TugasKeamananJaringanKomputer

Common Vulnerabilities and Exposures

Nama		**WahyuniOktarina**
NIM	**:**	**09011181419027**
Kelas	**:**	**SK8 PIL**
DosenPembimbing	**:**	**DerisStiawan, M.T., Ph.D**

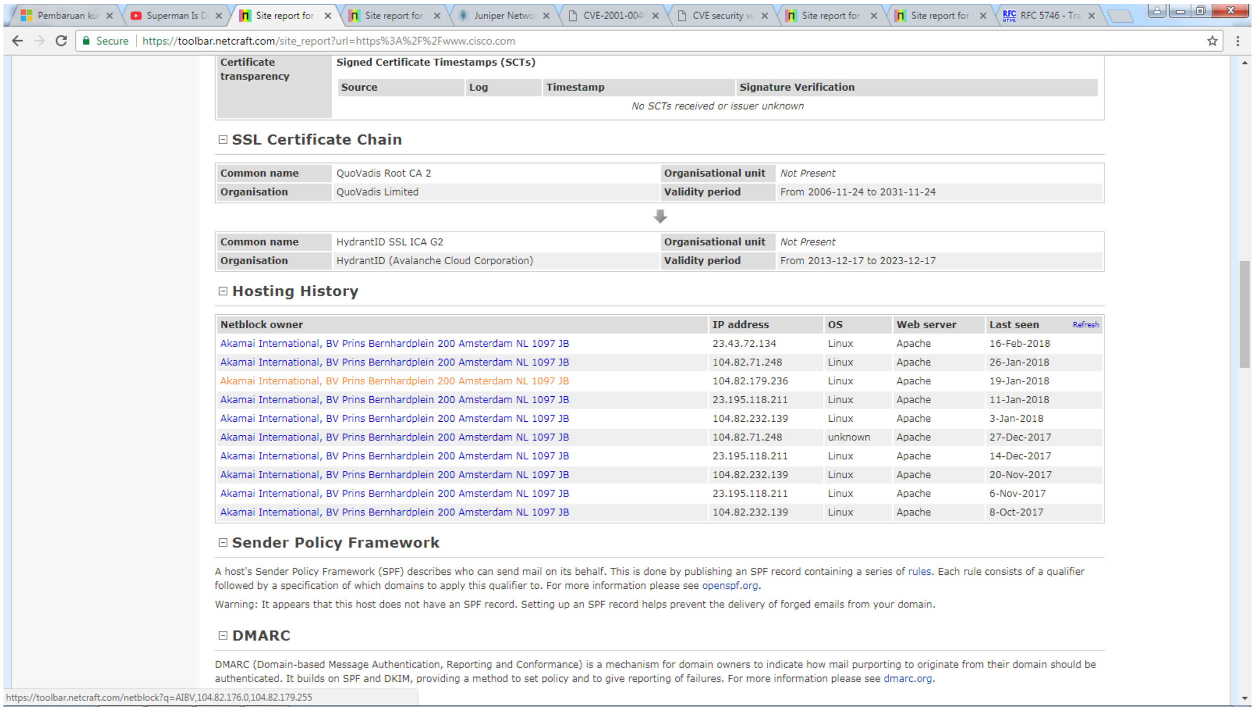
JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

Common Vulnerabilities abd exposures berdasarkan info yang didapatkan dari penjelasan bahwa ip yang digunakan pada saat mencat=ri seranggan CVE yang digunakan dengan cisco adalah 23.43.72.134 untuk terahir yang saya update.

Untuk mencari celah dari keamanan seranggan yang terdapat dalam menggunakan CVE yaitu common vulnerabilites and exposures CVE adala dalam kamus cyber security yang diketahui untuk kerentanan umum agar bertujuan untuk mengidentifikasi dan memberi nama secara terbuka kepada umum kerentanaan yang berkaitan dengan versi perangkat lunak tertentu dalam suatu code bases.



Certificate transparency	Signed Certificate Timestamps (SCTs)			
	Source	Log	Timestamp	Signature Verification
	No SCTs received or issuer unknown			

⊟ SSL Certificate Chain

Common name	QuoVadis Root CA 2	Organisational unit	*Not Present*
Organisation	QuoVadis Limited	Validity period	From 2006-11-24 to 2031-11-24

Common name	HydrantID SSL ICA G2	Organisational unit	*Not Present*
Organisation	HydrantID (Avalanche Cloud Corporation)	Validity period	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

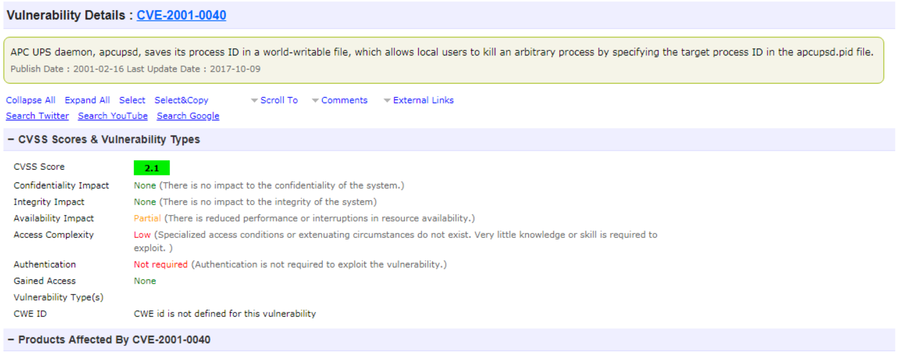
A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see openspf.org.

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=AIBV,104.82.176.0,104.82.179.255



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

− 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

Apache adalahsebuahnama web server yang bertanggungjawabpada request-response HTTP dan logging informasisecaradetail(kegunaanbasicnya). Selainitu, Apache jugadiartikansebagaisuatu web server yang kompak, modular, mengikutistandarprotokol HTTP, dantentusajasangatdigemari. Kesimpulaninibisadidapatkandarijumlahpengguna yang jauhmelebihiparapesaingnya.

Apache memilikifitur-fiturcanggihsepertipesankesalahan yang dapatdikonfigur, autentikasiberbasis basis data dan lain-lain.Apache jugadidukungolehsejumlahantarmukapenggunaberbasisgrafik (GUI) yang memungkinkanpenanganan server menjadimudah.Apache merupakanperangkatlunaksumberterbukadikembangkanolehkomunitasterbuka yang terdiridaripengembang-pengembangdibawahnaungan Apache Software Foundation.