# Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning

**Erick Irawadi Alwi[1], Herdianti[2], Fitriyani Umar[3]**
[1]Program Studi Sistem Informasi, Fakultas Ilmu Komputer Universitas Muslim Indonesia
[2,3]Program Studi Teknik Informatika, Fakultas Ilmu Komputer Universitas Muslim Indonesia
[1]erick.alwi@umi.ac.id, [2]herdianti.darwis@umi.ac.id, [3]fitriyani.umar@umi.ac.id

**ABSTRACT**

Website security is an effort to protect websites from hacker attacks connected through a network. Website security needs to be a concern in the midst of many cases of website hacking from irresponsible people, including websites at Indonesian tertiary institutions that provide information and services to the public, students, and alumni of tertiary institutions.

Higher education institution websites that can be accessed widely online can create vulnerabilities against threats from hacker attacks. To minimize this vulnerability, it is necessary to test the website of the higher education institution to assess and evaluate the security system of the university's website. The research method used in this study is the Ethical Hacking method which focuses on footprinting techniques and vulnerability scanning by only testing passive attacks. The results of this study have found information related to the target website (the website of an educational institution in one of the cities in Indonesia) and several vulnerability alerts after testing vulnerability scanning with high to low risk levels so that researchers recommend improving vulnerability to minimize security holes exploited by hackers .

***Keyword:*** Website, Security, Hacker, Footprinting, Vulnerability

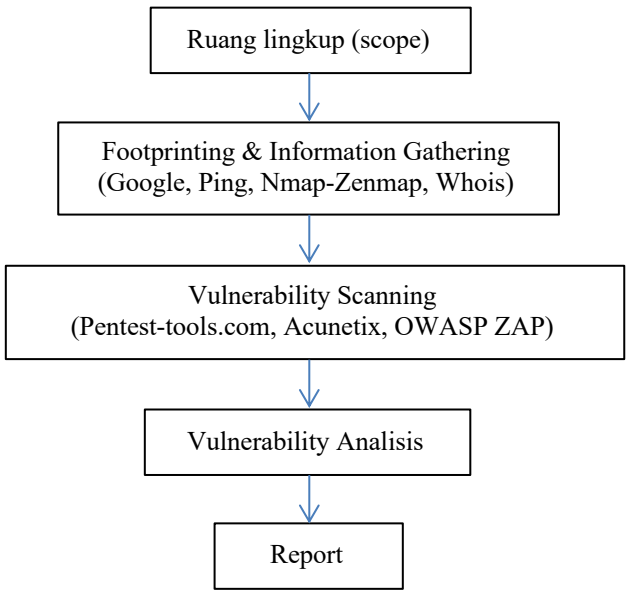
## 1. Introduction

Website adalah sekumpulan halaman informasi yang disediakan melalui jalur internet sehingga dapat diakses seluruh dunia selama terkoneksi dengan jaringan internet tanpa terbatas ruang dan waktu [1]. Keamanan informasi pada website merupakan suatu hal yang wajib diperhatikan, tidak terkecuali website pada institusi perguruan tinggi di indonesia yang menyajikan informasi dan layanan pada masyarakat, mahasiswa, dan alumni perguruan tinggi. Masalah tersebut penting karena jika informasi pada website diakses oleh orang yang tidak bertanggung jawab maka keakuratan informasi tersebut akan diragukan bahkan bisa menjadi informasi yang menyesatkan [2].

*Vulnerability* adalah suatu kelemahan yang mengancam nilai *integrity*, *confidentiality*, dan *availability* dari suatu aset [3]. *Ethical hacking* adalah suatu metode meliputi penggunaan aplikasi *hacking*, trik-trik dan teknik untuk mengidentifikasi *vulnerability* dari sistem guna memastikan keamanannya [4]. Dari permasalahan diatas peneliti akan melakukan pengujian terhadap website pada salah satu institusi perguruan tinggi di indonesia untuk menilai seberapa rentan celah keamanan untuk di eksploitasi oleh peretas (*hacker*). Pengujian penetrasi pada jaringan merupakan salah satu metode yang dapat digunakan untuk mengidentifikasi kerentanan keamanan pada website [5]. Kerentanan pada keamanan website merupakan hal yang harus diperhatikan bagi setiap institusi agar terhintar dari tindakan kejahatan di dunia maya *(CyberCrime)* [6].

