

Tugas Keamanan Jaringan Komputer
Common Vulnerabilities and Exposures



Nama : Wahyuni Oktarina
NIM : 09011181419027
Kelas : SK8 PIL
Dosen Pembimbing : Deris Stiawan, M.T., Ph.D

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

LINUX

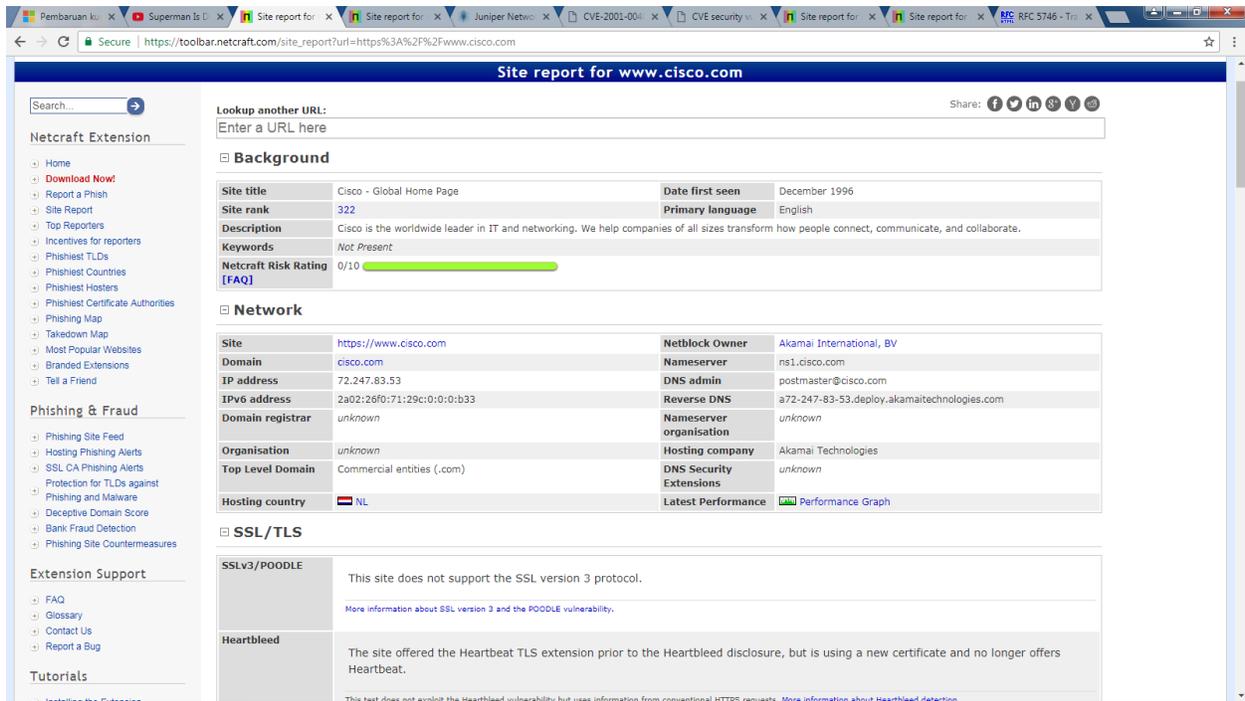
Linux adalah nama dari sebuah sistem operasi yang berbasis Unix yang disebarluaskan ke masyarakat secara gratis dan berada di bawah lisensi GNU General Public License (GPL), yang berarti bahwa Linux didistribusikan berikut dengan source code-nya. Ketersediaan akses kode sumber memungkinkan para pengguna untuk memodifikasi sistem operasi ini yang kemudian diperbolehkan juga untuk digunakan dan didistribusikan kembali secara bebas. Nama Linux sendiri diambil dari nama si penciptanya yaitu Linus Torvalds, untuk lebih jauh tentang sejarah Linux akan kami bahas pada artikel berikutnya. Yang menjadi perbedaan paling utama antara sistem operasi Linux dengan sistem operasi populer lainnya adalah terletak pada kernel Linux dan komponen-komponen yang menyusunnya yang bisa diakses secara bebas dan terbuka. Namun perlu pembaca ketahui, linux bukanlah satu-satunya sistem operasi yang berada pada kategori open source, masih terdapat beberapa sistem operasi lain yang bersifat sama dengan Linux. Akan tetapi Linux menjadi contoh terbaik dan sistem operasi open source yang paling banyak digunakan.

Pengembangan sistem operasi Linux dilakukan dengan cara mendistribusikannya secara bebas sehingga setiap calon pengguna dapat mendownload sistem operasi ini di internet atau mendapatkannya dari forum-forum khusus. Forum pengguna Linux biasanya membentuk sebuah komunitas khusus untuk memodifikasi sistem, setelah itu kode sumber yang telah dimodifikasi dan dikembangkan tersebut kembali dibagikan melalui internet atau media lainnya. Siapapun bebas untuk bergabung dengan komunitas dalam pengembangan sistem operasi Linux.

