Website : http://pilar.unmermadiun.ac.id/index.php/pilarteknologi

Analisis dan Pengujian Celah Keamanan pada Website DIV Teknik Informatika Politeknik Harapan Bersama

Dega Surono Wibowo[1], Ardi Susanto[2], Khibar Pusaka[3]

[1,2,3]*Program Studi DIV Teknik Informatika, Politeknik Harapan Bersama, Jl. Mataram No.9, Tegal, 52147*
*E-mail: *[1]dega.wibowo@poltektegal.ac.id, [2]ardisusanto@poltektegal.ac.id, [3]khibarpusaka01@gmail.com*

Abstract— **Dewasa ini halaman web merupakan salah satu media informasi modern yang berkembang pesat. Halaman web dibuat tidak hanya dari sisi desain dan informasi apa saja yang bisa disajikan, akan tetapi harus melihat dari aspek keamanannya juga. Karena keamanan halaman web merupakan hal yang sangat penting, jebutuhan tentang keamanan halaman web muncul untuk melindungi data dan informasi yang ada didalamnya. Metode yang digunakan untuk pengujian keamanan halaman web ini menggunakan tools yang berupa perangkat lunak dan dengan cara-cara tertentu untuk menguji keamanan halaman web. Sedangkan untuk melakukan analisis keamanannya juga digunakan tools yang serupa. Dengan demikian target khusus pada penelitian ini adalah seberapa rentan halaman web dari Program Studi DIV Teknik Informatika Politeknik Harapan Bersama dan dengan cara apa sajakah yang memungkinkan untuk menutup celah keamanan tersebut.**

Keywords*—: *web, keamanan, kerentanan

I. PENDAHULUAN

Informasi adalah hasil pengolahan data dalam suatu bentuk yang lebih berguna dan lebih memiliki arti bagi yang menerima informasi tersebut, sehingga penerima informasi dapat menggunakannya sebagai pengambilan keputusan. Sedangkan data merupakan representasi dari suatu fakta, yang dimodifikasi bias dalam bentuk gambar, kata, dan atau angka. Dikarenakan adanya tatacara penggunaan dan tujuan tertentu, data menjadi sangat sensitive ketika bersifat rahasia.

Keamanan sistem informasi merupakan topik utama dalam perkembangan teknologi informasi dan komunikasi. Untuk melindungi aset informasi suatu organisasi, perlu adanya pendekatan yang konprehensif dan terstruktur untuk memberikan perlindungan dari resiko yang mungkin akan dihadapi. Perlu ada jaminan keamanan data, transaksi, dan komunikasi dengan menerapkan sebuah Metode keamanan data [1]

Seiring pesatnya perkembangan teknologi maka para hacker juga semakin pintar dalam menjalankan pola kegiatan ilegal. Dengan kata lain semakin banyak para hacker yang memanfaatkan kelemahan pada sebuah Webserver untuk mendapatkan keuntungan pribadi maupun organisasi yang dijalankannya. Melihat kasus yang sering terjadi, seharusnya kita dapat mengambil langkah cepat untuk mengamankan Webserver dan apabila diabaikan maka webserver yang di miliki oleh suatu badan institusi baik milik perintah, swasta, maupun perseorangan dapat mengalami kerugian yang diakibatkan oleh para hacker [2]

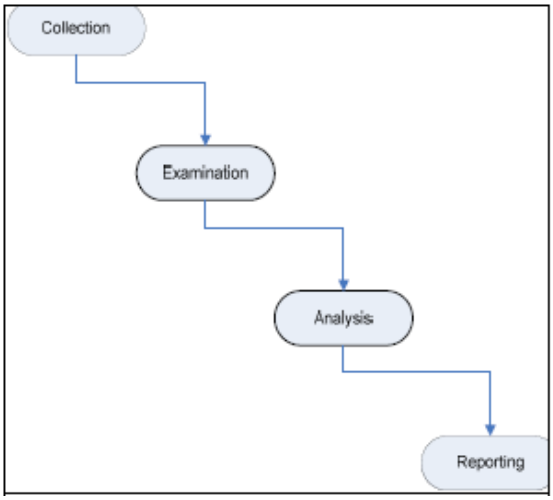
Prodi DIV Teknik Informatika Politeknik Harapan Bersama memiliki *website* yang saling berintegrasi dengan *website* Politeknik Harapan Bersama Tegal. Perlu adanya sistem kemananan yang baik agar data yang terdapat dalam website tidak bocor akibat serangan dari peretas.