## 2. Research Method

Penelitian ini dilakukan dengan menggunakan metode *Ethical Hacking*, dimana nantinya peneliti akan fokus pada tahapan *Footprinting* dan *Vulnerability Scanning* untuk melakukan pengujian *vulnerability*. Adapun objek (target) pada penelitian ini yaitu website salah satu institusi perguruan tinggi di indonesia yang akan dilakukan pengujian vulnerability dengan menggunakan tools dan aplikasi vulnerability scanner untuk mendapatkan informasi vulnerability. Berikut tahapan penelitian dapat dilihat pada Gambar 1.




Gambar 1. Tahapan Penelitian

1. Ruang lingkup (scope) : tahapan awal dalam melakukan penelitian ini adalah menentukan batasan-batasan (scope) terhadap website target yang akan diuji yaitu peneliti hanya melakukan *vulnerability* scanning (kerentanan) secara *passive attack* tanpa melakukan eksploitasi terhadap sistem seperti merubah tampilan, melakukan DDos, dan lain-lain.
2. *Footprinting & Information Gathering*: Tahapan ini dilakukan untuk mendapatkan informasi sebanyak-banyaknya yang terkait dengan *network inventory*, seperti perangkat apa saja yang digunakan merek, tipe, nomor versi OS, topologi fisik, perangkat *security network address*.
3. *Vulnerability Scanning*: tahapan dilakukan *scanning network* dengan memanfaatkan berbagai tools network scanning dan vulnerability scanner online. tujuan yang ingin dicapai adalah memperoleh informasi *vulnerability network* tersebut, misal daftar *port* yang terbuka, bug pada aplikasi server, dan lain-lain yang kadangkala fase ini disebut sebagai *passive attack*.
4. Vulnerability Analysis : pada tahap ini peneliti akan menganalisis informasi-informasi *vulnerability* yang ditemukan setelah dilakukan scanning terhadap target dengan beberapa tool network scanning dan web *vulnerability scanner online* serta akan memberikan rekomendasi bagaimana memperbaiki atau menutupi *vulnerability* yang telah ditemukan.
5. Dokumentasi dan Laporan: Tahapan ini akan mendokumentasikan hasil analisa dari celah keamanan website target yang nantinya dapat menjadi pegangan bagi pengelola website target untuk mengetahui apa saja yang sudah dilakukan peneliti.

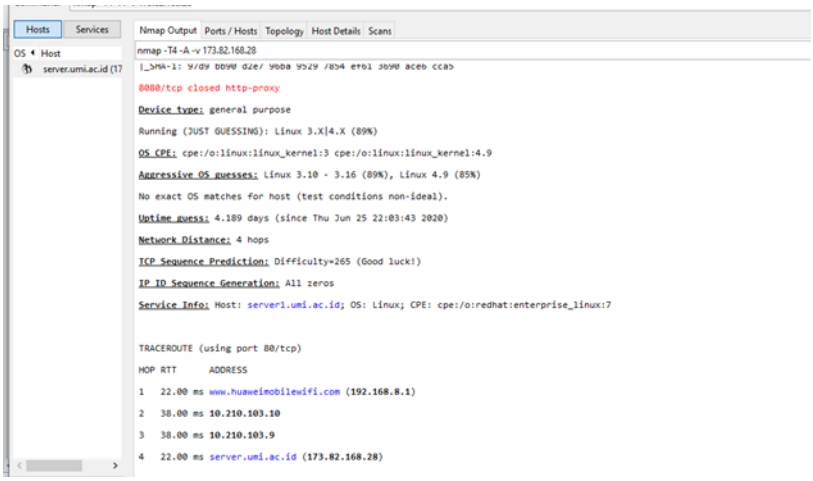
## 3. Result and Analysis

Metode pengujian pada website target dilakukan dengan 2 teknik di dalam metode *Ethical Hacking* yaitu *footprinting* dan *vulnerability scanning.*

