TUGAS KEAMANAN JARINGAN KOMPUTER

NAMA: SYAMSUDIN
NIM: 09011281320012

UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER

Scanning merupakan kegiatan yang bertujuan untuk mencari celah jalur penyusupan yang lebih spesifik lagi. Ada 3 macam tipe dari scanning, yaitu port scanning, network scanning dan vulnerability scanning.

Pertama penulis melakukan scanning untuk mendapatkan beberapa informasi seperti port yang dibuka dan service yang digunakan pada server PT. PUSRI, informasi yang didapat dengan melakukan nmap scan menggunakan command “nmap pusri.co.id” pada Ubuntu os pada pusri.co.id yaitu sebagai berikut:

```
sam@sam-SVE14131CVW:~$ nmap pusri.co.id

Starting Nmap 6.47 ( http://nmap.org ) at 2017-02-22 19:32 WIB
Nmap scan report for pusri.co.id (222.124.4.120)
Host is up (0.056s latency).
rDNS record for 222.124.4.120: 120.subnet222-124-4.astinet.telkom.net.id
Not shown: 996 closed ports
PORT    STATE    SERVICE
22/tcp open     ssh
25/tcp filtered smtp
53/tcp filtered domain
80/tcp open     http

Nmap done: 1 IP address (1 host up) scanned in 5.05 seconds
```

Kemudian penulis melakukan pencarian informasi lainnya menggunakan tools https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap, informasi yang didapat yaitu sebagai berikut:

Starting Nmap 6.00 (http://nmap.org) at 2017-02-14 09:23 EET
NSE: Loaded 17 scripts for scanning.
Initiating SYN Stealth Scan at 09:23
Scanning pusri.co.id (222.124.4.120) [100 ports]
Discovered open port 80/tcp on 222.124.4.120
Discovered open port 22/tcp on 222.124.4.120
Completed SYN Stealth Scan at 09:23, 1.63s elapsed (100 total ports)
Initiating Service scan at 09:23
Scanning 2 services on pusri.co.id (222.124.4.120)
Completed Service scan at 09:23, 6.54s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against pusri.co.id (222.124.4.120)
Retrying OS detection (try #2) against pusri.co.id (222.124.4.120)
Initiating Traceroute at 09:24
Completed Traceroute at 09:24, 0.26s elapsed
NSE: Script scanning 222.124.4.120.
[+] Nmap scan report for pusri.co.id (222.124.4.120)
Host is up (0.21s latency).
Not shown: 70 filtered ports, 28 closed ports
PORT   STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
80/tcp open http   Apache httpd 2.2.16 ((Debian))
Device type: general purpose|WAP|media device|webcam
Running (JUST GUESSING): Linux 2.6.X|3.X|2.4.X (95%), Netgear embedded (89%), Western Digital embedded (89%), AXIS Linux 2.6.X (88%), PheeNet embedded (88%)

OS CPE: cpe:/o:linux:kernel:2.6 cpe:/o:linux:kernel:3 cpe:/o:linux:kernel:2.4.20 cpe:/o:axis:linux:2.6 cpe:/h:pheenet:wap-854gp
Aggressive OS guesses: Linux 2.6.18 - 2.6.32 (95%), Linux 2.6.35 (95%), Linux 2.6.32 - 2.6.35 (94%), Linux 2.6.22 (93%), Linux 2.6.17 - 2.6.36 (93%), Linux 2.6.19 - 2.6.35 (93%), Linux 2.6.22 (SPARC) (92%), Linux 3.0 - 3.1 (91%), Linux 2.6.26 (91%), Linux 2.6.38 (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 3.164 days (since Sat Feb 11 05:27:36 2017)
Network Distance: 8 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel
TRACEROUTE (using port 3306/tcp)
HOP RTT ADDRESS
1 0.58 ms router1-lon.linode.com (212.111.33.229)
2 1.26 ms 109.74.207.10
3 0.62 ms 109.74.207.9
4 31.84 ms 195.66.226.8
5 213.58 ms 180.240.192.137
6 213.66 ms 97.subnet222-124-4.astinet.telkom.net.id (222.124.4.97)
7 213.63 ms 97.subnet222-124-4.astinet.telkom.net.id (222.124.4.97)
8 213.70 ms 120.subnet222-124-4.astinet.telkom.net.id (222.124.4.120)
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 19.46 seconds
Raw packets sent: 157 (11.294KB) | Rcvd: 248 (21.769KB)

Dari informasi diatas diketahui bahwa port yang dibuka hanya pada port 22 dan 80 yang mana merupakan port layanan ssh dan port http sedangkan port yang lainnya di filter seperti port 25 dan 53, sedangkan port lainnya di tutup.