Penelitian terdahulu tekait dengan keamanan halaman web antara lain, penelitian terkait forensic jaringan, yaitu melakukan eksperimen dasar forensic jaringan dengan menangkap lalulintas paket pada jaringan, menganalisa karakteristiknya dan mencoba untuk mengetahui aktivitas yang berbahaya dalam membantu mengidentifikasi sumber aktivitas yang ada dijaringan dengan menggunakan tools nmap, tcp-dump, tools tersebut terbukti ampuh untuk membantu dan menangkap serta menganalisa paket jaringan diantaranya sniffing dan port

scanning [3]. A. K. Kaushik melakukan forensic jaringan untuk serangan ICMP dengan cara mengusulkan model sistem forensic jaringan untuk ICMP dengan cara mengumpulkan data jaringan, mengidentifikasi paket yang mencurigakan, memeriksa protocol dan validasi serangan, untuk mengatasi masalah jumlah data yang besar, A. K. Kaushik hanya memeriksa informasi header dari paket ICMP, eksperimen dilakukan mengunakan nmap [4]. Halfond dan Orso menyajikan dan mengevaluasi Teknik baru untuk mendeteksi dan mencegah serangan SQL Injection, Halfond dan Orso juga mengembangkan alat AMNESIA (Analysis and Monitoring for Neutralizing SQL Injection Attacks) [5]. Pomeroy dan Tan, membahas mengenai tantangan rekaman jaringan dan manfaat penggunaannya dimasa yang akan datang. Perekaman yang dimaksud adalah untuk mendeteksi serta mengungkap serangan. SQL Injection merupakan salah satu serangan teratas selain XSS (Cross Site Scripting) dari tahun 2002 hingga tahun 2008 [6]. M. Nurkhamid, penelitian ini mempunyai manfaat untuk memberikan keefektifan sebuah jaringan intranet melalui bentuk topologi alternative yang diterapkan pada Universitas Muria kudus [7].

II. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini mengacu pada dua pendekatan, yaitu pendekatan forensik dan pendekatan studi Pustaka. Pendekatan forensic digunakan untuk menganalisa Teknik keamanan halaman web sedangkan pendekatan studi Pustaka digunakan sebagai referensi kajian dan teori dalam melakukan observasi penelitian. Metode dalam pelaksanaan penelitian ini dapat ditunjukkan pada diagram alir pendekatan forensik [8] pada Gambar 1.



Gambar 1. Diagram Alir Pendekatan Forensik

2.1 Metode Pendekatan Forensik

Tahapan-tahapan yang digunakan dalam proses forensic adalah :

1. Identifikasi (Collection)
   Tahap ini akan dilakukan identifikasi terhadap kebutuhan-kebutuhan, baik kebutuhan fungsional system maupun identifikasi kondisi dari halaman web Prodi DIV Teknik Informatika. Ditahap ini tim peneliti berhasil melakukan identifikasi kebutuhan alat dan bahan, serta data-data yang nanti dibutuhkan dalam penelitian ini.
2. Pengujian (Examination)
   Tahap ini mulai dilakukan pengujian terhadap keamanan dari halaman website Prodi DIV Teknik Informatika. Ditahap ini peneliti mulai melakukan scanning port

terhadap halaman web Prodi DIV Teknik Informatika. Scanning port disini dilakukan untuk melihat apakah peretas dapat melihat adanya port yang berpotensi sebagai port yang tidak aman atau vulnerable.

3. Analisa (Analisys)
   Tahap ini dilakukan Analisa terhadap hasil dari scanning terhadap port yang berpotensi memiliki celah keamanan. Dan juga berguna untuk menemukan kelemahan-kelemahann yang terdapat pada halaman web Prodi DIV Teknik Informatika. Dari hasil Analisa ini juga didapatkan solusi untuk pengembangan keamanan halaman web Prodi DIV Teknik Informatika.
4. Pelaporan (Reporting)
   Tahap pelaporan ini mulai dilakukan dokumentasi terhadap hasil penelitian berserta analisisnya

2. 2 Metode Pengumpulan Data

Pengumpulan data yang digunakan dalam penelitian ini dilakukan dengan cara:

