IMPLEMENTASI BOTNET SEDERHANA MENGGUNAKAN BAHASA PEMROGRAMAN C DAN C&C SERVER BERBASIS LINUX

Nurhuda Maulana, Radinal Setyadinsa, Musthofa Galih Pradana

Program Studi Teknik Informatika, Universitas Pembangunan Nasional Veteran Jakarta
Jl. R.S Fatmawati No. 1, Cilandak, Jakarta Selatan
nurhudamaulana@upnvj.ac.id, radinalsetyadinsa@upnvj.ac.id,
musthofagalihpradana@upnvj.ac.id

Abstract - Botnets pose a serious threat to network security. They are often exploited to launch attacks, cause damage, and steal sensitive information. This research aims to implement a simple botnet using the C programming language and a Linux-based Command and Control (C&C) Server. The methodology involves developing a bot application that runs on the Windows operating system and is capable of communicating with the C&C Server. The bot is distributed through a click-based mechanism using phishing files placed on USB flash memory. The results of this study demonstrate that the implementation of a simple botnet using the C programming language and a Linux-based C&C Server enables the authors to understand the basic mechanisms of botnet operation and structure. This research provides valuable insights into the workings of botnets and emphasizes the importance of developing effective security strategies to combat botnet threats.
Keywords - Botnet, bahasa pemrograman C, C&C Server, Network Security.

Abstrak **–** Botnet menjadi ancaman yang serius dalam keamanan jaringan. Botnet sering disalahgunakan untuk melancarkan serangan dan merusak serta mencuri informasi sensitif. Penelitian ini bertujuan untuk mengimplementasikan sebuah botnet sederhana menggunakan bahasa pemrograman C dan *Command and Control* (C&C) Server berbasis linux. Metode yang digunakan melibatkan pengembangan aplikasi bot yang berjalan di sistem operasi Windows dan mampu melakukan komunikasi dengan C&C Server. Penyebaran bot melalui mekanisme klik berupa berkas *phising* yang ditempatkan pada *USB flash memory*. Hasil penelitian menunjukkan bahwa implementasi botnet sederhana menggunakan bahasa pemrograman C dan C&C server berbasis Linux memungkinkan penulis memahami mekanisme dasar dalam operasi dan struktur botnet. Penelitian ini memberikan wawasan yang berharga tentang cara kerja botnet dan pentingnya pengembangan strategi keamanan yang efektif untuk melawan ancaman botnet.
Kata Kunci - Botnet, bahasa pemrograman C, C&C server, Linux, keamanan jaringan.

I. PENDAHULUAN

Keamanan Jaringan termasuk isu yang cukup viral di era digital saat ini. Berbagai kasus seperti malware, spyware, bahkan pencurian data ramai diberitakan media masa. Botnet adalah jaringan komputer yang terdiri dari sejumlah besar perangkat yang terinfeksi dan dikendalikan oleh pihak yang tidak sah[1]. Botnet seringkali disalahgunakan untuk melancarkan serangan, merusak sistem, dan mencuri informasi sensitif.

Bahasa pemrograman C dan server Linux merupakan komponen penting dalam pengembangan perangkat lunak dan infrastruktur jaringan. Bahasa pemrograman C digunakan oleh banyak pengembang perangkat lunak terlebih dalam pemrograman jaringan. Penggunaan bahasa pemrograman C memberikan fleksibilitas dan kontrol yang tinggi. Server linux menyediakan kestabilan dan kinerja yang andal dalam operasi jaringan.

penelitian ini bertujuan untuk mengimplementasikan sebuah botnet sederhana dengan menggunakan bahasa pemrograman C dan Command and Control (C&C) server berbasis Linux. Tujuan utama dari penelitian ini adalah untuk memahami mekanisme dasar operasi dan struktur botnet dengan memanfaatkan bahasa pemrograman C dan server Linux.