Selanjutnya penulis melakukan melakukan pencarian informasi operating system history dari server PT. PUSRI menggunakan tools http://toolbar.netcraft.com/site_report?url=http://www.pusri.co.id, dan mendapatkan hasil sebagai berikut:

Background

Site title	PT Pupuk Sriwidjaja Palembang (Pusri) | Home	**Date first seen**	February 1997
Site rank		**Primary language**	Indonesian
Description	PT Pupuk Sriwidjaja Palembang (Pusri) adalah Badan Usaha Milik Negara yang didirikan sebagai pelopor produsen pupuk urea di Indonesia		
Keywords	Pupuk, Urea, Pupuk Subsidi, Pupuk Non Subsidi, Amoniak		

Network

Site	http://pusri.co.id	**Netblock Owner**	PT MULTI DATA PALEMBANG
Domain	pusri.co.id	**Nameserver**	ns1.pusri.org
IP address	222.124.4.120	**DNS admin**	root@pusri.co.id
IPv6 address	*Not Present*	**Reverse DNS**	120.subnet222-124-4.astinet.telkom.net.id
Domain registrar	pandi.or.id	**Nameserver organisation**	whois.pir.org
Organisation	PT. Pupuk Sriwidjaja Palembang, Jl. Mayor Zen Sei-Selayur, Palembang, 30118, Indonesia	**Hosting company**	PT Telekomunikasi Indonesia Tbk
Top Level Domain	Indonesia (.co.id)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.4.120	Linux	Apache/2.2.16 Debian	13-Feb-2017
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	-	Apache/2.2.4 Unix DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e PHP/5.2.5 mod_apreq2-20051231/2.5.7 mod_perl/2.0.2 Perl/v5.8.7	25-Mar-2009
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	Linux	unknown	24-Mar-2009
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	Linux	Apache/2.2.4 Unix DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e PHP/5.2.5 mod_apreq2-20051231/2.5.7 mod_perl/2.0.2 Perl/v5.8.7	22-Mar-2009
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	Linux	Apache/2.2.4 Unix DAV/2 mod_ssl/2.2.4 OpenSSL/0.9.8d PHP/5.2.1 mod_apreq2-20051231/2.5.7 mod_perl/2.0.2 Perl/v5.8.7	3-Oct-2007
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	Linux	Apache/2.2.0 Unix DAV/2 mod_ssl/2.2.0 OpenSSL/0.9.8a PHP/5.1.2 mod_apreq2-20050712/2.1.3-dev mod_perl/2.0.2 Perl/v5.8.7	12-Mar-2007
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.120	Linux	Apache	4-Jun-2006
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.120	Linux	Apache/2.0.54	17-Sep-2005
PT. IndoInternet Cyber Building, 8th Flr Jl. Kuningan Barat no 8 Jakarta 12710	202.159.31.240	-	Apache/2.0.52 Unix mod_perl/1.99_17 Perl/v5.8.4 mod_ssl/2.0.52 OpenSSL/0.9.7d PHP/4.3.10	4-Mar-2005
PT. IndoInternet Cyber Building, 8th Flr Jl. Kuningan Barat no 8 Jakarta 12710	202.159.31.240	Linux	Apache/1.3.28 Unix PHP/4.3.2 mod_gzip/1.3.19.1a mod_fastcgi/2.2.12 mod_perl/1.27	9-May-2004

Dari informasi yang didapat dari netcraft.net diatas hosting history terbaru yaitu pada tanggal 13 Februari 2017 PUSRI menggunakan web server Apache/2.2.16.