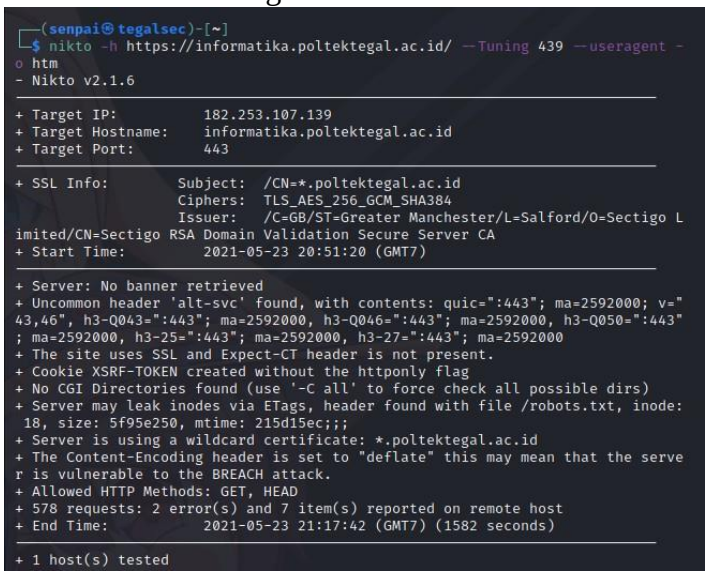
1. Library Research
   Dilakukan dengan cara mempelajari bahan-bahan tertulis berupa buku, browsing melalui internet terhadap masalah yang berkaitan dengan forensik
2. Interview dan Observasi
   Dilakukan dengan cara melakukan observasi secara virtual maupun non virtual, virtual dengan cara mengunjungi halaman web informatika.poltektegal.ac.id, sedangkan nonvirtual dilakukan dengan cara mengunjungi Unit Teknis Sistem Informasi (UPT SI) Politeknik Harapan Bersama Tegal.

III. HASIL DAN PEMBAHASAN

Pada tahap awal menggunakan nikto dengan hasil :