Dalam penelitian ini, kami akan menjelaskan langkah-langkah yang dilakukan dalam merancang dan membangun botnet sederhana, termasuk pengembangan modul bot, penyebaran bot melalui mekanisme infeksi, dan pengaturan komunikasi antara bot dan C&C server. Kami juga akan menganalisis potensi ancaman yang dapat ditimbulkan oleh botnet yang diimplementasikan.

Penelitian ini memberikan wawasan yang berharga tentang cara kerja botnet dan pentingnya pengembangan strategi keamanan yang efektif untuk melawan ancaman botnet yang semakin kompleks. Diharapkan hasil dari penelitian ini dapat membantu para profesional keamanan dan peneliti untuk mengembangkan solusi yang efektif dalam melindungi infrastruktur jaringan dari serangan botnet yang merusak dan mencuri informasi sensitif.

A. Socket Programming

Socket programming adalah teknik yang digunakan dalam implementasi sistem client-server untuk botnet. Melalui socket programming, botmaster dapat mengontrol dan berkomunikasi dengan bot yang

terinfeksi secara efisien. Implementasi ini melibatkan penggunaan protokol komunikasi yang sesuai, pemrograman socket, dan pengelolaan koneksi antara client dan server[2].

Pada sisi server, sebuah program server botnet dibangun menggunakan socket programming. Server botnet ini berfungsi sebagai C&C server, menerima permintaan dari bot yang terinfeksi, mengirim perintah, dan mengumpulkan data dari bot. Melalui socket programming, server botnet mendengarkan port tertentu dan menerima koneksi dari bot yang terhubung.

Pada sisi client atau bot, sebuah program client botnet juga dibangun menggunakan socket programming. Program ini berjalan pada komputer yang terinfeksi dan bertugas untuk terhubung ke server botnet. Setelah terhubung, client bot akan mengirimkan informasi mengenai status dan ketersediaannya kepada server. Client bot juga akan menerima perintah dari server dan menjalankannya pada sistem terinfeksi.

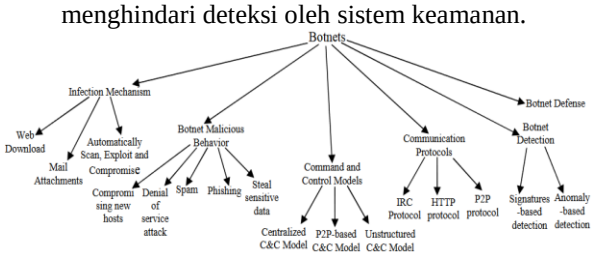
Socket programming memungkinkan komunikasi real-time antara server dan bot. Server dapat mengirim perintah kepada bot dan menerima laporan dari bot secara cepat. Dalam implementasi ini, perlunya keamanan menjadi penting. Penggunaan teknik enkripsi data dan otentikasi yang kuat perlu dipertimbangkan untuk melindungi komunikasi antara server dan bot dari deteksi dan intervensi yang tidak diinginkan.

B. Botnet

Botnet merupakan salah satu ancaman keamanan siber yang paling serius yang dihadapi oleh organisasi setiap harinya. Botnet menggunakan berbagai strategi, topologi, dan protokol komunikasi pada tahap-tahap tertentu dalam siklus hidupnya. Secara umum, botnet mengikuti infrastruktur command and control[3].

Botnet adalah jaringan komputer terpusat yang terdiri dari sejumlah besar perangkat yang terinfeksi oleh bot. Implementasi botnet melibatkan beberapa tahap, termasuk:

