BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan dunia teknologi dan informasi yang semakin maju memungkinkan masyarakat saat ini menggunakan teknologi dalam berbagai bidang, seperti pendidikan, bisnis, dan bahkan hiburan. Hal ini dikarenakan mudahnya dalam mengakses dan menyimpan data dengan hanya menggunakan komputer dan jaringan internet. Perkembangan jaringan internet dan komputer juga tidak menutup kemungkinan adanya rintangan dan permasalahan yang harus dihadapi. Salah satu di antara tantangan itu adalah sistem keamanan. Secara fisik, perangkat komputer dan keamanan server terjadi karena pencurian, bencana alam atau rusak. Sedangkan untuk non-fisik dapat terjadi berupa sistem operasi dan pencurian data yang dilakukan dengan hacking, virus dan sebagainya. Kejahatan non-fisik tersebut biasa disebut dengan CyberCrime atau kejahatan dalam dunia siber. Anomali sistem keamanan jaringan internet dan komputer merupakan salah satu ancaman yang dapat berimbas bagi penggunanya maupun sekitarnya. Contoh yang sering ditemukan adalah data privasi pengguna seperti username dan password pada proses otentikasi.

Dalam jaringan internet dan komputer, salah satu fitur yang menggunakan proses otentikasi adalah layanan protokol jaringan remote access yaitu protokol SSH (Secure Shell). Salah satu contoh ancaman keamanan jaringan komputer yang dapat menyerang sistem otentikasi adalah penyerang melakukan serangan Brute Force Attack. Brute Force Attack atau serangan beruntun merupakan salah satu serangan yang dimana mencoba berbagai deretan username dan password yang diinputkan secara beruntun untuk dapat login ke sistem baik itu menggunakan bot system ataupun login secara manual (Fathuzzikri et al., 2019). Brute Force memiliki tujuan untuk menemukan username dan password yang cocok pada login system pengguna, kemudian mereka akan bisa memasuki sistem inti dari target penyerang sehingga penyerang bisa mem-bypass sistem keamanan pengguna. Serangan brute force sekarang telah merambat ke layanan protokol SSH yang dapat mengambil alih administrasi sistem komputer jarak

jauh (remote), serangan tersebut dinamakan SSH Brute Force. Serangan ini merupakan serangan yang paling banyak terjadi di jaringan komputer. Tentu saja hal tersebut dicap ilegal karena penyerang masuk tanpa memenuhi syarat otentikasi dan akan mengambil alih sistem dengan layanan protokol SSH tersebut. Maka dari itu, keamanan pada jaringan komputer sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya (Arkaan & Sakti, 2019).

Pada penelitian ini, peneliti mengambil studi kasus di UPT TIK Universitas Pendidikan Ganesha yang dimana terdapat sebuah server khusus yang menyediakan segala bentuk informasi tentang universitas serta berbagai fasilitas berbasis online seperti e-journal, e-learning, mailing dan yang lainnya. Merujuk pada Lampiran 2, penggunaan remote access menggunakan protocol SSH menjadi kegiatan yang dilakukan dalam aktivitas monitoring dan konfigurasi server. Beberapa masalah terjadi pada server diantaranya adalah gangguan yang terjadi terhadap server seperti web server sistem informasi yang dimana sering digunakan oleh jajaran lingkup Undiksha. Mengetahui SSH menjadi protocol komunikasi ke jaringan server secara langsung, pihak administrator hanya mengatahui IP address dan Log aktivitas yang dilakukan tanpa adanya peringatan dini. Namun pada server khusus yang bertempat di gedung PUSKOM UPT TIK Undiksha belum terdapat sistem honeypot tersebut untuk penerapan keamanan pada server. Peneliti juga mengambil tindakan berupa port scanning vulnerable menggunakan tools Nmap script Vulnerable Scan (Vulscan) dan mendapatkan hasil port SSH terbuka di publik network. Hal tersebut akan berdampak pada server mengalami gangguan karena memungkinkan untuk melakukan brute forcing untuk mendapatkan hak akses secara ilegal. Maka dari itu implementasi keamanan akan berfokus pada protokol SSH untuk efisiensi sumber daya dan tidak mengganggu kinerja server.

Salah satu solusi yang dapat digunakan untuk menjaga /mencegah serangan terjadi pada sistem keamanan tersebut adalah dengan menggunakan Honeypot. Terkait dengan proses otentikasi, honeypot berperan penting dalam menjaga keamanan terutama pada sisi server. Honeypot berperan sebagai duplikat dari

server sehingga seolah-olah penyerang mengira telah berhasil masuk ke sistem inti. Dengan menggunakan layanan SSH, mereka dapat menerobos masuk ke dalam sistem tanpa menyadari mereka telah berada di server asli. Terdapat honeypot yang dibangun khusus untuk menangani serangan pada protokol Secure Shell (SSH). Salah satunya dengan menggunakan Honeypot Cowrie. Peneliti menggunakan Honeypot Cowrie yang merupakan honeypot khusus protokol SSH untuk implementasi SSH honeypot pada server UPT TIK Undiksha. Disamping itu, sistem monitoring akan diimplementasikan pada server sekaligus dengan notifikasi peringatan menggunakan API Telegram untuk mendapatkan informasi secara efektif dan efisien.