========== https://informatika.poltektegal.ac.id ==========

+ IP : 182.253.107.139
+ Hostname : informatika.poltektegal.ac.id
+ Port 443
+ SSL Info : Subject: /CN=*.poltektegal.ac.id
  Ciphers: TLS_AES_256_GCM_SHA384
  Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain Validation Secure Server CA



```
┌──(senpai㉿tegalsec)-[~]
└─$ nikto -h https://informatika.poltektegal.ac.id/ -Tuning 439 -useragent -
o htm
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          182.253.107.139
+ Target Hostname:    informatika.poltektegal.ac.id
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=*.poltektegal.ac.id
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo L
imited/CN=Sectigo RSA Domain Validation Secure Server CA
+ Start Time:         2021-05-23 20:51:20 (GMT7)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ Uncommon header 'alt-svc' found, with contents: quic=":443"; ma=2592000; v="
43,46", h3-Q043=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q050=":443"
; ma=2592000, h3-25=":443"; ma=2592000, h3-27=":443"; ma=2592000
+ The site uses SSL and Expect-CT header is not present.
+ Cookie XSRF-TOKEN created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /robots.txt, inode:
 18, size: 5f95e250, mtime: 215d15ec;;;
+ Server is using a wildcard certificate: *.poltektegal.ac.id
+ The Content-Encoding header is set to "deflate" this may mean that the serve
r is vulnerable to the BREACH attack.
+ Allowed HTTP Methods: GET, HEAD
+ 578 requests: 2 error(s) and 7 item(s) reported on remote host
+ End Time:           2021-05-23 21:17:42 (GMT7) (1582 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

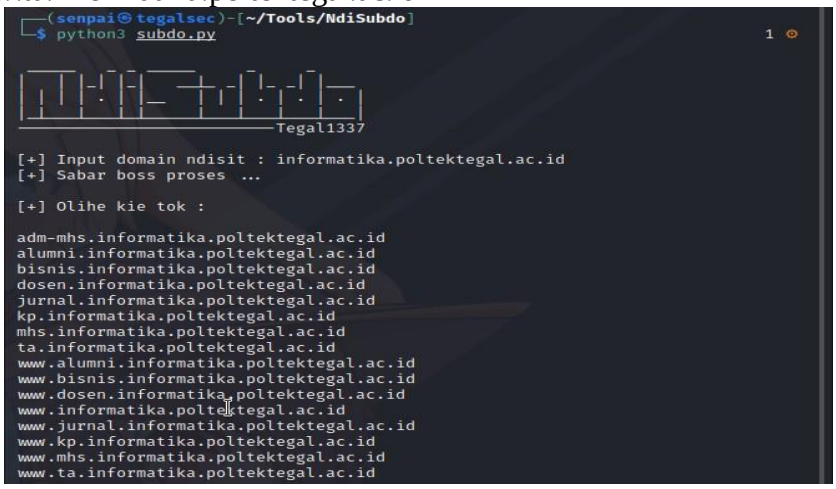
Gambar 2 Hasil Menggunakan Nikto

Setelah itu coba menganalisa lagi di https://informatika.poltektegal.ac.id
terdapat info : Informasi tentang server yang digunakan
+ Phpinfo: PHP Version 7.3.27
System: Linux cp1.poltektegal.ac.id 3.10.0-1160.25.1.el7.x86_64 #1 SMP Wed Apr 28 21:49:45 UTC 2021 x86_64
Server: LiteSpeed V7.8

Mendapatkan Informasi direktori yang terbuka
+ Open Directory: Server Dir Upload :
https://182.253.107.139/upload.html Server
Phpinfo : https://182.253.107.139/phpinfo.php
Host Login Page : https://informatika.poltektegal.ac.id/panel

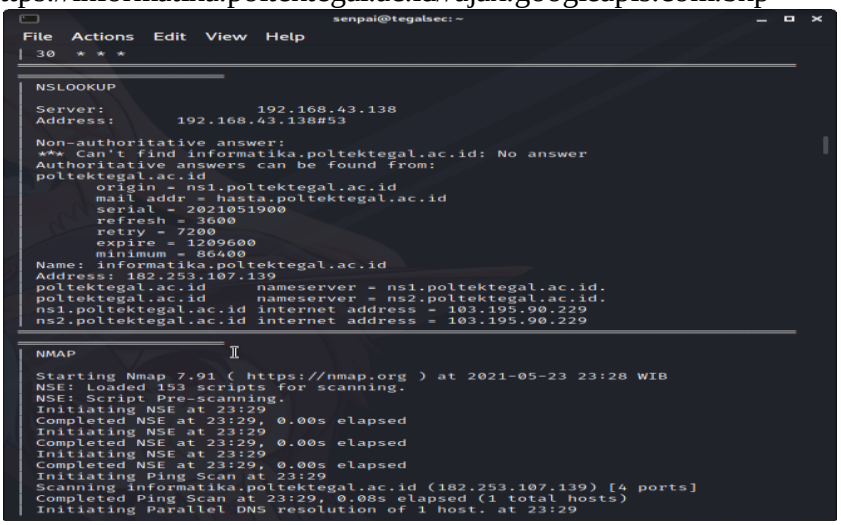
Mendapatkan Informasi file yang terbuka
+ Open Files: Config :
https://informatika.poltektegal.ac.id/web.config

Analisa selanjutnya pada subdomain :
+ Subdomain:
adm-mhs.informatika.poltektegal.ac.id
alumni.informatika.poltektegal.ac.id
bisnis.informatika.poltektegal.ac.id
dosen.informatika.poltektegal.ac.id
jurnal.informatika.poltektegal.ac.id
kp.informatika.poltektegal.ac.id
mhs.informatika.poltektegal.ac.id
ta.informatika.poltektegal.ac.id
www.alumni.informatika.poltektegal.ac.id
www.bisnis.informatika.poltektegal.ac.id
www.dosen.informatika.poltektegal.ac.id
www.informatika.poltektegal.ac.id
www.jurnal.informatika.poltektegal.ac.id
www.kp.informatika.poltektegal.ac.id
www.mhs.informatika.poltektegal.ac.id
www.ta.informatika.poltektegal.ac.id

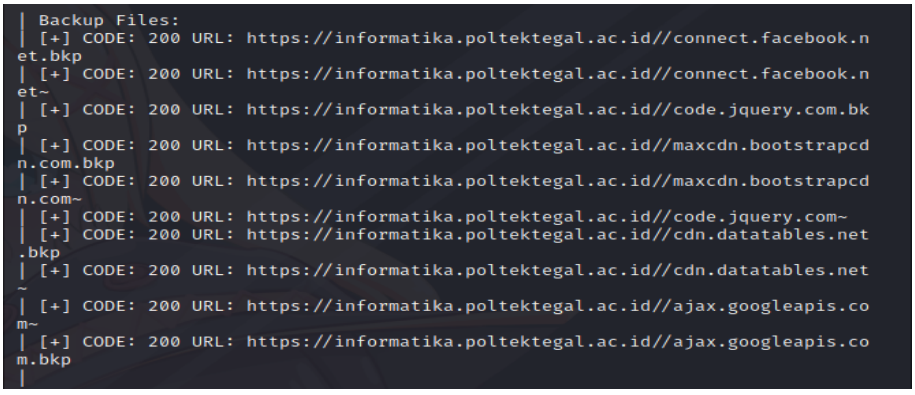


Gambar 3 Hasil Scanning SubDomain

Analisis selanjutnya dilakukan untuk mendapatkan informasi seperti :
+ NS Lookup:
    poltektegal.ac.id nameserver = ns2.poltektegal.ac.id.
    poltektegal.ac.id nameserver = ns1.poltektegal.ac.id.
    ns1.poltektegal.ac.id internet address = 103.195.90.229
    ns2.poltektegal.ac.id internet address = 103.195.90.229
+ Allowed HTTP Methods:
    GET HEAD POST OPTIONS
+ Email:
    informatika@poltektegal.ac.id
    laboratorium.informatika@poltektegal.ac.id
+ Backup:
    https://informatika.poltektegal.ac.id//connect.facebook.net.bkp
    https://informatika.poltektegal.ac.id//code.jquery.com.bkp
    https://informatika.poltektegal.ac.id//maxcdn.bootstrapcdn.com.bkp
    https://informatika.poltektegal.ac.id//cdn.datatables.net.bkp
    https://informatika.poltektegal.ac.id//ajax.googleapis.com.bkp



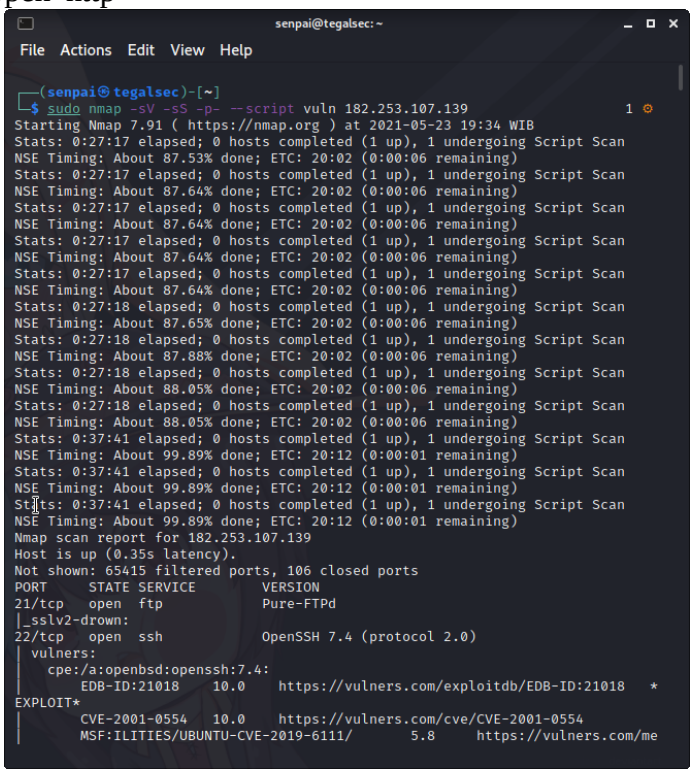
Gambar 4 NSLookup



Gambar 5 Hasil Nmap pencarian backup

Analisis selanjutnya dilakukan dengan melakukan scaning IP Port :
Scaning 65415 filtered port dan 106 closed port.
==========IP PORT==========

+ Open Port 21/tcp open ftp Pure-FTPd 80/tcp open http