a. Penyebaran Malware: Botnet dimulai dengan menyebarkan malware ke komputer target. Malware ini dapat dikirim melalui email phishing, situs web yang terinfeksi, atau serangan serupa.
b. Infeksi Bot: Setelah malware berhasil dijalankan pada komputer target, botnet mengambil alih kontrol dan mengubah komputer menjadi "bot" yang terhubung ke C&C server.
c. Command and Control (C&C) Server: C&C server adalah pusat pengendalian botnet. Botnet menggunakan protokol khusus untuk berkomunikasi dengan C&C server. C&C server memberikan instruksi kepada bot dan menerima laporan dari mereka.
d. Kontrol Bot: C&C server mengirimkan perintah kepada bot yang terhubung untuk melakukan tugas tertentu, seperti serangan DDoS, pencurian data, atau penyebaran malware lebih lanjut.
e. Kegiatan yang Tidak Terdeteksi: Botnet bekerja dengan cermat untuk tetap tersembunyi dan tidak terdeteksi. Mereka menggunakan teknik enkripsi, pengelabuan alamat IP, dan strategi lainnya untuk menghindari deteksi oleh sistem keamanan.



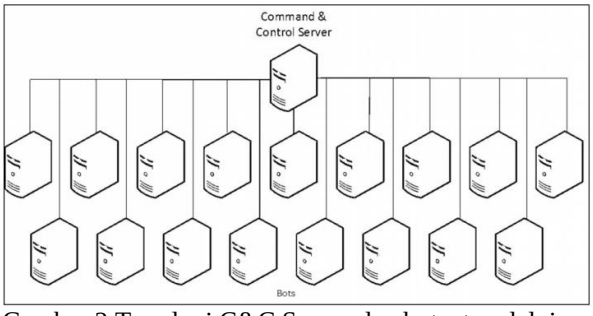
Gambar 1 Gambaran dari botnet[4]

C. C&C Server

Server Command and Control (C&C) memainkan peran penting dalam operasi sistem BotNet. Ini berfungsi sebagai titik kontrol sentral di mana botmaster dapat mengelola dan berkomunikasi dengan bot yang terinfeksi. C&C server bertanggung jawab untuk mengoordinasikan aktivitas bot, menerima perintah dari botmaster, dan mengumpulkan data atau mentransmisikan instruksi ke komputer yang terinfeksi.

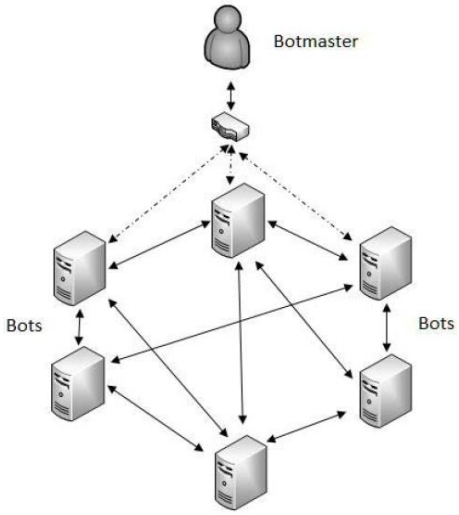
Implementasi C&C server melibatkan beberapa komponen utama, termasuk membangun infrastruktur server, membangun saluran komunikasi, dan mengembangkan protokol perintah. Infrastruktur server umumnya terdiri dari mesin server yang kuat yang dihosting di jaringan yang aman, seperti Virtual Private Server (VPS) yang menjalankan sistem operasi berbasis Linux. Ini memberikan platform yang tangguh dan dapat ditingkatkan untuk mengelola sejumlah besar bot secara efisien.

Untuk menjalin komunikasi dengan C&C server, berbagai saluran komunikasi dapat digunakan, seperti protokol HTTP, IRC (Internet Relay Chat), atau P2P (Peer-to-Peer). Saluran ini memungkinkan botmaster untuk mengeluarkan perintah dan menerima data dari bot yang terinfeksi. Pemilihan saluran komunikasi tergantung pada faktor seperti keamanan, anonimitas, dan kebutuhan skalabilitas. Gambar 2 merupakan topologi C&C Server dengan botnet menggunakan IRC.



