

ANALISIS KERENTANAN WEBSITE AKADEMIK MENGGUNAKAN METODE PENETRATION WEB

Zaky Nour Rizqy¹⁾, Bayu Murti²⁾, Syahrul Himawan³⁾

Program Studi Teknologi Informasi

^{1),2),3)}Universitas Jenderal Achmad Yani Yogyakarta

e-mail: ¹⁾Kelastambah@gmail.com, ²⁾Radenkuma040@gmail.com,

³⁾Keongkampung01@gmail.com

ABSTRACT

Vulnerability penetration is commonly considered to be the most efficient way to check your site against a huge list of known vulnerabilities - and identify potential weaknesses in the security of your applications. Vulnerability scanning can be used as part of a standalone assessment, or as part of a continuous overall security monitoring strategy.

Keywords : *Vulnerability penetration, Web vulnerability*

ABSTRAK

Penetrasi kerentanan umumnya dianggap sebagai cara paling efisien untuk memeriksa situs Anda terhadap daftar besar kerentanan yang diketahui dan mengidentifikasi potensi kelemahan dalam keamanan aplikasi Anda. Pemindaian kerentanan dapat digunakan sebagai bagian dari penilaian mandiri, atau sebagai bagian dari strategi pemantauan keamanan keseluruhan yang berkesinambungan.

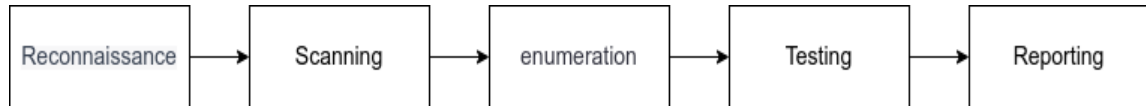
Kata kunci : *penetrasi kerentanan, kerentanan web*

I. PENDAHULUAN

Perkembangan teknologi dan informasi adalah sebuah peluang sekaligus tantangan yang melahirkan segala aspek kehidupan mulai dari ruang lingkup terkecil yaitu individu, sampai pada ruang yang begitu luas yaitu negara oerubahan dalam bahkan dunia. Pesatnya kemajuan di bidang teknologi dan infromasi juga telah memberikan pengaruh besar terhadap seluruh komponen kehidupan, mulai dari ekonomi, politik, social serta keamanan. Perkembangan teknologi dan informasi di era sekarang in telah membentuk ruang kehidupan baru untuk manusia saling berinteraksi, ruang tersebut disebut dengan cyber space. Secara singkat cyber space merupakan sebuah tempat maya dimana komunikasi antar pengguna terjadi, kemunculan dan meningkatnya penggunaan cyber space ini menghadirkan kemudahan bagi para oenggunanya untuk berhubungan dengan orang lain, namun hal tersebut juga bersamaan dengan dampak negative yang berupa ancaman dari dan untuk individu, organisasi dan pemerintahan.

II. METODE PENELITIAN

Penelitian ini adalah penelitian untuk menganalisis rentan keamanan suatu website menggunakan system penetration testing. Alur dari metode penelitian ini ditunjukkan pada Gambar 1.



Gambar 1. Metode analisis website

Tahap 1. Reconnaissance, Uji penetrasi di mana pentester menemukan informasi sebanyak mungkin tentang situs web target[1].

Tahap 2. Scanning, Fase awal setiap serangan pada website. Selama fase ini, penyerang mengumpulkan informasi tentang struktur web dan infrastruktur pendukung. Situs Web target dipindai untuk kerentanan yang diketahui dalam perangkat lunak infrastruktur serta kerentanan yang tidak diketahui dalam kode kustom yang dikembangkan untuk target tertentu[2].

Tahap 3. Enumeration, Dilakukan setelah tahap scanning selesai, dimana pentester telah menemukan kelemahan atau celah yang ada pada website tersebut[3].

Tahap 4. Testing, Suatu proses yang dilakukan untuk menguji keamanan suatu system, jaringan, atau aplikasi dengan cara menyerangnya seolah-olah seperti dilakukan oleh seorang hacker[4].

Tahap 5. Reporting, Proses menyampaikan laporan tentang keberhasilan atau kegagalan sebuah serangan penetrasi ke isstem atau jaringan tertentu[5].

III. PEMBAHASAN

Untuk melakukan penelitian ini Tool yang digunakan yaitu : Whatweb, WPScan, Dnsdmpstr, Amass.

- A. Informasi domain utama website akademik “X” menggunakan tools whatweb dan WPScan.

HTTPServer: Apache 2

IP: 103.28.xx.xx

CMS: Wordpress 6.1.1

Theme: Onepress

Plugin: Accesspress-social-icons, add-to-any, Contact-form-7, grid-plus, responsive tabs, sp-fag, whatsapp-for-wordpress, wordpress-seo, wp-simple-firewall.

