

**ANALISIS SERANGAN WATERING HOLE SEBAGAI TEKNIK
PENCURIAN DATA DIGITAL PADA WEBSITE KOPPERATI
MENGUNAKAN METODE PENETRATION TESTING**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika



Disusun oleh :

Muhammad Razzy Johan Maulana

18.11.1868

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

**ANALISIS SERANGAN WATERING HOLE SEBAGAI TEKNIK
PENCURIAN DATA DIGITAL PADA WEBSITE KOPPERATI
MENGUNAKAN METODE PENETRATION TESTING**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika



Disusun oleh :

Muhammad Razzy Johan Maulana

18.11.1868

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

HALAMAN PERSETUJUAN

SKRIPSI

**Analisis Serangan Watering Hole Sebagai Teknik Pencurian Data Digital Pada Website
KOPPERATI Menggunakan Metode Penetration Testing**

Yang disusun dan diajukan oleh

Muhammad Razzy Johan Maulana

18.11.1868

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 30 Maret 2023

Dosen Pembimbing,



Subektiningsih, M.Kom.
NIK. 190302413

HALAMAN PENGESAHAN

SKRIPSI

Analisis Serangan Watering Hole Sebagai Teknik Pencurian Data Digital Pada Website
KOPPERATI Menggunakan Metode Penetration Testing

Yang disusun dan diajukan oleh

Muhammad Razzy Johan Maulana

18.11.1868

Telah diperlihatkan di depan Dewan Penguji
pada tanggal 30 Maret 2023

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Ali Mustopa, M.Kom
NIK. 190302192

Banu Santoso, S.T., M.Eng
NIK.190302327

Subektiningsih, M.Kom
NIK. 190302413



Skrripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal

DEKAN FAKULTAS ILMU KOMPUTER



Haniif Al Fatta S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Muhammad Razzy Johan Maulana
NIM : 18.11.1868

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Serangan Watering Hole Sebagai Teknik Pencurian Data Digital Pada Website KOPPERATI dengan Metode Penetration Testing

Dosen Pembimbing: Subektiningsih, M.KOM.

1. Karya tulis ini adalah benar-benar **ASLI** dan **BELUM PERNAH** diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian **SAYA** sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab **SAYA**, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini **SAYA** buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka **SAYA** bersedia menerima **SANKSI AKADEMIK** dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 01 April 2023

Yang Menyatakan,



Muhammad Razzy Johan Maulana

DAFTAR ISI

HALAMAN PERSETUJUAN.....	Error! Bookmark not defined.
HALAMAN PENGESAHAN	i
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	Error! Bookmark not defined.
DAFTAR ISI.....	iii
DAFTAR TABEL.....	vi
DAFTAR GAMBAR.....	vi
INTISARI	vii
ABSTRACT.....	viii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan.....	2
1.4 Batasan Masalah.....	2
1.5 Manfaat Penelitian.....	3
1.6 Sistematika Penulisan.....	3
BAB II TINJAUAN PUSTAKA	4
2.1 Tinjauan Pustaka.....	4
2.2 Dasar Teori.....	9
2.2.1 Cybercrime.....	9
2.2.2 Jenis – Jenis Cybercrime.....	9
2.3 Serangan Watering Hole	10
2.3.1 Jenis-Jenis Serangan dalam <i>Watering Hole</i>	10
2.3.2 Fase Serangan <i>Watering Hole</i>	11
2.3.3 Serangan <i>Watering Hole</i> Bekerja.....	12
2.3.4 Kasus Serangan <i>Watering Hole</i>	12
2.4 Penetration Testing.....	13
2.4.1 Metode dalam Penetration Testing	13
BAB III METODE PENELITIAN	15
3.1 Alur Penelitian.....	15
3.1.1 Intelligence Gathering.....	16

3.1.2	Threat Modeling.....	17
3.1.3	Vulnerability Analysis.....	17
3.1.4	Exploiting.....	17
3.1.5	Reporting.....	17
3.2	Instrumen Penelitian.....	17
3.2.1	Data Penelitian.....	17
3.2.2	Alat dan Bahan.....	19
3.3	Skenario Serangan.....	19
3.3.1	Cross-Site Scripting.....	19
BAB IV HASIL DAN PEMBAHASAN.....		20
4.1	Intelligence Gathering.....	20
4.2	Vulnerability Analysis.....	21
4.3	Exploiting.....	23
4.3.1	Pengujian Serangan Cross-Site Scripting (XSS).....	23
4.4	Report.....	25
4.4.1	The Executive Summary.....	26
4.4.2	Vulnerabilities.....	26
4.4.3	Cara Menghindari.....	27
BAB V PENUTUP.....		28
5.1	Kesimpulan.....	28
5.2	Saran.....	28
REFERENSI.....		29