Gambar 2 Topologi C&C Server dan botnet melalui IRC[5]

Mengembangkan protokol perintah yang aman dan efisien sangat penting untuk pengelolaan botnet yang efektif. Protokol perintah ini menentukan format dan struktur perintah yang dipertukarkan antara C&C server dan bot. Protokol tersebut memastikan komunikasi yang handal dan menyediakan mekanisme untuk otentikasi, enkripsi, dan integritas data. Protokol perintah yang aman membantu mencegah deteksi dan gangguan oleh sistem keamanan jaringan. Gambar 3 merupakan P2P Botnet dengan topologi yang terdesentralisasi.



Gambar 3 Topologi P2P botnet terdesentralisasi[5]

II. METODE PENELITIAN

Metode penelitian ini melibatkan langkah-langkah studi literatur, identifikasi dan perancangan, pengembangan aplikasi bot, penyebaran bot, serta analisis dan evaluasi hasil. Dengan menggunakan metode ini, diharapkan penelitian dapat memberikan pemahaman yang lebih baik tentang implementasi dan dampak botnet, serta menghasilkan wawasan yang dalam pengembangan strategi keamanan jaringan.

1. Studi Literatur
   Studi dan tinjauan literatur dilakukan secara komprehensif tentang botnet, keamanan jaringan, bahasa pemrograman C, dan Command and Control (C&C) server berbasis Linux. Mengidentifikasi kerangka teoritis, konsep, dan penelitian terkait yang relevan untuk mendukung penelitian ini.
2. Identifikasi dan Perancangan Botnet
   Pada tahap ini dilakukan identifikasi fitur dan fungsionalitas yang akan diimplementasikan dalam aplikasi botnet.
3. Pengembangan Aplikasi Bot
   Aplikasi dikembangkan dengan menggunakan bahasa pemrograman C dengan compiler MinGW. Aplikasi dibangun untuk sistem operasi Windows dengan menerapkan fitur dan fungsi yang memungkinkan bot untuk berkomunikasi dengan C&C Server.
4. Implementasi Sistem
   Implementasi sistem dilakukan dengan merancang berkas yang menarik dan meyakinkan pengguna untuk mengkliknya. Penyebaran botnet ini menggunakan disebarkan melalui USB Flash Memory. pengujian penyebaran bot dengan menggunakan skenario yang relevan untuk mengevaluasi keberhasilannya.
5. Analisis dan Evaluasi Hasil
   Pada tahap ini, dilakukan pengumpulan data dan informasi terkait hasil implementasi botnet dan penyebaran bot. Data tersebut kemudian dianalisis untuk mengevaluasi kinerja botnet, efektivitas penyebaran, dan dampak serangan terhadap keamanan jaringan. Evaluasi juga dilakukan terhadap keberhasilan serangan, kerentanan yang dieksploitasi, serta efisiensi strategi keamanan yang digunakan. Dengan menganalisis data yang terkumpul, akan diperoleh pemahaman yang lebih mendalam tentang mekanisme operasi botnet dan tingkat risiko yang terkait. Hasil analisis dan evaluasi ini akan didiskusikan dalam konteks keamanan jaringan, sehingga dapat memberikan wawasan yang berharga dan relevan. Selain itu, rekomendasi juga akan diberikan untuk pengembangan strategi keamanan yang lebih efektif dalam menghadapi ancaman botnet.

III. HASIL DAN PEMBAHASAN

Dari penelitian yang telah dilakukan, terdapat beberapa subbab yang dapat dideskripsikan untuk hasil dan pembahasan. Bahasan yang disajikan antara lain pengembangan aplikasi bot, penetrasi botnet untuk target, dan implementasi sistem botnet.

A. Pengembangan Aplikasi Bot

Tahap ini akan dikembangkan sistem aplikasi botnet yang dibuat dengan menggunakan compiler MinGW berbasis bahasa pemrograman C.

