Teknologi Open Source Untuk Lomba Keamanan Jaringan Berbasis CTF

Sultan Baharuddin Ulil Amrie[1)], Eddy Tungadi [2)], Irfan Syamsuddin[3)]
[1] Teknik Elektro, Politeknik Negeri Ujung Pandang
sultanbaharuddin25@gmail.com
[2] Teknik Elektro, Politeknik Negeri Ujung Pandang
e_tungadi@yahoo.com
[3] Teknik Elektro, Politeknik Negeri Ujung Pandang
irfans@poliupg.ac.id

Abstrak

Talenta cyber security semakin diminati seiring meningkatnya ancaman penyalahgunaan teknologi informasi. Usaha yang dilakukan untuk menjaring talent tersebut antara lain melalui lomba Capture the Flag. Penelitian ini bertujuan untuk menyediakan tata cara pembangunan infrastruktur perlombaan Capture the Flag. Pada penelitian ini dimanfaatkan sebuah teknologi Open-Source CTFd dan Cardinal untuk dijadikan sebagai objek penelitian dalam membuat perlombaan Capture the Flag dengan format Jeopardy dan Attack-Defense. Penelitian ini dilakukan dengan menggunakan perangkat PC dengan membuat mesin virtual sebagai tempat berjalannya sistem perlombaan. Dari hasil penelitian ini dapat digunakan sebagai acuan atau tata cara dalam melaksanakan perlombaan Capture the Flag dengan memanfaatkan teknologi Open-Source.

Keywords: *Capture the Flag, Cyber Security, Open-Source, CTFd, Cardinal*

I. PENDAHULUAN

Jaringan Komputer atau internet sudah menjadi sangat populer dan juga kebutuhan orang-orang yang bertalenta di dunia teknologi informasi semakin dibutuhkan dalam kehidupan setiap hari. Di sisi yang lain semakin banyak pula kekhawatiran mengenai jaringan komputer ini.

Beberapa tahun belakangan ini banyak organisasi mencari orang-orang yang tidak hanya bertalenta di teknologi informasi tapi juga bertalenta pada bidang security [1]. Hal ini disebabkan bukan lain dikarenakan banyaknya kasus-kasus terjadi yang mengancam keamanan dari sebuah teknologi informasi.

Bebepa organisasi atau perusahaan melakukan banyak cara dalam mencari atau menjaring para talenta ahli ini. Usaha yang dilakukan untuk menjaring talent untuk kebutuhan tersebut antara lain melalui lomba seperti Capture the Flag yang selanjutnya akan disebut dengan CTF. Sebagai bahan referensi, diperlukan penelitian untuk mengetahui tata cara pembuatan infrastruktur perlombaan CTF.

Penelitian ini bertujuan untuk menyediakan tata cara pembangunan infrastruktur berbasis Open-Source dengan menggunakan CTFd dan Cardinal sehingga dapat dimanfaatkan untuk melaksanakan perlombaan CTF nantinya.

II. KAJIAN LITERATUR

Cyber Security adalah pendekatan dan aksi yang berkaitan dengan proses manajemen risiko keamanan yang dibarengi oleh organisasi atau pemerintahan untuk menjaga Confidentiality, Integrity, dan Availability suatu data dan aset yang berada pada dunia cyber.

Kebutuhan keahlian cyber security saat ini menjadi hal yang menjadi ketertarikan global dan penting. Lebih dari 50 negara telah secara resmi mempublikasikan dokumen mengenai strategi mereka terhadap cyberspace, cyber crime dan/atau cybersecurity [2]. Walaupun demikian, saat ini dunia masih kekurangan ahli dalam bidang cyberscurity dan salah satu cara untuk mengatasinya adalah membuat para edukator untuk secara efisien dan efektif mengedukasi para calon penggerak ahli cybersecurity. Salah satu alat pembelajaran yang kuat untuk mempelajari cybersecurity adalah dengan menggunakan pelatihan Capture the flag.

Perlombaan Capture the Flag sendiri dapat dilaksanakan dengan memanfaatkan program-program yang bersifat Open-Source yang tersedia secara gratis hanya dengan mengunduh dan melakukan instalasi. Open-Source sendiri memiliki makna bahwa sesuatu tersebut dapat di perbanyak dan di distribusikan ulang, pengguna dapat mengakses sumber kode dan memodifikasi kode tersebut.