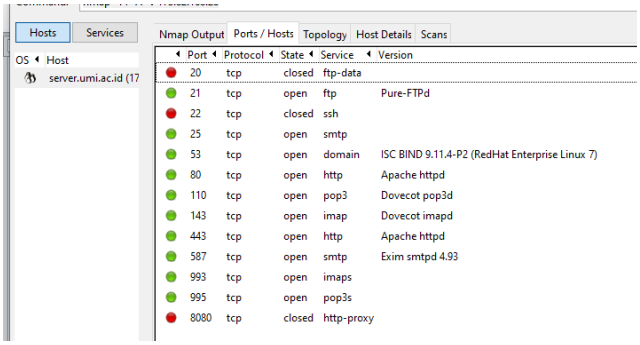
### 3.1. Hasil pengujian dengan teknik footprinting

*Footprinting* adalah kegiatan mengumpulkan informasi sebanyak-banyaknya yang terkait dengan target, seperti perangkat yang digunakan, merek, tipe, nomor versi OS, topology fisik network, perangkat *security, network address, subnetting*, dan lain-lain [7]. Adapun tools footprinting yang digunakan pada penelitian ini yaitu aplikasi CMD (command prompt), aplikasi Zenmap, dan Whois domain.

3.1.1 Hasil footprinting dengan Zenmap




Gambar 2. Hasil scanning Zenmap




Gambar 3. Hasil scanning port Zenmap

Dari hasil gambar 2 dan gambar 3 diatas bahwa dengan scanning IP server target (172.82.xxx.xx) dengan perintah command nmap –T4 –A –v 173.82.xxx.xx, aplikasi Zenmap menemukan beberapa informasi terkait target yaitu antara lain Operating system (OS) version, Traceroute , Topologi jaringan target , Service version pada server dan port yang terbuka. Dengan ditemukannya informasi-informasi tersebut dapat menjadi informasi penting bagi penyerang (hacker) untuk mengeksploitasi jaringan dari target.

Tabel 1. Hasil pengujian Footprinting pada website target

| No | Tools Footprinting & Information Gathering | Informasi yang ditemukan target |
|---|---|---|
| 1 | CMD (ping) | IP Server |
| 2 | Zenmap | Operating system (OS) version |
| | | Port-port yang terbuka |
| | | Traceroute |
| | | Topologi jaringan |
| | | Service pada server dan version |
| 3 | Whois | Nama domain |
| | | Alamat IP |
| | | Lokasi server |
| | | Server software |

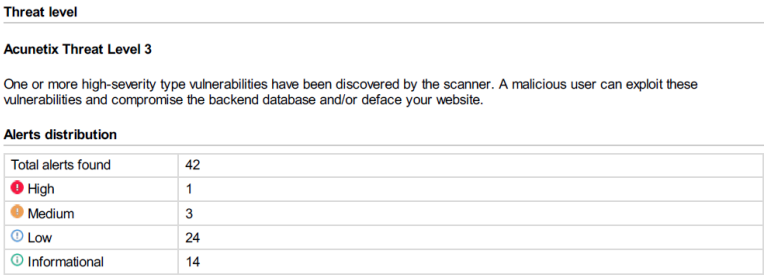
| No | Tools Footprinting & Information Gathering | Informasi yang ditemukan target |
|---|---|---|
| | | Reverse IP |

Dari hasil pengujian pada Tabel 1 terlihat hasil pengujian Footprinting pada website target dengan menggunakan tools Footprinting (Zenmap dan Whois) ditemukan beberapa informasi terkait target sebagai sub domain dari xxxxxx.ac.id antara lain IP Server, Operating system (OS) version server, port-port yang terbuka, topologi jaringan, service pada server dan version dan lokasi server. peneliti memberikan rekomendasi kepada admin pengelola website untuk memprotect informasi-informasi data sensitif dari website (whois protect) agar pihak yang tidak berkepentingan (hacker) tidak dapat mengakses dan tidak dapat mengekploitasi lebih lanjut informasi tersebut.

