TASK IV

KEAMANAN JARINGAN KOMPUTER

OLEH :

MARINI SUPRIANTY

09011181419016

FAKULTAS ILMU KOMPUTER

JURUSAN SISTEM KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

HASIL RECONNAISSANCE WEBSITE MICROSOFT.COM

STEP MAPPING MENGGUNAKAN NMS (MICROSOFT.COM)

Reconnaissance adalah sebuah fase persiapan sebelum attacker atau penyerang melakukan penyerangan, dimana kegiatan intinya adalah mengumpulkan informasi sebanyak mungkin mengenai sasaran. Terdapat sebuah tool yang digunakan untuk mendapatkan sejumlah data data yang berhubungan dengan Huawei, tool yangdigunakan dapat berupa whois, whatweb, ntcraft dan sebagainya. Maka berikut penjelasan yang dapat saya berikan.

1. **WhoIs**

   Whois atau disuarakan “who is” digunakan untuk mendapatkan data informasi domain tertentu seperti nama pemilik domain, ip address, name server dan umur domain. Whois lookup yaitu sebuah aplikasi berbasis command line digunakan untuk melakukan query terhadap database whois.

   Namun dalam perkembangannya, data whois suatu domain bisa dilihat di situs whois seperti domaintools atau whois.net. Sehingga user biasa seperti kita bisa mendapatkan informasi kepemilikan suatu domain dengan mudah. Walaupun demikian program whois berbasis command-line masih sering digunakan oleh Administrator jaringan.

RAW WHOIS DATA

```
Domain Name: microsoft.com
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2014-10-15T04:00:12-0700
Creation Date: 1991-05-01T21:00:00-0700
Registrar Registration Expiration Date: 2021-05-02T21:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited
(https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited
(https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited
(https://www.icann.org/epp#clientDeleteProhibited)
```

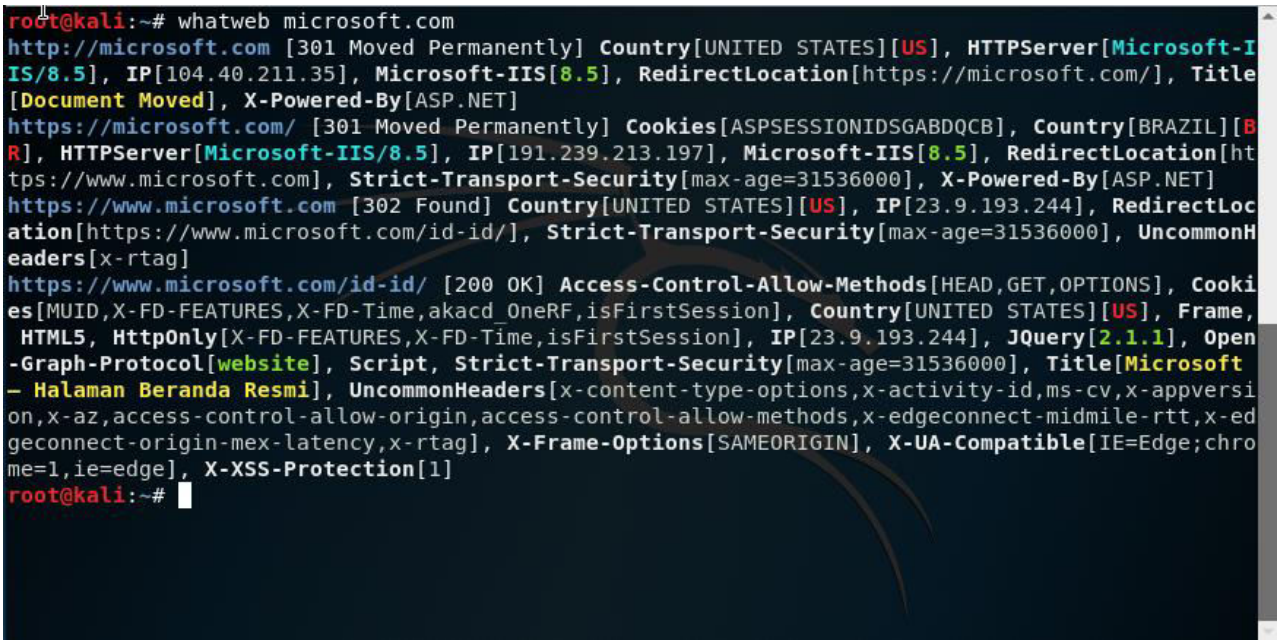
Domain Status: serverUpdateProhibited
(https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited
(https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited
(https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way,
Registrant City: Redmond
Registrant State/Province: WA
Registrant Postal Code: 98052
Registrant Country: US
Registrant Phone: +1.4258828080
Registrant Phone Ext:
Registrant Fax: +1.4259367329
Registrant Fax Ext:
Registrant Email: domains@microsoft.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Microsoft Corporation
Admin Street: One Microsoft Way,
Admin City: Redmond
Admin State/Province: WA
Admin Postal Code: 98052
Admin Country: US
Admin Phone: +1.4258828080
Admin Phone Ext:
Admin Fax: +1.4259367329
Admin Fax Ext:
Admin Email: domains@microsoft.com
Registry Tech ID:
Tech Name: MSN Hostmaster
Tech Organization: Microsoft Corporation
Tech Street: One Microsoft Way,
Tech City: Redmond
Tech State/Province: WA
Tech Postal Code: 98052
Tech Country: US
Tech Phone: +1.4258828080
Tech Phone Ext:
Tech Fax: +1.4259367329
Tech Fax Ext:
Tech Email: msnhst@microsoft.com
Name Server: ns3.msft.net
Name Server: ns4.msft.net
Name Server: ns1.msft.net
Name Server: ns2.msft.net
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2018-03-09T00:40:01-0800 <<<

```
     MarkMonitor.com (or its systems).
MarkMonitor.com reserves the right to modify these terms at any time.
By submitting this query, you agree to abide by this policy.

MarkMonitor is the Global Leader in Online Brand Protection.

MarkMonitor Domain Management(TM)
MarkMonitor Brand Protection(TM)
MarkMonitor AntiPiracy(TM)
MarkMonitor AntiFraud(TM)
Professional and Managed Services

Visit MarkMonitor at http://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220

For more information on Whois status codes, please visit
 https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en
```