A. Capture the Flag

Capture the flag atau yang selanjutnya akan disebut dengan CTF merupakan sebuah kompetisi ethical hacking paling terkenal pada komunitas para hacker. Seiring dengan ilmu pengetahuan pada umumnya, metode yang populer untuk mempraktikkan keterampilan keamanan siber adalah melalui permainan dan kompetisi informal CTF. Dalam acara ini, tim kecil berisi beberapa peserta berlatih keterampilan cybersecurity dengan menyelesaikan berbagai tugas dalam lingkungan pembelajaran online. Tugas (Task) CTF, yang disebut tantangan (Challenge), menampilkan

beragam tugas mulai dari mengeksploitasi situs web, memecahkan kata sandi, hingga menerobos jaringan yang tidak aman. Solusi yang berhasil dari sebuah tantangan menghasilkan string teks yang disebut "flag" yang dikirimkan secara online untuk membuktikan pencapaian solusi.

CTF memiliki tiga format berbeda dalam penyelenggaraannya yaitu Jeopardy, Attack-defense, dan campuran. Model jeopardy menampilkan sebuah papan pilihan, yang memiliki nilai poin berbeda yang ditunjukkan pada setiap kategori. jumlah nilai poin berdasarkan tingkat kesulitan dari soal pertanyaan [3]. Adapun beberapa kategori tantangan yang hadir didalam format Jeopardy ini yaitu Web, Forensic, Crypto, Binary, Reverse Engineering dan seterusnya. Peserta diminta untuk mencari jawaban (atau disebut dengan "flag") dari pertanyaan.

B. CTFd

CTFd merupakan sebuah framework CTF yang berfokus pada kemudahan dan penyeseuaian dalam penggunaan pada sebuah acara atau kompetisi termasuk lomba CTF [3]. CTFd adalah sebuah aplikasi web yang bertanggung jawab untuk memberikan antarmuka bagi peserta, yang memberikan akses ke tugas mereka masing-masing melalui web browser [5]. Framework CTFd merupakan Framework yang biasanya digunakan untuk melaksanakan perlombaan CTF dengan format Jeopardy.

C. Cardinal

Salah satu framework yang menyediakan layanan interface dan sistem perlombaan format Attack-defense adalah Cardinal. Cardinal adalah platform kompetisi AWD (Attack with Defense) yang dikembangkan oleh Vidar-Team, ditulis dalam Bahasa Pemrograman Go. Program ini dapat digunakan sebagai platform kompetisi offline CTF, dan juga dapat digunakan untuk latihan simulasi AWD untuk internal tim [6].

III. METODE PENELITIAN

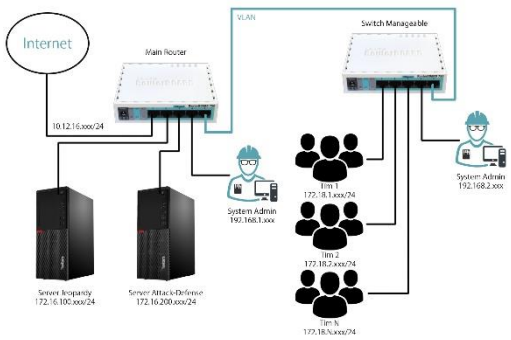
Penelitian ini dilaksanakan Politeknik Negeri Ujung Pandang dengan memanfaatkan infrastruktur yang dimiliki oleh Program Studi D4 Teknik Komputer dan Jaringan yaitu 2 buah perangkat PC yang masing-masing digunakan sebagai tempat berjalannya perlombaan CTF format jeopary dan Attack-Defense. Pengetesan sistem yang dirancang dilaksanakan oleh peserta mahasiswa Program Studi D4 Teknik Komputer dan Jaringan yang telah mengikuti Mata Kuliah Keamanan Jaringan.

Adapun langkah-langkah dalam perancangan yang dibentuk dalam penelitian ini sesuai dengan gambar 1 mengenai cara pembuatan infrastruktur lomba CTF dengan memanfaatkan Teknologi Open Source yaitu :

1. Mempersiapkan Peralatan yang dibutuhkan.

Perlatan-peralatan yang dibutuhkan antara lain PC Komputer, Managable Switch dan Kabel Ethernet Secukupnya.