Dari data atau informasi yang didapat dari scanning yang telah dilakukan selanjutnya penulis mencari CVE (Common Vulnerabilities and Exposures) yang ada di server PT. PUSRI tersebut menggunakan tools CVE Checker dari http://cve.mitre.org/

Apache/2.2.16

CVE-2016-4979 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4979

The Apache HTTP Server 2.4.18 through 2.4.20, when mod_http2 and mod_ssl are enabled, does not properly recognize the "SSLVerifyClient require" directive for HTTP/2 request authorization, which allows remote attackers to bypass intended access restrictions by leveraging the ability to send multiple requests over a single connection and aborting a renegotiation.

Berdasarkan CVE-2016-4979 diketahui bahwa terdapat celah ketika mod_http2 dan mod_ssl diaktifkan yang dapat memungkinkan remote attackers untuk melakukan pembatasan akses dengan memanfaatkan leveraging ability untuk mengirimkan bberapa request single connection dan aborting renegotiation.

CVE-2016-8740 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8740

The mod_http2 module in the Apache HTTP Server 2.4.17 through 2.4.23, when the Protocols configuration includes h2 or h2c, does not restrict request-header length, which allows remote attackers to cause a denial of service (memory consumption) via crafted CONTINUATION frames in an HTTP/2 request.

Berdasarkan CVE-2016-8740 diketahui bahwa terdapat celah ketika konfigurasi Protokol termasuk h2 atau H2C tidak membatasi panjang permintaan-header dapat memungkinkan remote attackers untuk melakukan denial of service atau penolokan layanan melalui frame CONTINUATION.

CVE-2010-2068 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2068

mod_proxy_http.c in mod_proxy_http in the Apache HTTP Server 2.2.9 through 2.2.15, 2.3.4-alpha, and 2.3.5-alpha on Windows, NetWare, and OS/2, in certain configurations involving proxy worker

pools, does not properly detect timeouts, which allows remote attackers to obtain a potentially sensitive response intended for a different client in opportunistic circumstances via a normal HTTP request.

Berdasarkan CVE-2010-2068 diketahui bahwa terdapat celah dalam konfigurasi tertentu yang melibatkan proxy worker pools yang tidak benar dalam mendeteksi timeout yang memungkinkan remote attackers mendapatkan respon yang berpotensi sensitif yang ditunjukkan untuk client yang berbeda melalui normal request HTTP.

OpenSSH 5.5p1

CVE-2016-8858 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8858

** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."

Berdasarkan CVE-2016-8858 diketahui bahwa terdapat celah yang memungkinkan remote attackers untuk melakukan denial of service atau penolakan layanan dengan cara mengirimkan banyak request KEXINIT. Status dari CVE ini sendiri masih DISPUTED atau diperdebatkan.

CVE-2016-10010 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10010

sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.

Berdasarkan CVE-2016-10010 diketahui bahwa terdapat celah ketika pemisahan hak akses tidak digunakan yang mengakibatkan diteruskannya soket Unix-domain sebagai root yang memungkinkan user lokal untuk mendapatkan akses melalui vektor yang ditentukan terkait dengan serverloop.c.

CVE-2016-6210 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6210

sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.

Berdasarkan CVE-2016-6210 diketahui bahwa terdapat celah ketika SHA256 atau SHA512 digunakan untuk melakukan hashing user password menggunakan blowfish hasing pada password statis ketika nama pengguna tidak tersedia yang memungkinkan remote attackers untuk menghitung jumlah pengguna dengan memanfaatkan perbedaan waktu antara respon ketika large password diberikan.

Apache httpd 2.2.16

CVE-2016-8740 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8740

The mod_http2 module in the Apache HTTP Server 2.4.17 through 2.4.23, when the Protocols configuration includes h2 or h2c, does not restrict request-header length, which allows remote attackers to cause a denial of service (memory consumption) via crafted CONTINUATION frames in an HTTP/2 request.

Berdasarkan CVE-2016-8740 diketahui bahwa terdapat celah ketika konfigurasi protokol termasuk h2 atau h2c yang tidak membatasi panjang permintaan header yang memungkinkan remote attackers untuk melakukan deniel of service atau penolakan layanan melalui frame CONTINUATION.