Bootstrap: 2.0.6

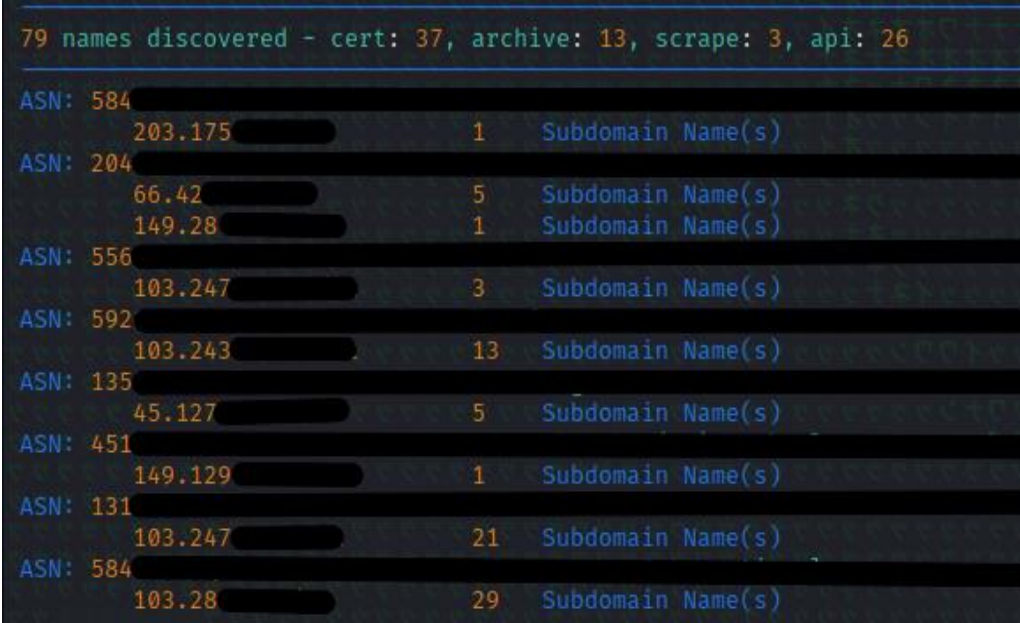
Email: info@X.ac.id

Cookies: Shield notbot nonce

X=XSS=Protection: 1: Mode-Block

B. Scanning subdomain website menggunakan tools Amass.

Tool Amass merupakan Proyek Amass OWASP melakukan pemetaan jaringan permukaan serangan dan penemuan system eksternal menggunakan pengumpulan informasi sumber terbuka dan system pengintaian aktif[6].



```

79 names discovered - cert: 37, archive: 13, scrape: 3, api: 26
ASN: 584
203.175 1 Subdomain Name(s)
ASN: 204
66.42 5 Subdomain Name(s)
149.28 1 Subdomain Name(s)
ASN: 556
103.247 3 Subdomain Name(s)
ASN: 592
103.243 13 Subdomain Name(s)
ASN: 135
45.127 5 Subdomain Name(s)
ASN: 451
149.129 1 Subdomain Name(s)
ASN: 131
103.247 21 Subdomain Name(s)
ASN: 584
103.28 29 Subdomain Name(s)

```

Gambar 2. Hasil Scanning

C. Scanning open port menggunakan nmap.

Nmap ("Network Mapper") merupakan sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Ia dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal. Nmap menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, system operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya. Meskipun Nmap umumnya digunakan untuk audit keamanan, namun banyak administrator system dan jaringan menganggapnya berguna untuk tugas rutin seperti inventori jaringan, mengelola jadwal upgrade layanan, dan melakukan monitoring uptime host atau layanan.

Output Nmap adalah sebuah daftar target yang diperiksa, dengan informasi tambahannya tergantung pada opsi yang digunakan. Hal kunci di antara informasi itu adalah "system port menarik". Tabel tersebut berisi daftar angka port dan system, nama layanan, dan status. Statusnya adalah terbuka (open), difilter (filtered), tertutup (closed), atau tidak difilter (unfiltered). Terbuka berarti bahwa aplikasi pada mesin target sedang mendengarkan (listening) untuk koneksi/paket pada port tersebut. Difilter berarti bahwa sebuah firewall, filter, atau penghalang jaringan lainnya memblokir port sehingga Nmap tidak dapat mengetahui apakah ia terbuka atau tertutup. Tertutup port tidak memiliki aplikasi yang sedang mendengarkan, meskipun mereka dapat terbuka kapanpun. Port digolongkan sebagai tidak difilter system mereka menanggapi probe Nmap, namun Nmap tidak

dapat menentukan apakah mereka terbuka atau tertutup. Nmap melaporkan kombinasi status open|filtered dan closed filtered system ia tidak dapat menentukan status manakah yang menggambarkan sebuah port. Tabel port mungkin juga menyertakan detail versi software system diminta melakukan pemeriksaan versi. Ketika sebuah pemeriksaan system IP diminta (-sO), Nmap memberikan informasi pada system IP yang didukung alih-alih port-port yang mendengarkan.

Selain system port yang menarik, Nmap dapat pula memberikan informasi lebih lanjut tentang target, termasuk nama reverse DNS, prakiraan system operasi, jenis device, dan alamat MAC[7].

