

KEAMANAN JARINGAN KOMPUTER
(REPORT: NETWORK MAPPING)



NAMA: ERDA JULIAN LESI

NIM: 09011181419065

KELAS: SK6B

DOSEN PENGAMPUH: DERIS STIAWAN, M.T., PH.D.

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

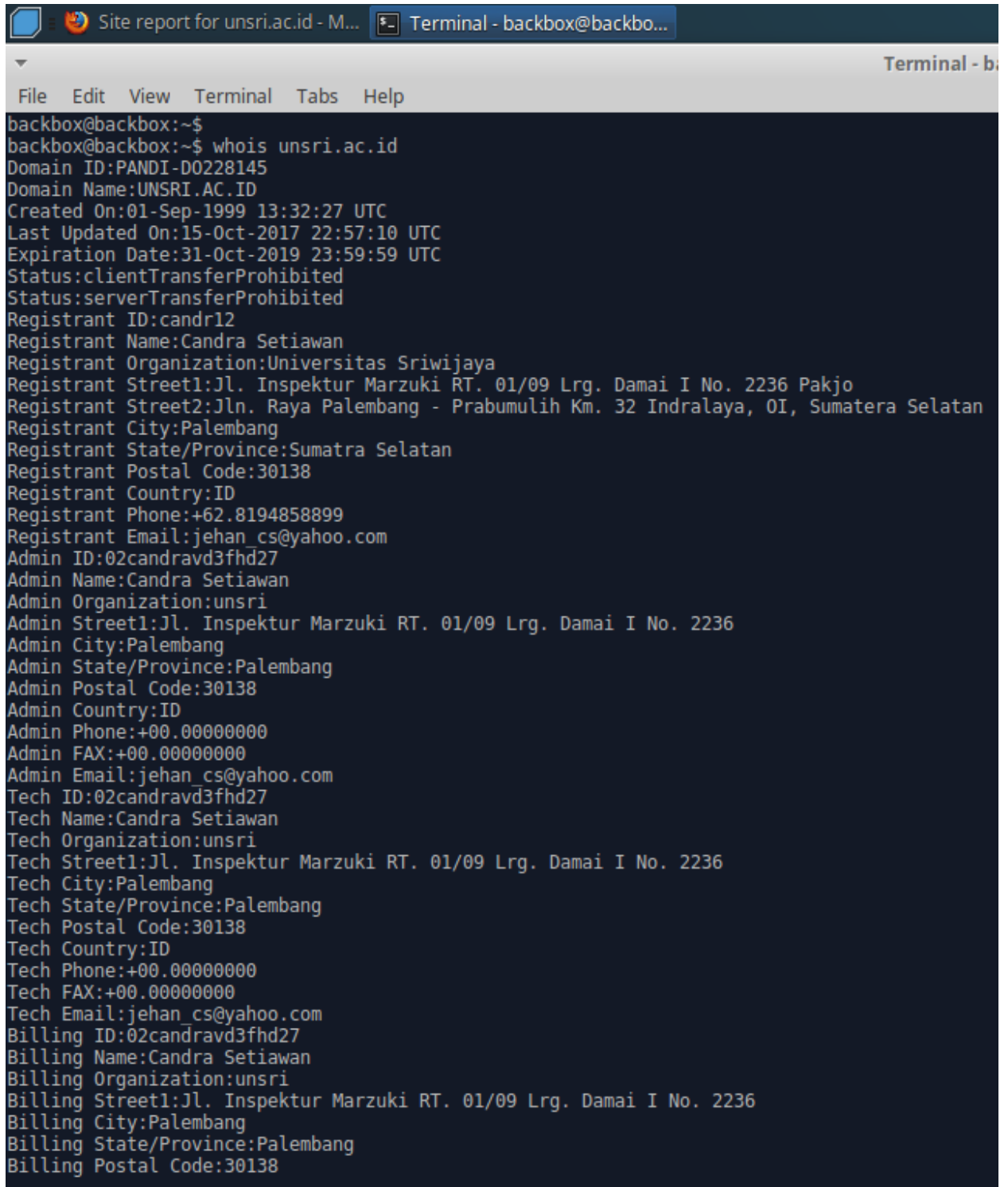
2018

NMAP (Network Mapping)

Target: unsri.ac.id

1. FOOT PRINTING

a. Who is?