2. WhatWeb

Whatweb adalah salah satu Tools untuk Scanning website yang biasanya sudah include di Sistem Operasi Pentest seperti Kali Linux dan Parrot OS Sec.

WhatWeb mengidentifikasi situs. Tujuannya adalah untuk menjawab pertanyaan, "Apa Website yang?". WhatWeb mengakui teknologi web termasuk sistem manajemen konten (CMS), platform blogging, statistik / paket analytics, perpustakaan JavaScript, server web, dan perangkat embedded. WhatWeb memiliki lebih dari 1700 plugin, masing-masing untuk mengenali sesuatu yang berbeda. WhatWeb juga mengidentifikasi nomor versi, alamat email, ID account, modul kerangka web, kesalahan SQL, dan banyak lagi.



3. Netcraft

Netcraft adalah perusahaan penyedia layanan Internet yang berbasis di Bath, Inggris. Pendapatan yang diperoleh oleh Netcraft bersumber dari:

Penyedia layanan keamanan Internet yang mencakup layanan anti-fraud dan anti-phishing, pengetesan aplikasi dan lain-lain.

Menyediakan data-data untuk penelitian pada berbagai aspek di Internet. Netcraft telah menjelajah Internet sejak 1995 dan memiliki kewenangan pada market share dari web server, sistem operasi, hosting providers, ISP, transaksi terenkripsi, bisnis secara elektronik, bahasa-bahasa scripting dan teknologi konten di Internet. Biaya iklan pada situs Netcraft.

Results for microsoft.com

Found 292 sites

	Site	Site Report	First seen	Netblock	OS
1.	go.microsoft.com		november 2001	akamai technologies	linux
2.	www.microsoft.com		august 1995	akamai international, bv	linux
3.	support.microsoft.com		october 1997	akamai international, bv	linux
4.	download.microsoft.com		august 1999	akamai international, bv	linux
5.	technet.microsoft.com		august 1999	microsoft corporation	windows server 2012
6.	msdn.microsoft.com		september 1998	microsoft corporation	windows server 2012
7.	answers.microsoft.com		august 2009	akamai international, bv	linux
8.	www.catalog.update.microsoft.com		december 2016	microsoft corporation	windows server 2016
9.	windows.microsoft.com		june 1998	akamai international, bv	linux
10.	social.technet.microsoft.com		august 2008	microsoft corporation	windows server 2012
11.	catalog.update.microsoft.com		october 2007	microsoft corporation	windows server 2008
12.	o15.officeredir.microsoft.com		may 2012	microsoft corporation	windows server 2016
13.	office.microsoft.com		november 1998	microsoft corp	unknown
14.	e.microsoft.com		january 2014	microsoft informatica ltda	f5 big-ip
15.	azure.microsoft.com		may 2014	microsoft informatica ltda	windows server 2012
16.	microsoft.com		may 1996	microsoft corporation	windows server 2012
17.	www.update.microsoft.com		may 2007	microsoft corporation	windows server 2012
18.	update.microsoft.com		febuary 2005	microsoft corp	windows server 2012
19.	fullproduct.download.microsoft.com		november 2007	akamai technologies	linux
20.	apps.microsoft.com		may 2012	akamai international, bv	linux