Hasil scanning open port menggunakan Nmap dengan kerentanan keamanan high.

Tabel 1. Hasil scanning menggunakan Nmap

IP Address	Hasil Scanning nmap
203.175xxx	- (<i>website mati</i>)
66.42xxx	FTP
149.28xxx	FTP, SSH
103.247xxx	SSH
103.243xxx	FTP
45.127xxx	-
149.129.xxx	SSH
103.247xxx	FTP
103.28xxx	-

D. Penetrasi menggunakan OWASP ZAP dan OWASP DirBuster

ZAP memungkinkan Anda mencoba menemukan direktori dan file menggunakan penelusuran paksa. Satu set file disediakan yang berisi sejumlah besar nama file dan direktori.

ZAP mencoba untuk langsung mengakses semua file dan direktori yang tercantum dalam file yang dipilih secara langsung daripada mengandalkan menemukan tautan ke sana.

Penetrasi menggunakan OWASP ZAP dan OWASP DirBuster memperoleh kerentanan sebagai berikut :

Tabel 2. Hasil Petrasi menggunakan OWASP ZAP dan OWASP DirBuster

Kerentanan	Jenis Kerentanan
High	Path Traversal Files Permissions

Berdasarkan Hasil pengujian OWASP ZAP dan OWASP DirBuster, Berikut kerentanan File Permissions yang ditemukan:

File permission adalah fitur keamanan yang berfungsi untuk mengamankan folder/ file agar tidak dapat dilihat atau dieksekusi oleh orang lain yang tidak memiliki hak.

DirBuster adalah alat pengujian penetrasi file/direktori dengan Antarmuka Pengguna Grafis (GUI) yang digunakan untuk memaksa direktori dan nama file di server aplikasi web[8].

```
<?php
if [REDACTED]
    return;
} else {
    [REDACTED]
}

$user=[REDACTED]
$password=[REDACTED]
$host=[REDACTED]

[REDACTED]
?>
```

Gambar 3. Database Login

```
<?php [REDACTED]

unset($CFG);
global $CFG;
$CFG = new stdClass();

$CFG->dbtype      = [REDACTED];
$CFG->dblibrary   = [REDACTED];
$CFG->dbhost      = [REDACTED];
$CFG->dbname      = [REDACTED];
$CFG->dbuser      = [REDACTED];
$CFG->dbpass      = [REDACTED];
$CFG->prefix      = [REDACTED];
$CFG->dboptions   = array (
    'dbpersist' => [REDACTED],
    'dbport'    => [REDACTED],
    'dbsocket'  => [REDACTED]
);

$CFG->wwwroot     = [REDACTED];
$CFG->dataroot     = '/var/www/[REDACTED]';
$CFG->admin       = [REDACTED];

$CFG->directorypermissions = 0777;

require_once(__DIR__ . [REDACTED])
```

Gambar 4. Database Login

```
[server:SMTP [REDACTED]]
[port:SMTP [REDACTED]]
[secure:SMTP [REDACTED]]
[username:SMTP [REDACTED]]
[password:SMTP [REDACTED]]
```

Gambar 5. Email Login

IV. KESIMPULAN

Penetration web pada sebuah instansi akademik sebaiknya dilakukan secara berkala sebagai wujud implementasi dan mengukur kesiapan keamanan dari serangan siber. Hasil dari penetration web yang dilakukan dapat disimpulkan bahwa rentan keamanan website akademik “X” dalam kategori medium. Tetapi, terdapat beberapa kerentanan keamanan dalam kategori high.

Hasil dari penetration web perlu ditindak lanjuti dengan tahapan berikutnya oleh eksternal penetration tester dari pihak akademik terkait. Hal ini bertujuan untuk memperbaiki celah keamanan sesuai temuan atau laporan pada penelitian ini.

V. DAFTAR PUSTAKA

- [1] shivaysabharwal, “Reconnaissance | Penetration Testing,” *www.geeksforgeeks.org*. <https://www.geeksforgeeks.org/reconnaissance-penetration-testing/>
 - [2] “Site Scanning/Probing,” *www.ptonline.com*. <https://www.ptonline.com/articles/how-to-get-better-mfi-results>
 - [3] “Emuration and its Types,” *greycampus.com*. <https://www.greycampus.com/opencampus/ethical-hacking/enumeration-and-its-types>
 - [4] “Penetration Testing,” *imperva.com*. <https://www.imperva.com/learn/application-security/penetration-testing/>
 - [5] “Web App PenTest Reporting - Introduction to writing a penetration testing report [FREE COURSE CONTENT],” *hakin9.org*. <https://www.imperva.com/learn/application-security/penetration-testing/>
 - [6] caffix, “OWASP/Amass,” *github.com*. <https://github.com/OWASP/Amass>
 - [7] “Panduan Refensi Nmap (Man Page, bahasa Indonesia),” *nmap.org*. <https://nmap.org/man/id/index.html>
 - [8] A. Kumar, “Explaining DirBuster,” *faun.pub*, 2021. <https://faun.pub/what-is-dirbuster-and-how-to-use-it-1db3c3d3113b>
-