MANAJEMEN KEAMANAN INFORMASI

LAPORAN ANALISIS WEBSITE PADA METROTVNEWS.COM DAN BKN.GO.ID

OLEH

Nama	**:**	**Dini Ayu Lestari**
NIM	**:**	**09031181520005**
Kelas	**:**	**SI Regular 6A**

Dosen Pembimbing : Deris Stiawan, M.T., Ph.D.

JURUSAN SISTEM INFORMASI

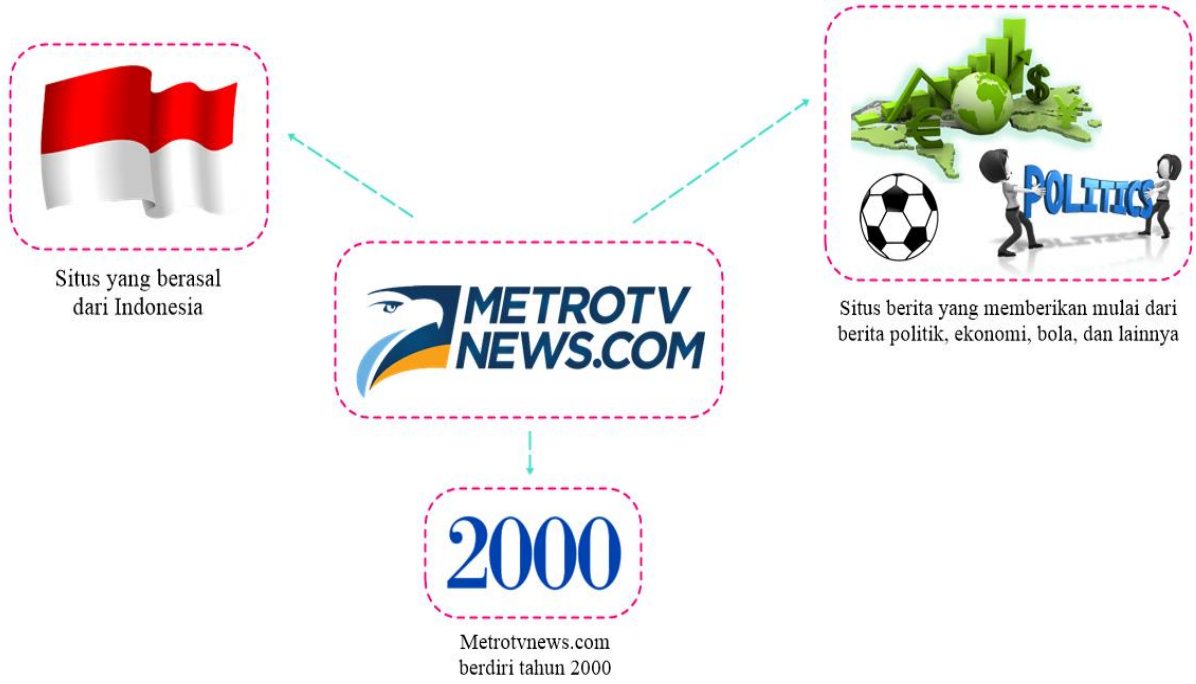
FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

~~~~~~~~~~~~~~~~~~~~ **Metrotvnews.com** ~~~~~~~~~~~~~~~~~~~~

A. Data Collection



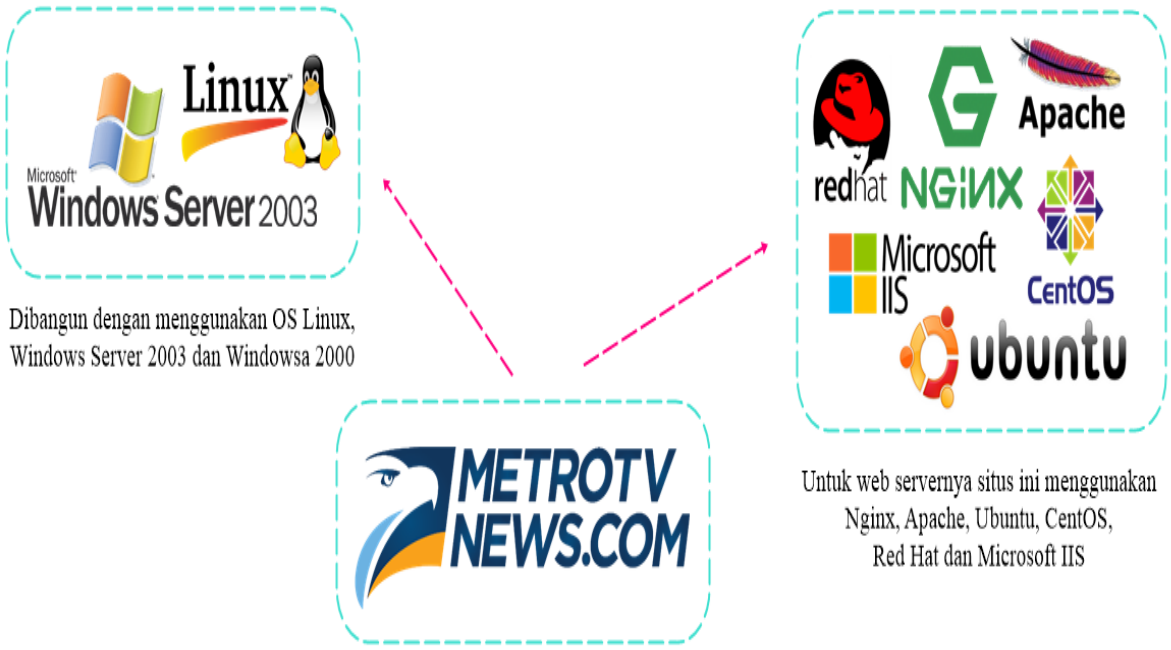
Gambar 1. Penjelasan Metrotvnews.com Secara Umum

Metrotvnews.com merupakan salah satu situs berita yang berasal dari Indonesia. Situs ini berdiri pada mei tahun 2000. Metrotvnews.com ini adalah situs yang berfokus pada pemberitaan mengenai situasi politik, video, ekonomi, bola, hobi dan lainnya. Situs ini berada pada peringkat 183.005 . Metrotvnews.com berkantor pusat di DKI Jakarta tepatnya di Jakarta Barat.

Berikut adalah tabel yang memuat informasi lebih detail mengenai situs atau website dari Metrotvnews.com :

1.	**Site**	http://www.metrotvnews.com
2.	**Domain**	metrotvnews.com
3.	**IP address**	103.225.66.90
4.	**Domain registrar**	tucows.com
5.	**Netblock owner**	PT. Media Televisi Indonesia
6.	**Name server**	ns1.metrotvnews.com
7.	**DNS admin**	sysadmin@metrotvnews.com
8.	**Reverse DNS**	ip66-90.metrotvnews.com

Tabel 1. Informasi Detail Situs Metrotvnews.com
~~~~~~~~~~~~~~~~~~~~