A terminal window titled "Terminal - backbox@backbo..." is open. The terminal shows the command "whois unsri.ac.id" and its output. The output provides detailed information about the domain, including its creation and expiration dates, registrant details (Candra Setiawan from Universitas Sriwijaya), and technical/billing information. The terminal window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help".

```
backbox@backbox:~$  
backbox@backbox:~$ whois unsri.ac.id  
Domain ID:PANDI-D0228145  
Domain Name:UNSRI.AC.ID  
Created On:01-Sep-1999 13:32:27 UTC  
Last Updated On:15-Oct-2017 22:57:10 UTC  
Expiration Date:31-Oct-2019 23:59:59 UTC  
Status:clientTransferProhibited  
Status:serverTransferProhibited  
Registrant ID:candr12  
Registrant Name:Candra Setiawan  
Registrant Organization:Universitas Sriwijaya  
Registrant Street1:Jl. Inspektur Marzuki RT. 01/09 Lrg. Damai I No. 2236 Pakjo  
Registrant Street2:Jln. Raya Palembang - Prabumulih Km. 32 Indralaya, OI, Sumatera Selatan  
Registrant City:Palembang  
Registrant State/Province:Sumatra Selatan  
Registrant Postal Code:30138  
Registrant Country:ID  
Registrant Phone:+62.8194858899  
Registrant Email:jehan_cs@yahoo.com  
Admin ID:02candravd3fhd27  
Admin Name:Candra Setiawan  
Admin Organization:unsri  
Admin Street1:Jl. Inspektur Marzuki RT. 01/09 Lrg. Damai I No. 2236  
Admin City:Palembang  
Admin State/Province:Palembang  
Admin Postal Code:30138  
Admin Country:ID  
Admin Phone:+00.00000000  
Admin FAX:+00.00000000  
Admin Email:jehan_cs@yahoo.com  
Tech ID:02candravd3fhd27  
Tech Name:Candra Setiawan  
Tech Organization:unsri  
Tech Street1:Jl. Inspektur Marzuki RT. 01/09 Lrg. Damai I No. 2236  
Tech City:Palembang  
Tech State/Province:Palembang  
Tech Postal Code:30138  
Tech Country:ID  
Tech Phone:+00.00000000  
Tech FAX:+00.00000000  
Tech Email:jehan_cs@yahoo.com  
Billing ID:02candravd3fhd27  
Billing Name:Candra Setiawan  
Billing Organization:unsri  
Billing Street1:Jl. Inspektur Marzuki RT. 01/09 Lrg. Damai I No. 2236  
Billing City:Palembang  
Billing State/Province:Palembang  
Billing Postal Code:30138
```

Mencari / mengumpulkan informasi yang berkaitan dengan target yang akan di serang. Dari hasil diatas ada beberapa informasi penting yang bisa di manfaatkan, di antaranya waktu expired domain. Ada juga nama penanggung jawab pendaftar domain, beserta alamat lengkapnya. Bahkan terdapat nomor handpone. Informasi diatas didapat dari terminal, bisa juga diakses di <https://www.whois.com/whois/>.

b. Whatweb

```

http://unsri.ac.id [302] Cookies[PHPSESSID],
  Email[yadiutama@unsri.ac.id],
  HTTPServer[nginx],
  IP[103.241.4.11],
  JQuery[1.2.6],
  Meta-Author[yadiutama@unsri.ac.id],
  PHP[5.3.10-lubuntu3.25],
  PasswordField[password],
  RedirectLocation[http://www.unsri.ac.id/],
  Script[text/javascript],
  Title[::: Halaman Utama | Universitas Sriwijaya - Indralaya, Sumatera Selatan],
  X-Powered-By[PHP/5.3.10-lubuntu3.25],
nginx
  