### 3.2. Hasil pengujian dengan teknik vulnerability scanning

Vulnerability scanning adalah proses memperoleh informasi *vulnerability network* dengan memanfaatkan berbagai *tools network scanning* dan *vulnerability scanner*, seperti port yang terbuka, *bugs* aplikasi server dan lain-lain [7]. adapun tools yang digunakan pada penelitian ini yaitu vulnerability scanner online pentest-tools.com, aplikasi web vulnerability Acunetix dan OWASP ZAP dalam melakukan pengujian vulnerability scanning pada target.

3.2.1 Hasil vulnerability scanning dengan Acunetix



**Threat level**

**Acunetix Threat Level 3**

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

**Alerts distribution**

| | |
|---|---|
| Total alerts found | 42 |
| High | 1 |
| Medium | 3 |
| Low | 24 |
| Informational | 14 |

Gambar 3. Hasil scanning Acunetix

Dari hasil gambar 3 diatas terlihat bahwa web aplikasi Acunetix mengkategorikan website target dengan High Risk Alert Level 3 yang artinya vulnerability yg ditemukan dikategorikan sebagai yang paling berbahaya, yang menempatkan target scan pada risiko maksimum untuk hacking dan pencurian data. Adapun rincian vulnerability yang ditemukan yaitu 1 high risk level, 3 medium risk level, 24 low risk level dan 14 informational.

Tabel 2. Hasil pengujian Vulnerability Scanning target

| No | Vulnerability Scanner | Alert | Risk Level |
|---|---|---|---|
| 1 | Pentest-tools.com | Insecure HTTP cookies | Medium |
| | | Directory listing is enabled | Medium |
| | | Server software and technology found | Low |
| | | Missing HTTP security headers | Low |
| | | Robots.txt file found | Low |
| 2 | Acunetix | CORS (Cross-Origin Resource Sharing) origin validation failure | High |
| | | Directory listing | Medium |
| | | HTML form without CSRF protection | Medium |
| | | WordPress username enumeration | Medium |
| | | Clickjacking: X-Frame-Options header | Low |

| No | Vulnerability Scanner | Alert | Risk Level |
|---|---|---|---|
| | | missing | |
| | | Cookie(s) without Secure flag set | Low |
| | | Login page password-guessing attack | Low |
| | | Cookie(s) without HttpOnly flag set | Low |
| | | Possible sensitive directories | Low |
| | | WordPress admin accessible without HTTP authentication | Low |
| | | WordPress REST API User Enumeration | Low |
| 3 | OWASP ZAP | X-Frame-Options Header Not Set | Medium |
| | | Incomplete or No Cache-control and Pragma HTTP Header Set | Low |
| | | X-Content-Type-Options Header Missing | Low |
| | | Cookie Without SameSite Attribute | Low |
| | | Absence of Anti-CSRF Tokens | Low |
| | | Cookie No HttpOnly Flag | Low |

Dari hasil pengujian vulnerability scanning pada Tabel 2 terlihat celah vulnerability scanning pada website target dengan menggunakan tools vulnerability scanner secara online (Pentest-tools.com dan Acunetix) maupun aplikasi vulnerability (OWASP ZAP) ditemukan beberapa risk vulnerability (kerentanan) terhadap website target antara lain. pada tools vulnerability scanning online pentest.com ditemukan 0 vulnerability risk high, 2 vulnerability risk medium, 3 vulnerability risk low, tool acunetix ditemukan 1 vulnerability risk high, 4 vulnerability risk medium, 7 vulnerability risk low, dan tool aplikasi OWASP ZAP ditemukan 0 vulnerability risk high, 1 vulnerability risk medium, dan 5 vulnerability risk low.