2. Membangun dan Mengkonfigurasi Infrastruktur Jaringan



Gambar 1. Infrastruktur Perlombaan

Dalam pembangunan dan konfigurasi infrastruktur jaringan ini, digunakan Hypervisor Proxmox VE untuk mengatur Virtual Machine. Serta Mikrotik untuk mengatur trafik Jaringan.

3. Membuat Mesin Virtual

Mesin virtual digunakan untuk menjalankan Sistem Operasi Debian sebagai environment sistem.

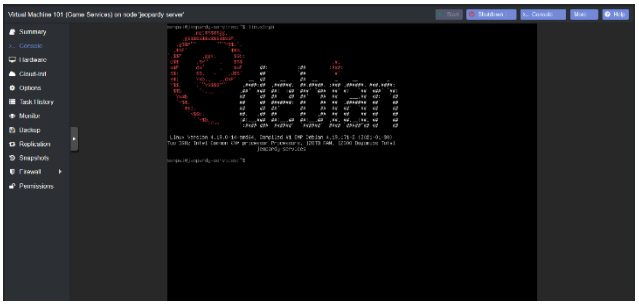
4. Instalasi framework CTFd dan Cardinal serta challenge.
5. Instalasi Landing Page Bundu'E.

Lalu untuk skenario perlombaan sebagai berikut :

1. Admin mengaktifkan perlombaan dan challenge lomba CTF Jeopardy.
2. Peserta melakukan perlombaan CTF Jeopardy
3. Admin mengaktifkan perlombaan dan challenge lomba CTF Attack-Defense.
4. Peserta melakukan perlombaan CTF Attack-Defense.

IV. HASIL DAN PEMBAHASAN

A. Pembuatan Mesin Virtual



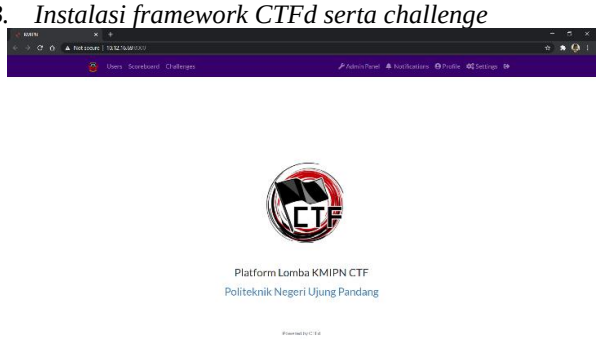
a. Mesin Virtual CTF Jeopardy

b. Mesin Virtual CTF Attack-Defense

Gambar 2. Instalasi Mesin Virtual

Menggunakan Hypervisor Proxmox VE sebagai mesin Virtual dengan Sistem Operasi Debian.

B. Instalasi framework CTFd serta challenge



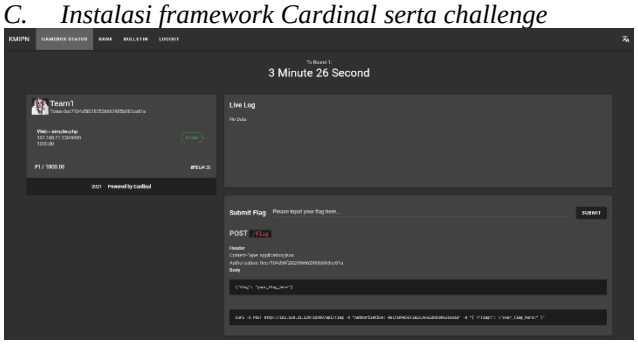
Gambar 3. Interface Platform CTFd

Platform Framework CTFd sebagai interface perlombaan CTF Jeopardy. Platform ini yang digunakan oleh peserta dalam mengikuti perlombaan CTF Jeopardy.

Gambar 4. Interface Challenge Robots kategori Web

Salah satu challenge perlombaan yang diajukan. Berisi sebuah tantangan dengan kategori Web. Challenge ini memiliki vulnerability pada halaman /robots.txt yang menampilkan string flagnya.