DAFTAR TABEL

Tabel 4.4.1 Hasil whois lookup	26
Tabel 4.4.2 Threat dan Severity Level.....	26
Tabel 4.4.3 Pengujian Serangan Cross Site Scripting.....	27
Tabel 4.4.5 Hasil Pengujian Serangan	27

DAFTAR GAMBAR

Gambar 2.1 Prinsip kerja Serangan <i>Watering Hole</i> . [3]	12
Gambar 3.1 Tahapan PTES.....	15
Gambar 3.2 Alur Penelitian	16
Gambar 3.4 Data Penelitian	18
Gambar 3.5 Skenario Serangan XSS S Pada	19
Gambar 4.1 Instalasi BeEF-XSS.....	20
Gambar 4.2 Instalasi Burp Suite.....	Error! Bookmark not defined.
Gambar 4.3 Hasil Identifikasi Website KOPPERATI Menggunakan whois lookup	21
Gambar 4.4 Hasil Scan Website KOPPERATI Menggunakan Acunetix.....	21
Gambar 4.5 Menjalankan BeEF Service.....	23
Gambar 4.6 Hasil Dari Hook.js Pada Website KOPPERATI.....	24
Gambar 4.7 Tab Command.....	24
Gambar 4.8 Halaman Google Phising Pada Browser Pengakses	25
Gambar 4.9 Hasil Dari Penggunaan Google Phising Pada Browser Pengakses.....	25

INTISARI

Di era digital, semua kegiatan pendukung kehidupan manusia telah dipermudah dengan adanya teknologi yang juga telah menimbulkan perubahan kebutuhan serta gaya hidup manusia yang semakin butuh dan bergantung pada teknologi. Namun kemunculan tersebut tidak semata-mata lepas dari kejahatan *cybercrime* terutama *watering hole attack* yang merupakan jenis serangan yang menargetkan kelompok tertentu dengan cara menyuntikan *malicious code* kedalam sistem dari web yang sering dikunjungi oleh target. Sehingga ketika target mengakses situs tersebut, perangkat dari target akan terinfeksi oleh payload *malicious code* yang di-*inject* oleh pelaku. Oleh karena itu, penulis bermaksud untuk menganalisis serangan *watering hole* dengan teknik XSS menggunakan metode *penetration testing* pada website KOPPERATI untuk mengetahui bagaimana cara kerja dari serangan tersebut. *Penetration Testing* merupakan sebuah metode yang digunakan untuk mengevaluasi keamanan dari suatu sistem dengan cara melakukan simulasi serangan pada sistem untuk mengetahui bagaimana sistem bereaksi terhadap serangan yang dilakukan. Sedangkan website KOPPERATI merupakan website yang berfungsi sebagai pengecekan transaksi koperasi PT. Aneka Tuna Indonesia secara mandiri. Hasil yang didapatkan dari penelitian yang dilakukan berupa serangan *watering hole* dengan teknik *cross site scripting* adalah penyerang akan menginject *script hook.js* kedalam sistem dari website dan menunggu hingga target mengakses website tersebut, setelah target mengakses website tersebut, maka *hook.js* secara otomatis akan mengirimkan respon kepada server dari *BeEF* untuk menjalankan *Command Exploitation* pada browser dari target.

Kata kunci : Serangan Watering Hole, Penetration Testing, Cross Site Scripting



ABSTRACT

In the digital era, all activities that support human life have been facilitated by technology, which has also led to changes in human needs and lifestyles that are increasingly dependent on technology. However, this emergence is not solely separated from cybercrime crimes, especially watering hole attacks which are types of attacks that target certain groups by injecting malicious code into the system from the web that is frequently visited by the target. So that when the target accesses the site, the target's device will be infected by the payload of the malicious code injected by the perpetrator. Therefore, the author intends to analyze watering hole attacks with XSS using the penetration testing method on the KOPPERATI website to find out how these attacks work. Penetration Testing is a method used to evaluate the security of a system by simulating attacks on the system to find out how the system reacts to the attacks being carried out. While the KOPPERATI website is a website that functions as a checking of PT. cooperative transactions. Various Indonesian Tuna independently. The results obtained from the research conducted in the form of a watering hole attack with a cross site scripting technique is that the attacker will inject the hook.js script into the system from the website and wait until the target accesses the website, after the target accesses the website, then hook.js will automatically send response to the server from BeEF to run an Exploitation Command on the target browser.

Keyword : *Watering Hole Attack, Penetration Testing, Cross Site Scripting*