Next page

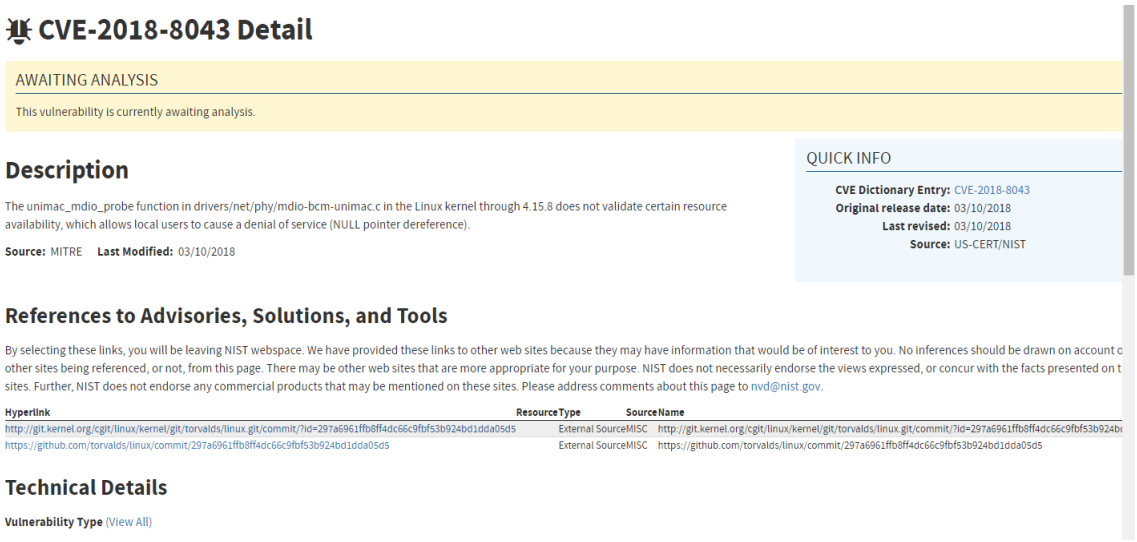
Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Akamai	88.221.16.244	Linux	unknown	12-Mar-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.44.101.131	Linux	unknown	5-Mar-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.133.197	Linux	unknown	4-Mar-2018
Akamai	88.221.16.244	Linux	unknown	1-Mar-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.133.197	Linux	unknown	1-Mar-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.44.101.131	Linux	unknown	27-Feb-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.133.197	Linux	unknown	26-Feb-2018
Akamai Technologies	2.19.152.139	Linux	unknown	17-Feb-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.60.196.55	Linux	unknown	9-Feb-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.99.6	Linux	unknown	6-Feb-2018

4. CVE

CVE-2018-8043 The unimac_mdio_probe function in drivers/net/phy/mdio-bcm-unimac.c in the Linux kernel through 4.15.8 does not validate certain resource availability, which allows local users to cause a denial of service (NULL pointer dereference).

Analisis pada hole yaitu Tanggal pembuatan entri mungkin mencerminkan kapan ID CVE dialokasikan atau dicadangkan, dan tidak harus menunjukkan kapan kerentanan ini ditemukan, dibagikan dengan vendor yang terkena dampak, diungkapkan kepada publik, atau diperbarui di CVE.



CVE-2018-8043 Detail

AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.

Description

The unimac_mdio_probe function in drivers/net/phy/mdio-bcm-unimac.c in the Linux kernel through 4.15.8 does not validate certain resource availability, which allows local users to cause a denial of service (NULL pointer dereference).

Source: MITRE **Last Modified:** 03/10/2018

QUICK INFO

CVE Dictionary Entry: CVE-2018-8043
Original release date: 03/10/2018
Last revised: 03/10/2018
Source: US-CERT/NIST

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account o other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on t sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource Type	Source Name
http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=297a6961ffb8ff4dc66c9fbf53b924bd1dda05d5	External Source MISC	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=297a6961ffb8ff4dc66c9fbf53b924b
https://github.com/torvalds/linux/commit/297a6961ffb8ff4dc66c9fbf53b924bd1dda05d5	External Source MISC	https://github.com/torvalds/linux/commit/297a6961ffb8ff4dc66c9fbf53b924bd1dda05d5

Technical Details

Vulnerability Type (View All)

Deskripsi

Fungsi unimac_mdio_probe pada driver / net / phy / mdio-bcm-unimac.c di kernel Linux melalui 4.15.8 tidak memvalidasi ketersediaan sumber daya tertentu, yang memungkinkan pengguna lokal menyebabkan penolakan layanan (NULL pointer dereference).

Dengan memilih link ini, Anda akan meninggalkan ruang web NIST. Kami telah menyediakan tautan ini ke situs web lain karena mereka mungkin memiliki informasi yang menarik bagi Anda. Tidak ada kesimpulan yang harus diambil karena situs lain yang dirujuk, atau tidak, dari halaman ini. Mungkin ada situs web lain yang lebih sesuai untuk tujuan Anda. NIST tidak selalu mendukung pandangan yang diungkapkan, atau sesuai dengan fakta yang disajikan di situs ini. Selanjutnya, NIST tidak mendukung produk komersial apa pun yang mungkin disebutkan di situs ini. Tolong sampaikan komentar tentang halaman ini ke nvd@nist.gov .