Dalam sebuah penelitian terkait dengan judul "IMPLEMENTASI HONEYPOT KIPPO PADA SISTEM KEAMANAN SERVER BERBASIS WEB MONITORING DENGAN NOTIFIKASI OTOMATIS MENGGUNAKAN API TELEGRAM" (Fathuzzikri et al., 2019), menggunakan honeypot jenis Kippo untuk melindungi server pada protokol SSH dan sukses mendeteksi serangan dengan persentase 99%. Sedangkan penelitian terkait dari Devi & Aulia (2020) dengan judul "HONEYPOT COWRIE IMPLEMENTATION TO PROTECT SSH PROTOCOL IN UBUNTU SERVER WITH VISUALISATION USING KIPPO-GRAPH", menggunakan sistem operasi Ubuntu Server untuk menanam honeypot Cowrie pada server dan melindungi protokol SSH dengan persentase sukses sebesar 95,6% (Putri & Rachmawati, 2019). Jenis honeypot yang sama diterapkan pada penelitian lainnya yaitu penelitian dari (Tati Ernawati & Fikri Faiz Fadhlur Rachmat, 2021) yang menerapkan Cowrie dengan Snort sebagai IPS. Penelitian tersebut menggunakan metode NDLC serta menguji dengan parameter CIA (Confident, Integrity dan Available). Berdasarkan penelitian sebelumnya, notifikasi untuk peringatan awal serangan untuk server perlu diterapkan pada penelitian ini. Sistem notifikasi yang dimaksud adalah notifikasi pada perangkat mobile, hal tersebut diterapkan karena peringatan hanya terdapat pada visualisasi yang terdapat pada web browser dan perlu perluasan informasi seperti direksi ke administrator saat berada dimanapun.

Berdasarkan pemaparan di atas, maka penulis akan mengambil penelitian dengan judul “Implementasi Honeypot Cowrie untuk Mendeteksi Serangan Protokol SSH pada Server beserta Web Monitoring dan Notifikasi Otomatis (Studi Kasus UPT TIK Undiksha)”. Metode yang digunakan pada penelitian ini adalah metode Network Life Development Cycle (NDLC). Untuk akurasi data, penulis menggunakan pengukuran confusion matrix untuk mendapatkan nilai True / False serta tahap monitoring menggunakan pengukuran availability.

1.2 IDENTIFIKASI MASALAH

Berdasarkan latar belakang tersebut ada beberapa hal yang dapat diidentifikasi masalah pada penelitian ini. Adapun masalah yang dapat diidentifikasi adalah yaitu :

1. Proses port vulnerable scan pada port 22 SSH server dalam server lingkup UPT TIK Undiksha yang masih aktif untuk publik menjadi rentan terhadap serangan.
2. Belum ada sistem Honeypot di server UPT TIK Undiksha.

1.3 RUMUSAN MASALAH

Berdasarkan latar belakang masalah yang telah dipaparkan sebelumnya. Maka dapat dirumuskan menjadi permasalahan sebagai berikut :

1. Bagaimana rancangan dan implementasi notifikasi peringatan awal Honeypot Cowrie serta implementasinya pada server di UPT TIK Undiksha?.
2. Bagaimana persentase keamanan yang diperoleh dengan menggunakan Cowrie Honeypot pada server di UPT TIK untuk memproteksi protokol SSH ?.

1.4 TUJUAN PENELITIAN

Berdasarkan rumusan masalah yang disebutkan sebelumnya, tujuan penelitian yang ingin dicapai adalah sebagai berikut:

1. Untuk mengetahui rancangan dan implementasi notifikasi peringatan awal Honeypot Cowrie pada server UPT TIK Undiksha
2. Untuk mengetahui persentase keamanan yang diperoleh dengan menggunakan Cowrie Honeypot pada server UPT TIK Undiksha untuk memproteksi protokol SSH.

1.5 MANFAAT HASIL PENELITIAN

Hasil dari penelitian ini diharapkan memiliki manfaat tersendiri, diantaranya yaitu :

1. Manfaat Teoritis

   Penelitian ini sangat bermanfaat untuk ilmu sekuritas khusus pada dunia cyber terutama pada peneliti keamanan jaringan dan kaitannya dengan masyarakat luas akan pentingnya keamanan jaringan serta privasi data. Manfaat teoritis terutama pada UPT TIK Undiksha adalah sektor masalah keamanan data yang bersifat sensitif (data personal mahasiswa/dosen/staff).

2. Manfaat praktis

   a. Bagi Masyarakat

      Penelitian ini diharapkan bermanfaat bagi masyarakat karena berperan penting dalam proteksi privasi data pada masing masing individu. Tentu juga ditunjukan pada pemilik server untuk perlindungan server pribadinya dari jaringan publik.

   b. Bagi Peneliti

      Diharapkan memiliki manfaat untuk peneliti terutama dalam bidang cyber serta penggunaannya yang dapat bermanfaat untuk dikembangkan lebih baik lagi.

   c. Bagi UPT TIK

      Diharapkan dapat bermanfaat untuk perlindungan data serta pengembangan aplikasi keamanan jaringan untuk server yang dimiliki oleh UPT TIK Undiksha.

   d. Bagi Enterprise / Perusahaan

      Diharapkan juga dari sisi pengguna yang mengutamakan server sebagai sumber daya mereka serta diharapkan membantu integritas dari masing masing individu untuk memproteksi data mereka

1.6 BATASAN MASALAH

Batasan masalah yang ada dalam penelitian ini adalah kebutuhan hardware untuk penerapan honeypot sebagai pengujian serta sebanding dengan server untuk mengetahui performa dari platform honeypot Cowrie pada server UPT

TIK. Selain itu dilakukan pengujian untuk menguji performa honeypot Cowrie pada server dengan melakukan tindakan brute force serta tidak berakibat pada kerusakan server inti.

Berdasarkan batasan tersebut sebelumnya, peneliti akan menggunakan server yang bersifat dummy / uji coba untuk mengimplementasikan Honeypot Cowrie dalam jaringan server lokal di UPT TIK.