```
┌──(senpai㉿tegalsec)-[~]
└─$ sudo nmap -sV -sS -p- --script vuln 182.253.107.139                  1 ⚙
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 19:34 WIB
Stats: 0:27:17 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 87.53% done; ETC: 20:02 (0:00:06 remaining)
Stats: 0:27:17 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 87.64% done; ETC: 20:02 (0:00:06 remaining)
Stats: 0:27:17 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 87.64% done; ETC: 20:02 (0:00:06 remaining)
Stats: 0:27:17 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 87.64% done; ETC: 20:02 (0:00:06 remaining)
Stats: 0:27:17 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 87.64% done; ETC: 20:02 (0:00:06 remaining)
Stats: 0:27:18 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 87.65% done; ETC: 20:02 (0:00:06 remaining)
Stats: 0:27:18 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 87.88% done; ETC: 20:02 (0:00:06 remaining)
Stats: 0:27:18 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 88.05% done; ETC: 20:02 (0:00:06 remaining)
Stats: 0:27:18 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 88.05% done; ETC: 20:02 (0:00:06 remaining)
Stats: 0:37:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.89% done; ETC: 20:12 (0:00:01 remaining)
Stats: 0:37:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.89% done; ETC: 20:12 (0:00:01 remaining)
Stats: 0:37:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.89% done; ETC: 20:12 (0:00:01 remaining)
Nmap scan report for 182.253.107.139
Host is up (0.35s latency).
Not shown: 65415 filtered ports, 106 closed ports
PORT     STATE SERVICE        VERSION
21/tcp   open  ftp            Pure-FTPd
|_sslv2-drown:
22/tcp   open  ssh            OpenSSH 7.4 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:7.4:
|       EDB-ID:21018    10.0    https://vulners.com/exploitdb/EDB-ID:21018   *
EXPLOIT*
|       CVE-2001-0554   10.0    https://vulners.com/cve/CVE-2001-0554
|       MSF:ILITIES/UBUNTU-CVE-2019-6111/       5.8     https://vulners.com/me
```

Gambar 6 Hasil Nmap untuk pencarian port

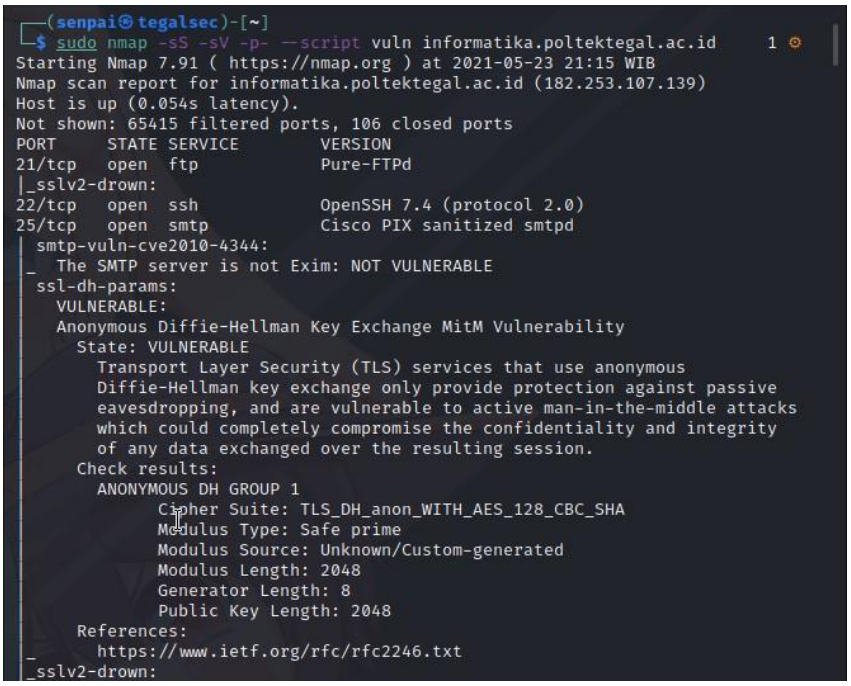
+ Vulnarable Port