```

Dari hasil scanning menggunakan tool Whatweb, di dapat beberapa informasi penting, di antaranya web server yang digunakan dalah nginx dengan IP 103.241.4.11, versi php yang di gunakan 5.3.10- lubuntu3.25 dan terdapat password.

c. Netcraft

Background

Site title	::: Halaman Utama Universitas Sriwijaya - Indralaya, Sumatera Selatan	Date first seen	June 2000
Site rank		Primary language	Indonesian
Description	Not Present		
Keywords	Not Present		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://unsri.ac.id	Netblock Owner	Universitas Sriwijaya
Domain	unsri.ac.id	Nameserver	ns1.unsri.ac.id
IP address	103.241.4.11	DNS admin	admin@unsri.ac.id
IPv6 address	2001:df1:7000:0:0:0:a2	Reverse DNS	ns4.unsri.ac.id
Domain registrar	pandi.or.id	Nameserver organisation	whois.pandi.or.id
Organisation	Universitas Sriwijaya, Jl. Inspektur Marzuki RT. 01/09 Lrg. Damai I No. 2236 Pakjo, Jln. Raya Palembang - Prabumulih Km. 32 Indralaya, OI, Sumatera Selatan, Palembang, 30138, Indonesia	Hosting company	unsri.ac.id
Top Level Domain	Indonesia (.ac.id)	DNS Security Extensions	unknown
Hosting country	ID		

☐ Hosting History


Netblock owner	IP address	OS	Web server	Last seen Refresh
Universitas Sriwijaya University / Direct Member IDNIC Jl. Raya Palembang - Prabumulih Km. 32 Indralaya, Ogan Ilir Sumatera Selatan 30662, Indonesia	103.241.4.11	Linux	nginx	6-Mar-2018
Universitas Sriwijaya University / Direct Member IDNIC Jl. Raya Palembang - Prabumulih Km. 32 Indralaya, Ogan Ilir Sumatera Selatan 30662, Indonesia	103.241.4.11	Linux	nginx/1.1.19	24-Apr-2016
Universitas Sriwijaya University / Direct Member IDNIC Jl. Raya Palembang - Prabumulih Km. 32 Indralaya, Ogan Ilir Sumatera Selatan 30662, Indonesia	103.241.4.11	Linux	Apache	3-Mar-2016
PT Telkom Indonesias customer.	222.124.194.11	Linux	Apache	2-Nov-2013
PT Telkom Indonesias customer.	222.124.194.11	Linux	Apache/2.2.22 Ubuntu	25-Nov-2012
PT Telkom Indonesias customer.	222.124.194.11	Linux	Apache	6-Sep-2012
PT Telkom Indonesias customer.	222.124.194.11	Linux	Apache/2.2.3 CentOS	6-Aug-2012
PT Telkom Indonesias customer.	222.124.194.11	Linux	unknown	1-Mar-2011
PT Telkom Indonesias customer.	222.124.194.11	Linux	Apache/2.2.3 CentOS	26-Feb-2011
PT Telkom Indonesias customer.	222.124.194.11	Linux	Apache/2.2.8 Fedora	23-Mar-2009

Mengetahui informasi dari server unsri.ac.id yang digunakan, mengetahui Risk rating (resiko keamanan website) unsri dimana warna hijau artinya hole rendah untuk dapat diserang, mengetahui Operating System (OS) yang digunakan dan masih banyak lagi fitur menarik yang ada didalamnya.

d. Reserve Domain

Reverse IP Domain Check

Remote Address

 Found **22** domains hosted on the same web server as [unsri.ac.id](#) (103.241.4.11).