Gambar 2. Sistem Operasi dan Web Server Metrotvnews.com

Situs Metrotvnews.com dibangun dengan menggunakan tiga **sistem operasi** yaitu Windows 2000, Windows Server 2003 dan Linux. Untuk **web servernya** situs ini menggunakan Microsoft IIS, Apache, CentOS, Red Hat, Ubuntu dan Nginx. Berikut adalah hosting – hosting yang pernah dilakukan oleh Metrotvnews.com :

No.	Netblock owner	IP address	OS	Web server	Last seen
1.	PT Media Televisi Indonesia Corporate / Direct Member IDNIC Jl. Pilar Mas Raya Kav.A-D Kedoya Kebon Jeruk, Jakarta 11015.	103.225.66.90	Linux	nginx	6-Mar-2018
2.	PT Media Televisi Indonesia Corporate / Direct Member IDNIC Jl. Pilar Mas Raya Kav.A-D Kedoya Kebon Jeruk, Jakarta 11015.	103.225.66.90	Linux	nginx/1.6.0	26-Oct-2014
3.	PT Media Televisi Indonesia Corporate / Direct Member IDNIC Jl. Pilar Mas Raya Kav.A-D Kedoya Kebon Jeruk, Jakarta 11015.	103.225.66.90	Linux	nginx/1.2.6 Ubuntu	15-Jul-2014