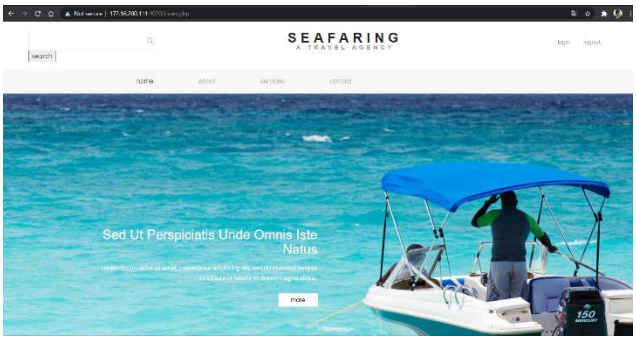
C. Instalasi framework Cardinal serta challenge



Gambar 5. Interface Platform Cardinal

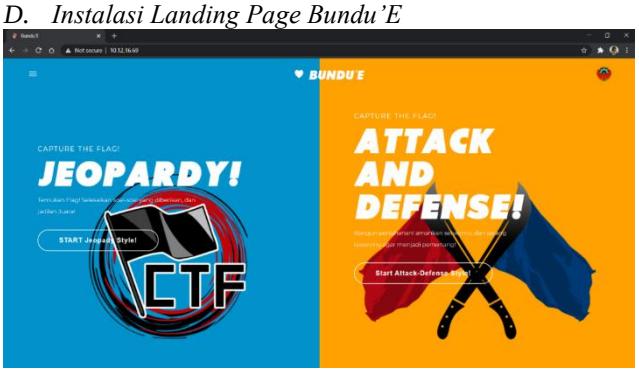
Platform Framework Cardinal sebagai interface perlombaan CTF Attack-Defense. Platform ini yang digunakan oleh peserta dalam mengikuti perlombaan CTF Attack-Defense.

Salah satu challenge perlombaan Attack-Defense yang diajukan. Berisi sebuah tantangan dengan kategori Web. Challenge ini memiliki vulnerability pada section footer yang menampilkan sebuah form yang dapat menjalankan kode Shell dan memberikan hak akses ke sistem.



Gambar 6. Interface Challenge Simple-php

D. Instalasi Landing Page Bundu'E



Gambar 7. Interface Landing Page Bundu'E

Landing Page Bundu'E berfungsi sebagai halaman utama perlombaan. Pada halaman ini, peserta diberikan kesempatan untuk memilih jenis perlombaan yang ingin mereka ikuti.

V. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan dapat disimpulkan bahwa untuk membangun infrastruktur perlombaan Capture the Flag adalah sebagai berikut :

1. Mempersiapkan perangkat yang dibutuhkan.
2. Membangun dan mengkonfigurasi infrastruktur jaringan.
3. Membuat mesin virtual pada PC 1 (Jeopardy) dan PC 2 (Attack-defense) dengan menggunakan hypervisor Proxmox VE.
4. Intalasi Framework CTFd dan Cardinal serta challenge perlombaan.
5. Instalasi Landing Page Bundu'E.

REFERENSI

[1] Syamsuddin, Irfan. "VILARITY-Virtual Laboratory for Information Security Practices." TEM Journal 8, no. 3 (2019): 1011-1016.

[2] Hathaway, Melissa, and Alexander Klimburg. "Preliminary considerations: on national cyber security." National Cyber Security Framework Manual. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn (2012).

[3] Khan, Mohammad N., Abdulwahab Telmesani, Abdulaziz Alkhotani, Abdelaziz Elzouki, Burhan Edrees, and Mohammad H. Alsulimani. "Comparison

of jeopardy game format versus traditional lecture format as a teaching methodology in medical education." Saudi Med J 32, no. 11 (2011): 1172-1176.

[4] LLC, Kevin Chung // CTFd. “CTFd : The Easiest Capture the Flag Framework.” CTFd LLC. Accessed September 12, 2021. https://ctfd.io/.

[5] Panum, Thomas Kobber, Kaspar Hageman, Jens Myrup Pedersen, and René Rydhof Hansen. "Haaukins: A highly accessible and automated virtualization platform for security education." In 2019 IEEE 19th International Conference on Advanced Learning Technologies (ICALT), vol. 2161, pp. 236-238. IEEE, 2019.

[6] Vidar-Team. "Cardinal." Cardinal. Accessed September 12, 2021. https://cardinal.ink/.