103.241.4.11

[bse-diknas.unsri.ac.id](#)

[kemahasiswaan.unsri.ac.id](#)

[lemilit.unsri.ac.id](#)

[mkk.unsri.ac.id](#)

[pustaka.unsri.ac.id](#)

[www.baliteks.unsri.ac.id](#)

[www.kemahasiswaan.unsri.ac.id](#)

[www.nhk.or.jp](#)

[www.pdu.fk.unsri.ac.id](#)

[www.unsri.ac.id](#)

[archery.unsri.ac.id](#)

[digilib.unsri.ac.id](#)

[lecturer.unsri.ac.id](#)

[mipa.unsri.ac.id](#)

[pdu.fk.unsri.ac.id](#)

[unsri.ac.id](#)

[www.digilib.unsri.ac.id](#)

[www.lemilit.unsri.ac.id](#)

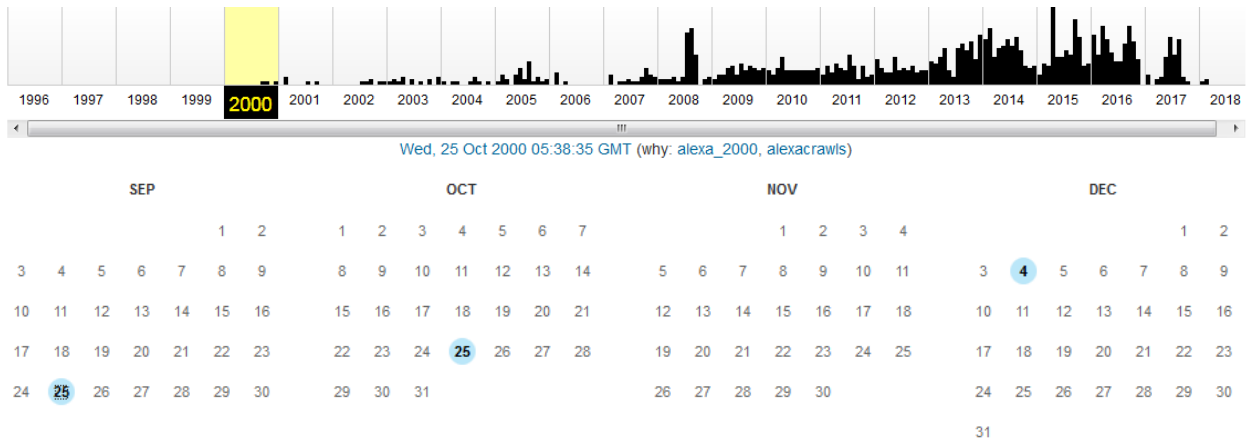
[www.pdg.fk.unsri.ac.id](#)

[www.sipil.ft.unsri.ac.id](#)

[yadiutama.unsri.ac.id](#)

Dari hasil reverse IP ke domain, di dapat bahwa domain unsri.ac.id bukan lah satu satunya domain yang hosting di satu web server tersebut, melainkan ada 22 domain, tindakan seperti ini sangatlah bahaya apalagi bila layanan website kita mempunyai informasi penting, karena penyerang bisa saja masuk kedalam sistem dari website lain yang mempunyai bug atau celah.

e. Web Archive



UNSR I Home Page: Welcome t... x +

https://web.archive.org/web/20000925035043/http://www.unsri.ac.id:80/

WayBackMachine 1,289 captures 25 Sep 2000 - 24 Feb 2018

Go **SEP 25** 1999 2000 2002

Logo UNSRI

Logo UNSRI

Sejarah

- Sejarah
- Visi, misi & tujuan

Fakultas

- Ekonomi
- Hukum
- Teknik
- Kedokteran
- Pertanian
- Keguruan / Ilmu Pendidikan
- MIPA
- Sosial / Politik

Pasca

- Magister Manajemen
- Magister Ilmu Ek.
- Magister Ilmu Tanam
- Magister Agribisnis
- Magister Ilmu

Situs Lembaga-lembaga :

Lembaga Penelitian

- +Pus. penelitian pemb.
- +Pus. penelitian lingk. hidup.
- +Pus. penelitian kependudukan.
- +Pus. penelitian Sosbud.
- +Pus. penelitian studi wanita.
- +Pus. penelitian energi.
- +Pus. penelitian tata ruang.
- +Pus. penelitian manaj. air
- +Pus. kajian mknan tradisional.