```
22/tcp  open  ssh      OpenSSH 7.4 (protocol 2.0)
vulners:
cpe:/a:openbsd:openssh:7.4:
EDB-ID:21018       10.0    https://vulners.com/exploitdb/EDB-ID:21018
CVE-2001-0554      10.0    https://vulners.com/cve/CVE-2001-0554
EDB-ID:46516       5.8     https://vulners.com/exploitdb/EDB-ID:46516
CVE-2019-6111      5.8     https://vulners.com/cve/CVE-2019-6111
SSH_ENUM           5.0     https://vulners.com/canvas/SSH_ENUM
25/tcp  open  smtp          Cisco PIX sanitized smtpd
          smtp-vuln-cve2010-4344:
          The SMTP server is not Exim: NOT VULNERABLE
465/tcp  open  ssl/smtp          Postfix smtpd
          smtp-vuln-cve2010-4344:
          The SMTP server is not Exim: NOT VULNERABLE
587/tcp  open  smtp          Postfix smtpd
          smtp-vuln-cve2010-4344:
          The SMTP server is not Exim: NOT VULNERABLE
993/tcp  open  imaps?
            ssl-ccs-injection: No reply from server (TIMEOUT)
            sslv2-drown:
995/tcp  open  pop3s?
            ssl-ccs-injection: No reply from server (TIMEOUT)
            sslv2-drown:
3636/tcp open  ssl/http         LiteSpeed httpd
            http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
```