Dasar pengembangan botnet sebagai bot yang berjalan di komputer korban adalah socket programming, khususnya dalam membangun jaringan client dan server. Dengan memanfaatkan pustaka yang tersedia dalam bahasa pemrograman C, maka digunakan pustaka winsock.

```
#include <winsock2.h>
#include <ws2tcpip.h>
#include <windows.h>
#include <tchar.h>
```

Gambar 4 Pemanggilan pustaka windows socket

Kode program mencakup definisi alamat IP dari server linux, port, dan ukuran maksimal buffer data yang digunakan.

```
#define CC_SERVER "167.88.124.101"
#define CC_PORT 9999
#define MAX_BUF 1024
```

Gambar 5 Definisi C&C server

Alamat IP server yaitu 167.88.124.101 dan transmisi data melalui port 9999 dengan buffer data 1024 byte.

```
void addstartup()
{
    TCHAR path[100];
    GetModuleFileName(NULL,path,100);
    HKEY newValue;
    RegOpenKey(HKEY_CURRENT_USER ,"Software\\Microsoft
    \\Windows\\CurrentVersion\\Run",&newValue);
    RegSetValueEx(newValue,"botnet",0,REG_SZ,(LPBYTE)path
    ,sizeof(path));
    RegCloseKey(newValue);
}
```

Gambar 6 Fungsi Windows startup

Fungsi addstartup() merupakan fungsi yang dibuat sebagain metode yang bertujuan untuk menulis ke registry Windows dan menjadikan program tersebut selalu berjalan di proses background saat komputer pertama kali dihidupkan.

```
cc_s = bot_connect_cc (CC_SERVER, CC_PORT);
while (1)
  {
    bot_read (cc_s, msg);
    bot_parse (cc_s, msg);
  }
}
```

Gambar 7 Fungsi utama program botnet

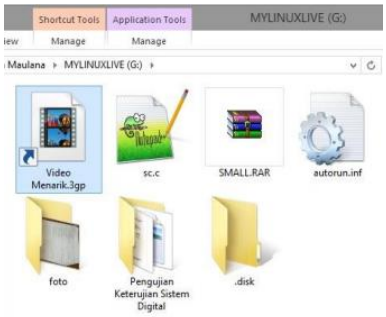
Dalam fungsi utama program, terdapat sintaks socket programming. Variabel cc_s merupakan variabel untuk menghubungkan bot dengan server C&C. Fungsi utama ini selalu menjalankan fungsi baca dan parsing data socket jaringan. Untuk menjalankan program botnet melalui Putty dengan memanfaatkan protokol SSH.

B. Penetrasi Botnet

Tahap ini membahas hasil dari penetrasi botnet di sistem operasi Windows dengan memodifikasi berkas menjadi menarik untuk diklik.

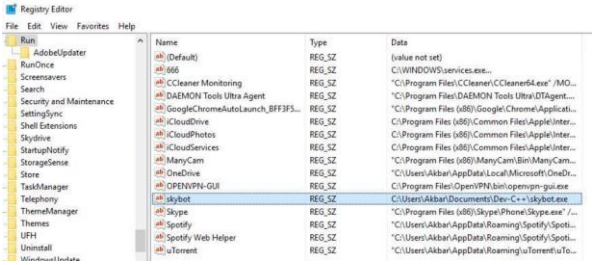
Gambar 8 Properti berkas Video

Modifikasi dilakukan dengan mengubah nama menjadi video menarik dengan format video 3gp. Berkas dimodifikasi dengan mereferensikan ke target berkas botnet bernama skybot bertipe exe. Berkas botnet tersebut tersembunyi dalam direktori USB Flash Memory.



Gambar 9 Tampilan berkas botnet

Ketika seseorang tidak sengaja mengaktifkan program Bot melalui metode penyebaran yang digunakan, program Bot akan secara otomatis membuat dirinya menjadi program startup dan tersimpan dalam registri komputer. Hal ini berarti program Bot akan selalu aktif setiap kali komputer yang terinfeksi dihidupkan. Gambar 10 memperlihatkan alamat registry.

