BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era digital, semua kegiatan yang mendukung kehidupan manusia telah dipermudah dengan adanya teknologi.[1]. Penggunaan teknologi telah menimbulkan perubahan kebutuhan serta gaya hidup manusia yang semakin butuh dan bergantung pada teknologi. Berbagai macam teknologi telah diciptakan dan dikembangkan dengan tujuan untuk membantu pekerjaan manusia. Namun, kemunculan teknologi tidak semata-mata lepas dari kejahatan yang disebut *cybercrime*.

Seiring dengan meningkatnya pengguna dari teknologi, *cybercrime* pun juga ikut meningkat dan berdampak pada banyaknya kasus *cyberattack*. Berdasarkan data yang dikumpulkan oleh Badan Siber dan Sandi Negara (BSSN) pada Januari sampai dengan Agustus dari tahun 2019 hingga 2020 terdapat kenaikan signifikan *cyberattack* dari 39 juta menjadi 189 juta. Salah satu contohnya adalah pencurian data yang merupakan bentuk kejahatan dengan mencuri data atau informasi dari orang lain yang disimpan di komputer, server, atau perangkat lain dengan tujuan untuk mendapatkan informasi rahasia atau membahayakan privasi. Data yang dicuri dapat berupa informasi rekening bank, password online, nomor paspor, nomor sim, nomor jaminan sosial, dan sebagainya. Pencurian data pertama kali terjadi pada tahun 1834 yang dialami oleh French Telegraph System, dimana sepasang pencuri meretas sistem French Telegraph System dan mencuri data informasi pasar market.[2]. Para pelaku mengembangkan berbagai jenis teknik untuk mengikuti tren terbaru agar dapat melancarkan aksinya dalam melakukan kejahatan mencuri data dari orang lain.

Salah satu teknik yang digunakan adalah *Watering Hole* yang merupakan jenis serangan menargetkan individu, organisasi, perusahaan, bahkan pemerintahan. Dalam serangan tersebut, pelaku melakukan observasi terhadap situs web yang sering dikunjungi korban, kemudian pelaku memasukan *malicious code* ke dalam situs yang sering dikunjungi oleh individu, organisasi, maupun perusahaan. Sehingga ketika korban membuka situs tersebut, perangkat dari korban akan terinfeksi oleh *payload malicious code* yang di-*inject* oleh pelaku. Pada tahun 2020 perusahaan teknologi informasi Amerika SolarWinds menjadi target dari serangan *Watering Hole* yang membutuhkan waktu hingga berbulan-bulan untuk mengidentifikasinya. Sedangkan di tahun 2021, *Google Threat Analysis* (TAG) menemukan serangan *Watering Hole* yang menargetkan pengunjung situs web outlet media, kelompok buruh, dan politik pro-demokrasi di Hongkong. Dalam serangan *Watering Hole* terdapat beberapa jenis teknik yang sering digunakan oleh pelaku untuk melancarkan aksinya, seperti *Cross-Site Scripting* (XSS), *SQL Injection*, *Brute Force*, *Zero-Day Exploitation*, *DNS Cache Spoofing*, *Malvertising*, dan *Drive-by Download*.

Serangan tersebut akan diujikan pada clone dari website KOPPERATI (Koperasi Pekerja PT. Aneka Tuna Indonesia), website tersebut berfungsi sebagai pengecekan transaksi koperasi dari PT. Aneka Tuna Indonesia secara mandiri. PT. Aneka Tuna Indonesia merupakan sebuah perusahaan yang terletak di daerah pegunungan propinsi jawa timur dan bergerak dibidang produksi dan penjualan tuna kalengan.