Kalender Akademik Universitas Sriwijaya 2000 / 2001

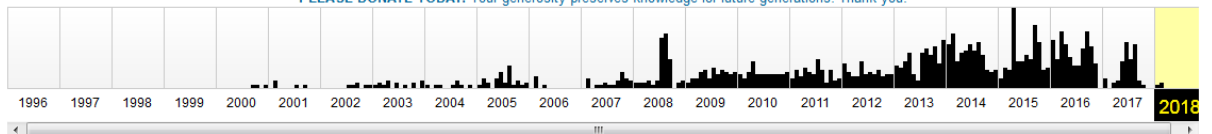
SEMESTER KHUSUS	
1. Pengumuman jadwal kuliah	2 Juni 2000
2. Pendaftaran peserta	8 - 19 Juni 2000
3. Awal perkuliahan	3 Juli 2000
4. Akhir perkuliahan	23 Agustus 2000
5. Masa Gajian	24 - 29 Agustus 2000
6. Penyerahan Nilai	28 - 31 Agustus
SEMESTER GANJIL	

Lembaga

Saved 1,289 times between September 25, 2000 and February 24, 2018.

[Summary of unsri.ac.id](#) · [Site Map of unsri.ac.id](#)

PLEASE DONATE TODAY. Your generosity preserves knowledge for future generations. Thank you.



Sat, 24 Feb 2018 03:17:03 GMT (why: webwidercrawl, survey_00007, survey_crawl)

The image shows a calendar for the year 2018, with February 24th highlighted. Below the calendar is a screenshot of a web browser displaying the Wayback Machine interface for the website <http://www.unsri.ac.id/>. The browser's address bar shows the URL, and the Wayback Machine interface indicates that there are 1,289 captures of the website from September 25, 2000, to February 24, 2018. The website's homepage is visible, featuring a large banner with the text "UNSR I" and a navigation menu with items like Beranda, Profil, Akademik, Fakultas, Civitas Akademika, Struktur Organisasi Senat, Pascasarjana, and Helpdesk. There are also banners for "Pendaftaran Online Ujian Saringan Masuk (USM) Program Pendidikan Dokter Spesialis (PPDS) Universitas Sriwijaya" and "SOP BANTUAN AKADEMIK TAHUN 2017".

Dari informasi yang di dapat dari archive.org, website unsri pertama kali online pada 25 september tahun 2000, webtool archive.org banyak menyimpan perubahan pada website <http://unsri.ac.id> yang mana informasi di sana bisa di manfaatkan penyerang apabila ada data penting di website unsri.ac.id, meskipun sudah di hapus dari server unsri.ac.id.

2. Scanning Network
 - a. Scanning Network

```
backbox@backbox:~$ nmap -sP 103.241.4.1 103.241.4.254

Starting Nmap 7.50 ( https://nmap.org ) at 2018-03-07 04:29 UTC
Nmap scan report for ip-103-241-4-1.unsri.ac.id (103.241.4.1)
Host is up (0.075s latency).
Nmap scan report for ip-103-241-4-254.unsri.ac.id (103.241.4.254)
Host is up (0.075s latency).
Nmap done: 2 IP addresses (2 hosts up) scanned in 0.08 seconds
```

Range ip yang dilihat 103.241.4.1 103.241.4.254, dimana seharusnya informasi semua range ip tertampil, saat asisten praktikum mengajarkan, namun pada pc yang saya coba tidak tampil, bisa saja karena connection yang kurang. Sehingga hanya 2 range ip yang tertampil.