```
http-csrf:
Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=182.253.107.139
Found the following possible CSRF vulnerabilities: Path:
http://182.253.107.139:3636/
Form id: loginform Form
action: /
7080/tcp open ssl/http (PHP 5.6.36)
fingerprint-strings:
GetRequest: HTTP/1.0
302 Found
X-Powered-By: PHP/5.6.36
X-Frame-Options: SAMEORIGIN X-
XSS-Protection: 1;mode=block
Referrer-Policy: same-origin
X-Content-Type-Options: nosniff
Set-Cookie:
LSUI37FE0C43B84483E0=1e008246dfa713b961329a84cd88c141;
path=/; secure; HttpOnly http-
slowloris-check:
VULNERABLE:
Slowloris DOS attack
State: LIKELY VULNERABLE IDs:
CVE:CVE-2007-6750
```

Analisis selanjutnya melakukan scaning IP Port berikutnya :
Scaning 65415 filtered port dan 106 closed port.

```
======================HOST PORT=====================
+ Open Port 21/tcp open ftp Pure-FTPd
22/tcp open ssh OpenSSH 7.4 (protocol 2.0)
80/tcp open http
```



Gambar 7 Hasil Nmap untuk vulnerability

+ Vulnarable Port

25/tcp open smtp Cisco PIX sanitized smtpd
smtp-vuln-cve2010-4344:
The SMTP server is not Exim: NOT VULNERABLE
443/tcp open ssl/https
fingerprint-strings:
GetRequest:
HTTP/1.0 200 OK
Etag: "36a9-606c7506-cc2b7;;;"
Last-Modified: Tue, 06 Apr 2021 14:49:42 GMT
Content-Type: text/html
Content-Length: 13993
Accept-Ranges: bytes
http-slowloris-check:
VULNERABLE:
Slowloris DOS attack
State: LIKELY VULNERABLE
IDs: CVE:CVE-2007-6750
465/tcp open ssl/smtp Postfix smtpd
smtp-vuln-cve2010-4344:
The SMTP server is not Exim: NOT VULNERABLE
587/tcp open smtp Postfix smtpd
smtp-vuln-cve2010-4344:
The SMTP server is not Exim: NOT VULNERABLE
993/tcp open imaps?
ssl-ccs-injection: No reply from server (TIMEOUT)
sslv2-drown:
995/tcp open pop3s?
ssl-ccs-injection: No reply from server (TIMEOUT)

```
        sslv2-drown:
3636/tcp open  ssl/http          LiteSpeed httpd
        http-csrf:
                Spidering limited to: maxdepth=3; maxpagecount=20;
                withinhost=informatika.poltektegal.ac.id
                Found the following possible CSRF vulnerabilities:  Path:
                https://informatika.poltektegal.ac.id:3636/   Form id: loginform
                Form action: /