Dari Tabel 2 dapat disimpulkan bahwa ada celah keamanan (vulnerability) dari website target yang ditemukan paling sering baik dengan tool vulnerability scanner online maupun aplikasi vulnerability scanning antara lain, X-Frame-Options Header Not Set, Cookie No HttpOnly Flag, Directory listing is enabled sehingga peneliti merekomendasikan beberapa perbaikan pada konfigurasi web server dari website target untuk meminimalisir celah keamanan tersebut di eksploitasi oleh hacker. Rekomendasi perbaikan celah keamanan (vulnerability) dari website target dibuat dalam bentuk report (laporan) detail terkait, vulnerability, dampak dari vulnerability, dan rekomendasi perbaikan vulnerability yang ditemukan.

## 4. Conclusion

Beberapa hal yang dapat disimpulkan dari hasil penelitian ini, antara lain:

1. Pada website target telah ditemukan celah keamanan (*vulnerability*) dengan *alert risk level high* hingga *low* antara lain CORS (*Cross-Origin Resource Sharing*) *origin validation failure (high)*, X-Frame-Options Header Not Set (Medium), *Directory listing is enabled* (Medium), HTML form without CSRF protection (Medium), WordPress username enumeration (Medium), dan Cookie No HttpOnly Flag (Low)
2. Dengan ditemukannya beberapa *vulnerability* pada website target, peneliti membuat rekomendasi perbaikan dalam bentuk *report* (laporan) untuk pengelola website sehingga dapat menjadi pegangan untuk admin pengelola website dalam melakukan perbaikan celah keamanan (*vulnerability*).

**Acknowledgements**

Alhamdulillah puji syukur kepada Allah swt, karena kehendak dan ridha-Nya peneliti dapat menyelesaikan penelitian ini serta ucapan terima kasih kepada YW Universitas Muslim Indonesia untuk dana penelitian dosen pemula LP2S UMI dan Dr. Ir. Hj. Setyawati Yani, ST., MT., PhD., IPM., ASEAN.Eng sebagai reviewer penelitian dosen pemula LP2S UMI atas saran dan tanggapannya pada penelitian ini.

**References**

[1] Robby, Pratama, "Analisis Web Vulnerability pada Portal Pemerintahan Kota Palembang menggunakan Acunetix Vulnerability", *Thesis* Universitas bina darma, 2013.
[2] Marsoni, Toibah Umi Kalsum, Adhadi Kurniawan," Analisa Implementasi Teknik *Reconnaissance* Pada Webserver (Studi Kasus: UPT Puskom Universitas Dehasen)", Jurnal Media Infotama Vol. 12 No. 1, Februari 2016
[3] Devi Christiani Angir, Agustinus Noertjahyana, Justinus Andjarwirawan, "*Vulnerability* Mapping Pada Jaringan Komputer Di Universitas X", Jurnal infra Vol 3, No. 2: 2015
[4] Richard Pangalila, Agustinus Noertjahyana, Justinus Andjarwirawan, "*Penetration Testing* Server Sistem Informasi Manajemen dan Website Universitas Kristen Petra", Jurnal infraVol 3, No 2: 2015
[5] Wahyudi, "*Analisa Pengujian Kerentanan Terhadapweb Serversimak (Studi Kasus: STMIK Kharisma Karawang)*", Jurnal Teknologi Informasi Vol. 5, No. 1: Juni 2019
[6] Yunus, "*Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Projectberdasarkan Framework OWASP VERSI 4*", Jurnal Ilmiah Informatika Komputer Vol. 24, No. 1: April 2019
[7] Sofana, Iwan. 2019. *Network Security dan Cyber Security*. Bandung : Informatika Bandung