4.	Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.22	Linux	Apache/2.2.15 CentOS	12-Feb-2014
5.	Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.22	Linux	Apache/2.2.3 CentOS	7-Mar-2012
6.	Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.22	Linux	Apache/2.2.3 Red Hat	30-Jul-2011
7.	Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.22	Linux	Apache/2.2.3 CentOS	2-May-2009
8.	Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.22	Windows Server 2003	Microsoft-IIS/6.0	25-Jul-2008
9.	Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.158	Windows Server 2003	Microsoft-IIS/6.0	27-Jun-2005
10.	Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.158	Windows 2000	Microsoft-IIS/5.0	21-Apr-2005

Tabel 2. Hosting History dari Metrotvnews.com

Pada aplikasi **Nmap**, situs Metrotvnews.com ini memiliki 1 port yang terbuka yaitu :
Discovered open port 53/tcp on 103.225.66.90

B. Vulnerability Assessment

Vulnerability assessment adalah suatu langkah untuk mendeteksi, mengidentifikasi dan mempelajari kelemahan yang dimiliki dari suatu sistem atau infrastruktur yang berbasis teknologi informasi.

Berikut adalah kelemahan atau hole yang teridentifikasi dari **web server yang pertama** kali digunakan oleh metrotvnews.com yaitu :

Web Server	Kelemahan
Microsoft IIS	• **CVE-2005-2089** : Baik versi **5.0** ataupun **6.0** memungkinkan penyerang jarak jauh meracuni cache web, melewati perlindungan firewall aplikasi web dan melakukan serangan XSS melalui permintaan HTTP dengan header “Transfers-Encoding: chunked” dan header Content-Length. • **CVE-2006-0026** : Adanya buffer overflow di Microsoft IIS **5.0** dan **6.0** yang memungkinkan hacker lokal maupun jarak jauh untuk mengeksekusi kode dengan sewenang – wenang melalui Active Server Pages (ASP) yang dibuat. • **CVE-2009-3023** : Adanya buffer overflow di Microsoft IIS **5.0** dan **6.0** yang memungkinkan hacker lokal maupun jarak jauh untuk mengeksekusi kode dengan sewenang – wenang melalui perintah NLIST (Name List) yang dibuat menggunakan wildcard dimanan menyebabkan korupsi memori atau “IIS FTP Service RCE and DoS Vulnerability”.

Tabel 3. Beberapa Kelemahan dari Microsoft IIS 5.0 dan 6.0

Berikutnya adalah beberapa hole ataupun kelemahan dari **web server terbaru** yang digunakan oleh metrotvnews.com pada 6 maret 2018 yaitu Nginx :