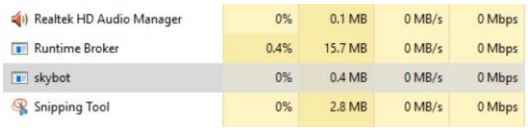


Gambar 10 Alamat Registry Windows

Gambar 11 menunjukkan bahwa program tersebut telah berhasil menjadi program startup dengan tingkat medium.

Gambar 11 Program botnet di program startup

Program bot yang tersembunyi di dalam komputer berjalan pada proses background, sehingga sulit terdeteksi oleh pemilik komputer. Gambar 12 terlihat dalam Task Manager bahwa program bot berjalan.

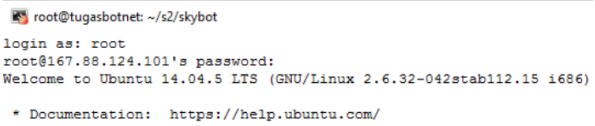


Gambar 12 Program botnet dalam task manager

Aplikasi botnet beberapa kali gagal menginfeksi komputer korban ketika komputer tersebut menggunakan Antivirus dan Windows Defender dengan update versi terbaru.

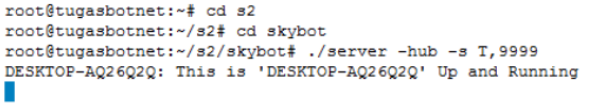
C. Implementasi Sistem

Dalam implementasi sistem botnet, langkah awal adalah mengunggah program botnet ke server Linux yang dihosting di VPS (Virtual Private Server) menggunakan filezilla. Dengan memanfaatkan SSH, seperti Putty, peneliti dapat mengakses server dan memulai menjalankan program C&C server. Gambar 13 adalah antarmuka putty saat login ke server.



Gambar 13 Antarmuka CLI login pada server

Program dijalankan pada server dengan nama server dalam direktori skybot. Sedangkan program dilewatkan melalui port 9999 Saat program berjalan, ketika terdapat komputer korban yang aktif dan terhubung, pemberitahuan akan diberikan untuk mengindikasikan keberadaan Bot pada komputer tertentu, dengan menyebutkan nama komputer korban yang sedang aktif. Pada Gambar 14, terlihat adanya 1 (satu) komputer korban yang aktif dengan nama "DESKTOP-AQ26Q2Q".

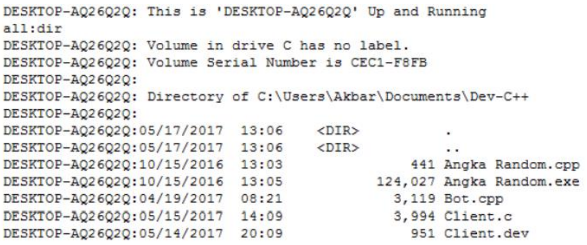


Gambar 14 Sintaks menjalankan program C&C Server

Untuk mengirim perintah kepada Bot yang aktif, salah satu contoh sintaksis yang dapat digunakan adalah "all:dir". Sintaksis ini bertujuan untuk meminta C&C Server agar menampilkan direktori dari komputer-komputer korban yang terhubung. Dengan demikian, perintah tersebut akan diteruskan kepada seluruh Bot yang aktif.

Namun, jika diinginkan untuk memberikan perintah hanya kepada Bot yang terhubung dengan komputer target tertentu, sintaksis "all" dapat diganti dengan nama komputer target tersebut. Setelah titik koma, perintah yang ingin diberikan kepada Bot aktif dapat dituliskan.

Pada Gambar 15, terlihat contoh penggunaan fitur C&C Server dalam mengetahui isi direktori dari komputer korban.