Pengujian serangan *watering hole* pada clone website KOPPERATI akan dilakukan menggunakan *Penetration Testing*, yang merupakan sebuah metode untuk mengevaluasi keamanan dari suatu sistem, jaringan, aplikasi web, dan perangkat dalam sebuah organisasi. Evaluasi dilakukan dengan cara melakuan sebuah simulasi serangan berdasarkan dari kejadian nyata untuk menemukan kelemahan yang ada pada sistem, jaringan, aplikasi web, dan perangkat tersebut. Tujuannya adalah mengetahui bagaimana sistem bereaksi terhadap berbagai jenis serangan yang dilakukan dan juga akibat yang dapat terjadi karena kelemahan sistem. Dalam *Penetration Testing* terdapat jenis-jenis metode yang dapat digunakan yaitu *Black Box*, *White Box*, *Grey Box*, dan juga terdapat tahapan-tahapan yang harus dilakukan seperti *Intelligence Gathering*, *Threat Modeling*, *Vulnerability Analysis*, *Exploiting*, dan *Reporting*. *Penetration Testing* merupakan metode yang penting dilakukan untuk mengeksekusi simulasi serangan guna mengeksploitasi kerentanan demi menguji keamanan sistem dari sebuah organisasi. *Penetration Testing* membantu memastikan tingkat keamanan untuk penyerang ketika mencoba untuk mendapatkan akses ke dalam jaringan internal. Itulah mengapa *Penetration Testing* memainkan peranan penting dalam jaringan dan administrasi domain supaya mencapai standar keamanan yang tinggi.

Oleh karena itu, penulis bermaksud untuk menganalisis serangan *Watering Hole* dengan teknik *Cross Site Scripting* yang digunakan sebagai teknik pencurian data dengan metode *Penetration Testing* untuk mengetahui bagaimana cara kerja serangan tersebut dan cara menghindarinya.

1.2 Rumusan Masalah

Adapun dalam pelaksanaan penelitian ini, terdapat beberapa rumusan masalah yang ingin di selesaikan, yaitu:

1. Bagaimana simulasi serangan *Watering Hole* dengan teknik XSS pada website KOPPERATI?
2. Bagaimana menganalisis serangan *Watering Hole* yang digunakan sebagai teknik pencurian data digital?

1.3 Tujuan

Adapun tujuan yang ingin dicapai dalam pelaksanaan penelitian ini adalah:

1. Menganalisis serangan *Watering Hole* sebagai teknik pencurian data digital dengan metode *Penetration Testing*.
2. Mengetahui bagaimana cara kerja dari serangan *Watering Hole*.

1.4 Batasan Masalah

Adapun batasan – batasan masalah yang dicakup dalam penelitian ini, antara lain:

1. Dalam pengujiannya, serangan *watering hole* akan disimulasikan dengan teknik *XSS*.
2. Tools yang digunakan dalam pengujian teknik *XSS* menggunakan *tool BeEF*.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian yang dilakukan adalah :

1. Diharapkan dapat memberikan manfaat tentang bahaya dari serangan *Watering Hole* yang digunakan sebagai teknik pencurian data, sehingga dapat menghindari atau mencegah kejahatan dari penggunaan teknik tersebut dimasa mendatang.
2. Dapat menjadi ilmu pengetahuan serta sumber acuan yang bermanfaat dan juga sebagai perbandingan untuk penelitian yang akan dilakukan selanjutnya.

1.6 Sistematika Penulisan

Demi memudahkan pembahasan dalam skripsi, maka penulisan dibagi menjadi beberapa BAB dengan sistematika sebagai berikut :

BAB I : Pendahuluan

Pada Bab ini meliputi latar belakang permasalahan, tujuan, rumusan masalah, Batasan masalah, metodologi penelitian dan juga sistematika penulisan.

BAB II : Landasan Teori

Pada Bab ini menjelaskan tentang konsep dari serangan *Watering Hole* dan metode *Penetration Testing*.

BAB III : Metode Penelitian

Pada Bab ini menjelaskan tentang bagaimana *serangan Watering Hole* bekerja yang akan diujikan pada website KOPPERATI menggunakan metode *penetration testing*.

BAB IV : Hasil dan Pembahasan

Dalam BAB ini akan membahas tentang Analisis dari serangan yang telah disimulasikan menggunakan tools dan metode yang digunakan, serta menjelaskan apakah serangan yang disimulasikan berjalan dengan baik dan benar.

BAB V : Penutup