada jaringan *digital signage*, dengan tingkat keberhasilan 100% untuk *Port Scanning Attack*, 90% untuk *Brute force Attack*, 100% untuk *Remote Login Attac*k dan 90% untuk *Denial of Service* (DoS) *Attack*. Meskipun penyerang berhasil menemukan *port* server SSH melalui *port scanning Attack* atau *brute force attack*, server tetap terlindungi. Teknik *honeypot Cowrie* dan konfigurasi *port* yang tidak standar, efektif dalam mengelabui penyerang dan mencegah akses tidak sah.

REFERENSI

[1] Farizy, S., & Eriana, E. S. (2022). Keamanan sistem informasi. Unpam Press, Tangerang Selatan-Banten, Universitas Pamulang.

[2] Sulaksono, W. A., & Suharyanto, C. E. (2020). Implementasi *Honeypot* Sebagai Sistem Keamanan Jaringan Pada Virtual Private Server. 5.

[3] Susanti, R. E., Muhammad, A. W., & Prabowo, W. A. (2022). Implementasi *Intrusion Prevention System* (IPS) OSSEC dan *Honeypot Cowrie*. Jurnal Sisfokom. 11(1), 73–78.

[4] Panuntun, R., Rochim, A. F., & Martono, K. T. (2015). Perancangan Papan Informasi Digital Berbasis Web pada *Raspberry-pi*. Jurnal Teknologi dan Sistem Komputer, 3(2),192–197.

[5] Wahid, A., & Luhriyani, S. (2017). Pengembangan Model *Online Digital Signage* berbasis *XIBO* di Fakultas Bahasa dan Sastra UNM. Seminar Nasional LP2M UNM, 2(1).

[6] Samudra, M. I. (2016). Simulasi *Kippo Honeypot* dengan *Kippo-Graph* sebagai Pengumpulan Informasi Serangan pada Jaringan [Thesis, Program Studi Teknik Informatika FTI-UKSW].

[7] Uray Ristian, F., Ikhwan Ruslianto. (2019). Implementasi *Honeypot Kipo* pada Sistem Keamanan Server Berbasis Web Monitoring dengan Notifikasi Otomatis menggunakan API Telegram. Coding Jurnal Komputer dan Aplikasi, 7(03).

[8] Desmira, D., & Wiryadinata, R. (2022). Rancang Bangun Keamanan *Port Secure Shell* (SSH) Menggunakan Metode *Port Knocking*. INSANtek, 3(1), 1–5.

[9] Sahara, A. D., Sapri, S., & Akbar, A. A. (2024). *The Design And Implementation Of Computer Network Monitoring And Security System Using Linux Ubuntu Server. Journal Media Computer Science*, 3(1), 1–16.

[10] Ahmad, W., Raza, M. A., Nawaz, S., & Waqas, F. (2023). *Detection and Analysis of Active Attacks using Honeypot. International Journal of Computer Applications*, 184(50), 27–31