Gambar 15 Fitur C&C Server untuk melihat direktori komputer korban

Dengan adanya kemampuan untuk mengirim perintah secara spesifik kepada Bot yang diinginkan, peneliti dapat mengontrol aksi dan mendapatkan informasi yang relevan dari komputer-komputer korban yang terinfeksi Botnet.

Berdasarkan langkah-langkah implementasi yang telah dijelaskan, sistem Botnet yang telah dikembangkan berhasil diimplementasikan dengan sukses pada sistem operasi Windows. Sistem ini beroperasi dengan baik dan sesuai dengan tujuan yang diinginkan. Dalam konteks ini, sistem Botnet yang dikembangkan dapat digambarkan sebagai contoh implementasi BotNet sederhana yang berhasil.

Melalui pengembangan sistem Botnet ini, telah terbukti bahwa sistem tersebut mampu berfungsi dengan baik dan menjalankan tugasnya dengan efektif. Implementasi ini memberikan gambaran nyata tentang kemampuan dan potensi Botnet dalam menginfeksi komputer-komputer korban serta melakukan serangkaian operasi yang telah ditetapkan.

Dalam penelitian ini, langkah-langkah implementasi yang telah dilakukan pada sistem operasi Windows dapat dijadikan sebagai fondasi dan panduan bagi pengembangan sistem Botnet yang lebih kompleks dan canggih di masa depan. Hasil implementasi ini memberikan kontribusi dalam memahami mekanisme dasar dan karakteristik Botnet, serta memperkuat upaya mitigasi dan perlindungan terhadap serangan cyber yang menggunakan botnet sebagai alat utama.

Dengan demikian, dapat disimpulkan bahwa implementasi sistem Botnet pada sistem operasi Windows merupakan langkah awal yang penting dalam pengembangan dan pemahaman lebih lanjut tentang ancaman cyber yang terkait dengan botnet.

IV. KESIMPULAN

Berdasarkan penelitian, implementasi dan pengujian, maka dapat diambil kesimpulan sebagai berikut :

1. Implementasi botnet sederhana menggunakan bahasa pemrograman C dan C&C server berbasis Linux memberikan pemahaman yang lebih baik tentang mekanisme dasar operasi dan struktur botnet.
2. Botnet gagal menginfeksi komputer korban saat komputer tersebut disematkan antivirus dan Windows Defender terbaru.

3. Botnet memiliki potensi sebagai alat yang kuat untuk melancarkan serangan, merusak, dan mencuri informasi sensitif dalam konteks keamanan jaringan.
4. Pentingnya pengembangan strategi keamanan yang efektif untuk melawan ancaman botnet dan melindungi infrastruktur jaringan dari serangan yang semakin kompleks.

Dengan demikian, dapat disimpulkan bahwa implementasi sistem Botnet pada sistem operasi Windows merupakan langkah awal yang penting dalam pengembangan dan pemahaman lebih lanjut tentang ancaman cyber yang terkait dengan botnet.

DAFTAR PUSTAKA

[1] Institute of Electrical and Electronics Engineers., *Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on : date, 7-9 Dec. 2009.* IEEE, 2009.

[2] K. Davis, J. W. Turner, and N. Yocom, *The definitive guide to linux network programming*. Springer.

[3] S. F. Shetu, Mohd. Saifuzzaman, N. N. Moon, and F. N. Nur, "A Survey of Botnet in Cyber Security," in *2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT)*, 2019, pp. 174–177. doi: 10.1109/ICCT46177.2019.8969048.

[4] C. Li, W. Jiang, and X. Zou, "Botnet: Survey and Case Study," in *2009 Fourth International Conference on Innovative Computing, Information and Control (ICICIC)*, 2009, pp. 1184–1187. doi: 10.1109/ICICIC.2009.127.

[5] T. Hyslip and J. Pittman, "A Survey of Botnet Detection Techniques by Command and Control Infrastructure," *Journal of Digital Forensics, Security and Law*, 2015, doi: 10.15394/jdfsl.2015.1195.