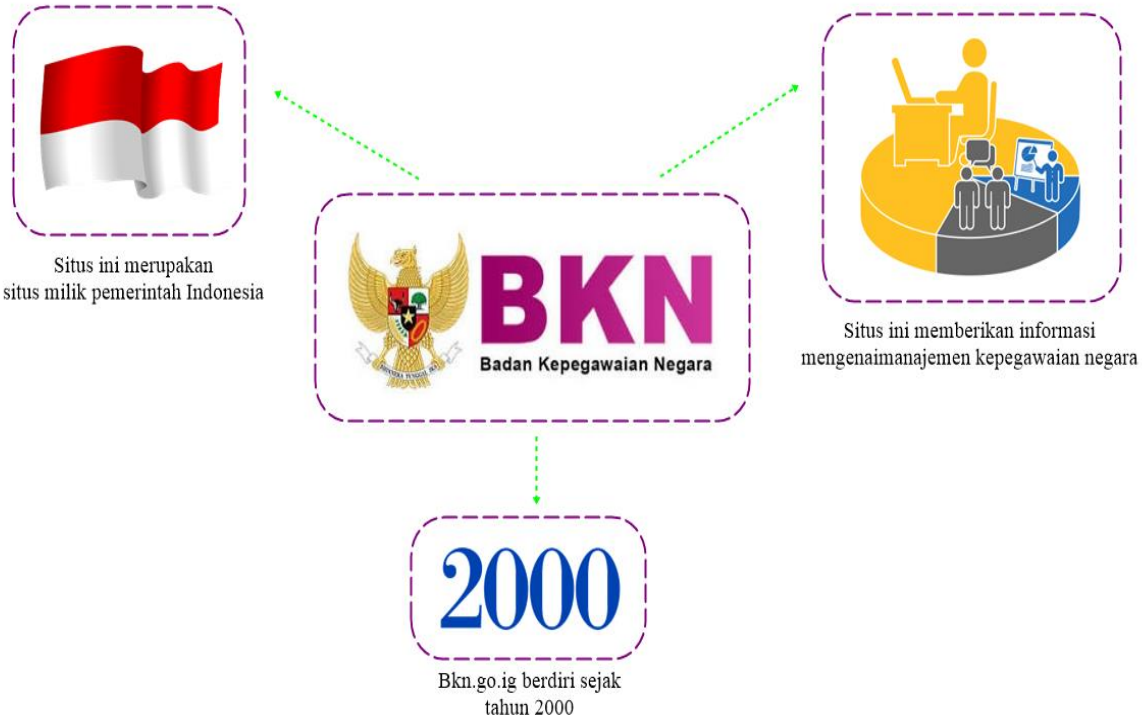
Web Server	Kelemahan
NGINX	• **CVE-2016-1247 :** Paket nginx sebelum 1.6.2-5 + deb8u3 pada Debian jessie, paket nginx sebelum 1.4.6-1ubuntu3.6 di Ubuntu 14.04 LTS, sebelum 1.10.0-0ubuntu0.16.04.3 di Ubuntu 16.04 LTS, dan sebelum 1.10. 1-0ubuntu1.1 di Ubuntu 16.10, dan ebuild nginx sebelum 1.10.2-r3 di Gentoo memungkinkan pengguna lokal mengakses akun pengguna server web untuk mendapatkan hak istimewa root melalui serangan symlink pada log kesalahan. • **CVE-2016-0746 :** Sebelum nginx 1.8.1 dan 1.9.x sebelum 1.9.1 memungkinkan penyerangan jarak

	jauh menyebabkan penolakan layanan atau mungkin memiliki dampak lain yang tidak ditentukan melalui respon DNS yang dibuat terkait dengan proses respons CNAME.

Tabel 4. Beberapa Kelemahan dari Nginx

~~~~~~~~~~~~~~~~~~~~ **Bkn.go.id** ~~~~~~~~~~~~~~~~~~~~

A. Data Collection



Gambar 3. Penjelasan Bkn.go.id Secara Umum

Bkn.go.id adalah salah satu situs milik pemerintah Indonesia yang didirikan pada bulan Juni tahun 2000. Situs ini berfungsi untuk memberikan informasi – informasi mengenai kepegawaian negara mulai layanan mutasi kepegawaian, syarat – syarat administrasi kepegawaian dan lainnya.

Berikut adalah tabel yang memuat informasi lebih detail mengenai situs atau website dari Metrotvnews.com :

1.	**Site**	http://www.bkn.go.id
2.	**Domain**	bkn.go.id
3.	**IP address**	180.250.80.39
4.	**Top level domain**	Indonesia (.go.id)
5.	**Netblock owner**	PT TELKOM INDONESIA
6.	**Name server**	ns1.telkomhosting.com
7.	**DNS admin**	hostmaster@telkom.net.id
8.	**Name server organisation**	whois.onlinenic.com

Tabel 5. Informasi Detail Situs Bkn.go.id
~~~~~~~~~~~~~~~~~~~~

Gambar 4. Sistem Operasi dan Web Server Bkn.go.id

Gambar diatas menunjukkan bahwa situs Bkn.go.id menggunakan sistem operasi Linux, Windows server 2003 dan Windows 2000 sedangkan untuk web servernya bkn.go.id menggunakan Apache, Ubuntu, Nginx dan Redhat. Berikut adalah hosting – hosting yang pernah dilakukan oleh Bkn.go.id :