Apache adalah sebuah nama web server yang bertanggung jawab pada request-response HTTP dan logging informasi secara detail(kegunaan basicnya). Selain itu, Apache juga diartikan sebagai suatu web server yang kompak, modular, mengikuti standar protokol HTTP, dan tentu saja sangat digemari. Kesimpulan ini bisa didapatkan dari jumlah pengguna yang jauh melebihi para pesaingnya.

Apache memiliki fitur-fitur canggih seperti pesan kesalahan yang dapat dikonfigur, autentikasi berbasis basis data dan lain-lain. Apache juga didukung oleh sejumlah antarmuka pengguna berbasis grafik (GUI) yang memungkinkan penanganan server menjadi mudah. Apache merupakan perangkat lunak sumber terbuka dikembangkan oleh komunitas terbuka yang terdiri dari pengembang-pengembang dibawah naungan Apache Software Foundation.

Dari pembahasan diatas, saya mengambil contoh website : <https://www.cisco.com> yang menggunakan LINUX sebagai OS dan web servernya :Apache, saya mendapatkan info melalui website www.netcraft.com .



The screenshot shows a web browser displaying a Netcraft site report for <https://www.cisco.com>. The page is titled "Site report for www.cisco.com" and includes a search bar, a "Look up another URL" field, and a "Share" button. The report is organized into several sections:

- Background:** A table with fields: Site title (Cisco - Global Home Page), Date first seen (December 1996), Site rank (322), Primary language (English), Description (Cisco is the worldwide leader in IT and networking...), Keywords (Not Present), and Netcraft Risk Rating (0/10).
- Network:** A table with fields: Site (<https://www.cisco.com>), Netblock Owner (Akamai International, BV), Domain (cisco.com), Nameserver (ns1.cisco.com), IP address (72.247.83.53), DNS admin (postmaster@cisco.com), IPv6 address (2a02:26f0:71:29c:0:0:0:b33), Reverse DNS (a72-247-83-53.deploy.akamaitechnologies.com), Domain registrar (unknown), Nameserver organisation (unknown), Organisation (unknown), Hosting company (Akamai Technologies), Top Level Domain (Commercial entities (.com)), DNS Security Extensions (unknown), Hosting country (NL), and Latest Performance (Performance Graph).
- SSL/TLS:** A section titled "SSLV3/POODLE" stating "This site does not support the SSL version 3 protocol." with a link for more information. A "Heartbleed" section states "The site offered the Heartbeat TLS extension prior to the Heartbleed disclosure, but is using a new certificate and no longer offers Heartbeat." with a link for more information.

The left sidebar contains navigation links for "Netcraft Extension", "Phishing & Fraud", "Extension Support", and "Tutorials".

Secure | https://toolbar.netcraft.com/site_report?url=https%3A%2F%2Fwww.cisco.com

Certificate transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
No SCTs received or issuer unknown			

SSL Certificate Chain

Common name	Organisation	Organisational unit	Validity period
QuoVadis Root CA 2	QuoVadis Limited	Not Present	From 2006-11-24 to 2031-11-24
↓			
HydrantID SSL ICA G2	HydrantID (Avalanche Cloud Corporation)	Not Present	From 2013-12-17 to 2023-12-17

Hosting History

Netblock owner	IP address	OS	Web server	Last seen	Refresh
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.43.72.134	Linux	Apache	16-Feb-2018	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.71.248	Linux	Apache	26-Jan-2018	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.179.236	Linux	Apache	19-Jan-2018	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.118.211	Linux	Apache	11-Jan-2018	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.232.139	Linux	Apache	3-Jan-2018	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.71.248	unknown	Apache	27-Dec-2017	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.118.211	Linux	Apache	14-Dec-2017	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.232.139	Linux	Apache	20-Nov-2017	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.118.211	Linux	Apache	6-Nov-2017	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.232.139	Linux	Apache	8-Oct-2017	

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see opendsa.org.

Warning: It appears that this host does not have an SPF record. Setting up an SPF record helps prevent the delivery of forged emails from your domain.

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see dmarc.org.

https://toolbar.netcraft.com/netblock?q=AIBV10482176010482179255

Berdasarkan info yang didapat dari penjelasan diatas IP yang digunakan oleh pertamina.com ialah 23.43.72.134 untuk yang terakhir di update pada tanggal 16-Februari-2018. Untuk mencari celah keamanan nya menggunakan CVE yaitu Common Vulnerabilities and Exposures

CVE adalah kamus cyber security yang diketahui untuk kerentanan umum. Tujuan: Mengidentifikasi dan memberi nama secara terbuka kepada umum kerentanan yang berkaitan dengan versi perangkat lunak tertentu atau code bases.

Vulnerability Details : CVE-2001-0040

APC UPS daemon, apcupsd, saves its process ID in a world-writable file, which allows local users to kill an arbitrary process by specifying the target process ID in the apcupsd.pid file.
Publish Date : 2001-02-16 Last Update Date : 2017-10-09

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

- CVSS Scores & Vulnerability Types

CVSS Score	2.1
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	CWE id is not defined for this vulnerability

- Products Affected By CVE-2001-0040