7080/tcp open  ssl/http          (PHP 5.6.36)
        fingerprint-strings:
                GetRequest:
                HTTP/1.0 302 Found
                X-Powered-By: PHP/5.6.36
                X-Frame-Options: SAMEORIGIN
                X-XSS-Protection: 1;mode=block
                Referrer-Policy: same-origin
                X-Content-Type-Options: nosniff
                Set-Cookie:
                LSUI37FE0C43B84483E0=cf25523a7f66de860fd7f492
                d188540a; path=/; secure;HttpOnly
        http-enum:
                /login.php: Possible admin folder
                http-slowloris-check:
                VULNERABLE:
                Slowloris DOS attack
        State: LIKELY VULNERABLE
        IDs:  CVE:CVE-2007-6750
```

Setelah melakukan analisis berdasarkan hasil CVE yang diperoleh, didapatkan tidak adanya celah keamanan kearah SSL, PHP.cgi dan kea rah DNS Server,tetapi terdapat celah keamanan kearah DOS (Denial Of Sevice), Exploit, Buffer Overflow. Artinya peretas bisa melakukan peretasan dengan menggunakan DOS, Exploit dan Buffer Overflow, selama celah keamanan tersebut tidak di antisipasi, halaman web Prodi DIV Teknik informatika masih sangat rentan untuk masuki peretas, apalagi halaman web Prodi DIV Teknik informatika masih satu induk dengan halaman web Politeknik Harapan Bersama, dimana di dalam halaman web Politeknik Harapan Bersama terdapat halaman web yang sangat-sangat krusial contohnya halaman system informasi akademik dan halaman keuangan.

VI. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan maka kesimpulan dari penelitian ini adalah, tidak adanya system yang benar-benar aman, sehingga aktifitas jaringan yang paling kecil harus bisa dipantau, pemantauanya dengan cara mengamati paket-paket yang berjalan didalam jaringan, diusahakan mematikan port-port yang tidak perlu, sysadmin juga harus mampu membaca script-script yang terindikasi bisa memanfaatkan celah keamanan.

Untuk perbaikan ke depan, peneliti mempunyai saran yang harus segera dilakukan yaitu lakukan pembaharuan untuk Operating System yang digunakan pada server, melakukan pembaharuan pada sisi webserver serta CGI, tutup halaman web yang sudah tidak digunakan.

Sysadmin sebaiknya dibekali dengan bahasa pemrograman sehingga dapat mengetahui script-script yang berbahaya bagi halaman web Prodi DIV Teknik Informatika, maupun halaman web Utama Politeknik Harapan Bersama.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada tim penelitiaan ini dan kepada UPT Sistem Informasi Politeknik Harapan Bersama karena sudah diijinkan untuk melakukan penetrating system ke halaman web Prodi DIV Teknik Informatika

DAFTAR PUSTAKA

X. YAO, B. SUN, Z. Yang, and J. CAO, "A New Method For Vulnerability Analysis And Application In Rural Dwellings," in *2019 13th Symposium on Piezoelectrcity, Acoustic Waves and Device Applications (SPAWDA)*, Jan. 2019, vol. 7, no. 1, pp. 1–4, doi: 10.1109/SPAWDA.2019.8681872.

K. Sicchio, "Hacking Choreography: Dance and Live Coding," *Comput. Music J.*, vol. 38, no. 1, pp. 31–39, Mar. 2014, doi: 10.1162/COMJ_a_00218.

A. Fadlil, I. Riadi, and S. Aji, "Development Of Computer Network Security Systems So That Network Forensic Analysis," *J. Ilmu Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, pp. 11–18, 2017.

A. K. Kaushik, "2010c - Network Forensic System for ICMP Attacks - 2010.pdf," vol. 2, no. 3, pp. 14–21, 2010.

W. G. J. Halfond and A. Orso, "AMNESIA: Analysis and monitoring for NEutralizing SQL-injection attacks," *20th IEEE/ACM Int. Conf. Autom. Softw. Eng. ASE 2005*, pp. 174–183, 2005, doi: 10.1145/1101908.1101935.

A. Pomeroy and Q. Tan, "Effective SQL injection attack reconstruction using network recording," *Proc. - 11th IEEE Int. Conf. Comput. Inf. Technol. CIT 2011*, pp. 552–556, 2011, doi: 10.1109/CIT.2011.103.

M. Nurkamid, "Analisa Keefektifan Jaringan Local Area Network (Intranet) Universitas Muria Kudus," *J. Sains dan Teknol.*, vol. 4, no. 2, pp. 143–150, 2011.

V. Baryamureeba and F. Tushabe, "The enhanced digital investigation process model," *Proc. Digit. Forensic Res. Conf. DFRWS 2004 USA*, pp. 1–9, 2004.