Netblock owner	IP address	OS	Web server	Last seen Refresh
PT Infinys System Indonesia Indonesia Stock Exchange Building Suite 1601B	103.43.44.178	Linux	nginx/1.4.6 Ubuntu	18-Jan-2017
PT Infinys System Indonesia Indonesia Stock Exchange Building Suite 1601B	103.43.44.178	Linux	Apache/2.4.7 Ubuntu	5-Apr-2016
PT Infinys System Indonesia Corporate / Direct Member IDNIC Office 88Kasablanka Tower A, unit 7H Jl Kasablanka Raya Kav. 88 Jakarta 12870, Indonesia	103.23.20.239	Linux	Apache	2-Sep-2015
PT Telkom Indonesias customer.	118.97.48.2	Linux	Apache/2.2.3 Red Hat	27-May-2014
PT Telkom Indonesias customer.	118.97.48.2	Windows Server 2003	Apache/2.2.11 Win32 DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i mod_autoindex_color PHP/5.2.8	4-Mar-2010
PT Telekomunikasi Indonesia Menara Multimedia Lt. 7 Jl. Kebon Sirih No. 12 JAKARTA - 10340	118.97.48.2	Windows Server 2003	Apache/2.0.55 Win32 PHP/4.4.2	29-Oct-2008
Excelcomindo Pratama, PT. Internet Service Provider	202.152.239.70	Windows Server 2003	Apache/2.0.49 Win32 PHP/4.3.6	29-Jan-2007
LAN Badan Kepegawaian Nasional Jakarta	202.152.28.200	unknown	Apache/2.0.49 Win32 PHP/4.3.6	24-Jun-2006

LAN Badan Kepegawaian Nasional Jakarta	202.152.28.200	Windows Server 2003	Apache/2.0.49 Win32 PHP/4.3.6	2-Jun-2006
LAN Badan Kepegawaian Nasional Jakarta	202.152.28.200	Windows 2000	Apache/2.0.49 Win32 PHP/4.3.6	10-Aug-2005

Gambar 5. Hosting History dari Bkn.go.id

Pada aplikasi **Nmap**, situs Bkn.go.id ini memiliki 1 port yang terbuka yaitu : **Discovered open port 53/tcp on 180.250.80.39** .

B. Vulnerability Assessment

Vulnerability assessment adalah suatu langkah untuk mendeteksi, mengidentifikasi dan mempelajari kelemahan yang dimiliki dari suatu sistem atau infrastruktur yang berbasis teknologi informasi.

Berikutnya adalah beberapa hole ataupun **kelemahan** dari **web server terakhir** yang digunakan oleh Bkn.go.id pada 18 Januari 2017 yaitu Nginx/1.4.6 Ubuntu :

Web Server	Kelemahan
NGINX	• **CVE-2016-0746 :** Sebelum nginx 1.8.1 dan 1.9.x sebelum 1.9.1 memungkinkan penyerangan jarak jauh menyebabkan penolakan layanan atau mungkin memiliki dampak lain yang tidak ditentukan melalui respon DNS yang dibuat terkait dengan proses respons CNAME. • **CVE-2009-2629 :** Adanya buffer overflow memungkinkan penyerang jarak jauh untuk mengeksekusi sewenang-wenang kode melalui permintaan HTTP dibuat. • **CVE-2016-0742 :** Sebelum nginx 1.8.1 dan 1.9.x sebelum 1.9.1 memungkinkan penyerangan jarak jauh menyebabkan penolakan layanan melalui respon UDP DNS yang dibuat. • **CVE-2016-4450 :** Sebelum nginx 1.10.1 dan 1.11.x sebelum 1.11.1 memungkinkan penyerang jarak jauh menyebabkan penolakan layan melalui permintaan yang dibuat, yang melibatkan penulisan permintaan klien ke file sementara.

Tabel 6. Beberapa Kelemahan dari Nginx/1.4.6 Ubuntu