BAB 1

PENDAHULUAN

1. 1 Latar Belakang

Setiap tahun banyak sekali serangan dari kerentanan sebuah web, yang harus dianalisa. Analisa ini penting untuk memperkuat keamanan pada web dari serangan. Serangan ini, datangnya dari *hacker*/peretas yang menyerangnya dengan bertahap. Tahap pertama, adalah *passive information gathering* adalah tahap dimana *hacker* akan mencari sebuah kerentanan atau celah yang terlihat pasif pada sebuah *web* yang akan menjadi target *hacker*. Setelah mendapatkan informasi pasif, lalu ditingkatkan menjadi *active information gathering. Active information gathering* adalah tahap kedua *hacker* yaitu, mencari informasi kerentanan spesifik pada port dari sebuah web yang melibatkan hal-hal sensitif didalamnya. Lalu, tahap terakhir adalah mengeksploitasi kerentanan spesifik pada port dari hasil langkah sebelumnya.[1]

Hacker hanya membutuhkan satu celah kecil saja untuk bisa mengacak-acak bahkan memiliki sebuah sistem yang ada. Celah kecil sangat banyak jenisnya. Akan tetapi, kali ini yang akan dibahas adalah bahasan celah yang terstruktur dan berelevasi. Celah yang dimulai dari *passive information gathering* hingga sampai *exploitation.* Dimulai dari mengumpulkan informasi *ip address,scanning and enumeration*,mencari *weaknesses* dari *port-port* yang tersedia,lalu *exploitation.*[2]

Passive information gathering mengacu pada pengumpulan informasi sebanyak mungkin tanpa menjalin kontak antara penguji dengan target yang anda kumpulkan informasinya.[3] *Passive information gathering* melibatkan penggunaan sumber daya internet untuk mengetahui informasi yang tersedia untuk umum tentang perusahaan[4]. Menggunakan *OSINT(Open Source Intellegence)* anda dapat mengumpulkan hal-hal seperti alamat *IP(Internet Protocol)*, nama domain, alamat email, nama, nama *host*, catatan *DNS*, bahkan perangkat lunak apa yang berjalan di situs *web* dan *CVE (Common Vulnerabilities Exposure*) terkait. [5]

Peran *cybersecurity* untuk melindungi sistem dengan keamanan yang baik. Akan tetapi, *cybersecurity* harus berpikir seperti *hacker* untuk menutupi semua celah yang ada sebisa mungkin. Maka dari itu *cybersecurity* di khalayak umum berpegang dengan prinsip *CIA Triad (Confidentiality, Integrity, Availablity)* dan tambahan yang lain yaitu *authenticity*, untuk menjadi standar internasional. Dan, untuk memperketat keamanan menggunakan, yaitu: menggunakan *https*, WAF(*Web Application Firewall),*dan selalu *update version port* pada sebuah web.[6]

1. 2 Rumusan Masalah

1. Apa saja hasil yang ditemukan dari *recon-ng*?
2. Ancaman apa yang ditemukan sehingga berpotensi eksploitasi?
3. Apa solusi dari hasil ancaman yang ditemukan untuk memperkuat keamanan pada *web*?
4. Hasil apa yang membuktikan jika solusi dari hasil ancaman eksploitasi berhasil?

1. 3 Tujuan Penelitian

Tujuan dari penelitian ini dilakukan yaitu:

1. Meningkatkan kesadaran kepada *devsecops* akan pentingnya meningkatkan keamanan pada web dari *hacker*.
2. Meningkatkan kesadaran bahayanya *passive information gathering*, *active information gathering,* elevasi ke ancaman eksploitasi kepada *devsecops*
3. Menyulitkan *hacker.* Sehingga, *hacker* diharuskan mencari 'jalan lain'.

1. 4 Batasan Masalah

Adapun untuk menjaga fokus analisa dalam tugas akhir ini, beberapa batasan berikut yang harus diperhatikan:

1. *Tools* yang digunakan selain *recon-ng* adalah *framework* tambahan yang bertujuan hanya untuk memperjelas dari judul tugas akhir ini.
2. *Tools* tambahan yang digunakan lebih dari satu.
3. Melibatkan *active information gathering*.
4. Tidak menampilkan simulasi yang mengeksploitasi.
5. Hanya mencari kerentanan *port* umum pada sebuah web yang sudah ditentukan. Port tersebut adalah port 0-1024.

1. 5 Manfaat Penelitian

Manfaat penelitian ini dilakukan yaitu:

1. Untuk meningkatkan keamanan pada sebuah web yang dimiliki oleh pembaca akan ancaman dari *hacker.*
2. Untuk meningkatkan *awareness* pada sebuah web yang dimiliki oleh pembaca
   akan ancaman dari *hacker.*