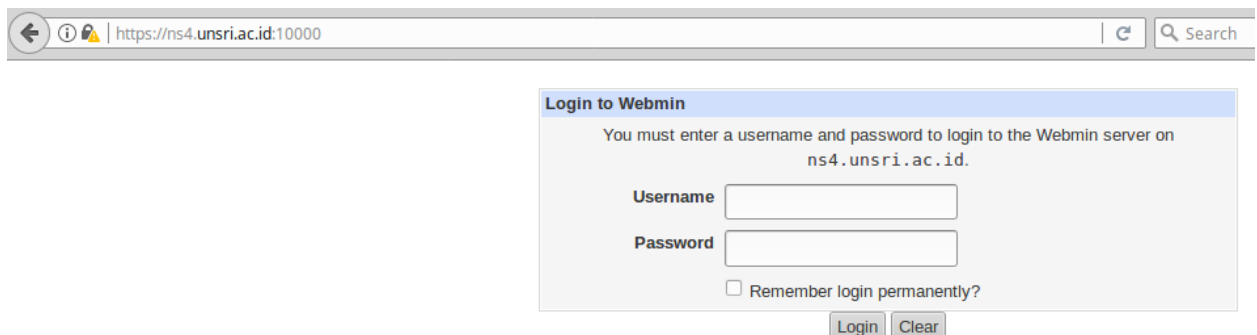
- b. Memeriksa service yang berjalan pada port

```
backbox@backbox:~$ nmap -sV 103.241.4.11

Starting Nmap 7.50 ( https://nmap.org ) at 2018-03-07 04:30 UTC
Nmap scan report for ns4.unsri.ac.id (103.241.4.11)
Host is up (0.088s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.0.8 or later
22/tcp    filtered ssh
53/tcp    filtered domain
80/tcp    open  http    nginx
111/tcp   open  rpcbind?
443/tcp   open  ssl/http nginx
8000/tcp  open  http    Apache httpd
10000/tcp open  http    MiniServ 1.860 (Webmin httpd)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.71 seconds
backbox@backbox:~$
```

Dari perintah diatas kita bisa mengetahui port terdapat informasi port, status, bahkan versi.



Saat mencoba salah satu port yang terbuka adalah port 10000 seperti tampilan diatas

```
backbox@backbox:~$ nc unsri.ac.id 21
220 Sriwijaya University
```

```
Terminal - backbox@backbox: ~
File Edit View Terminal Tabs Help
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=300 ttl=56 time=334 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=301 ttl=56 time=89.0 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=302 ttl=56 time=318 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=303 ttl=56 time=188 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=304 ttl=56 time=76.8 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=305 ttl=56 time=7734 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=306 ttl=56 time=7812 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=310 ttl=56 time=3738 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=308 ttl=56 time=5786 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=307 ttl=56 time=6810 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=309 ttl=56 time=4762 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=312 ttl=56 time=1700 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=311 ttl=56 time=2725 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=313 ttl=56 time=701 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=314 ttl=56 time=308 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=315 ttl=56 time=101 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=316 ttl=56 time=67.8 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=317 ttl=56 time=79.1 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=318 ttl=56 time=86.9 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=319 ttl=56 time=76.0 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=320 ttl=56 time=71.8 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=321 ttl=56 time=80.1 ms
64 bytes from ns4.unsri.ac.id (103.241.4.11): icmp_seq=322 ttl=56 time=4533 ms
```

c. Mengidentifikasi sistem operasi mesin (OS)

```
backbox@backbox:~$ sudo nmap -O 103.241.4.11

Starting Nmap 7.50 ( https://nmap.org ) at 2018-03-07 04:57 UTC
Nmap scan report for ns4.unsri.ac.id (103.241.4.11)
Host is up (0.38s latency).
Not shown: 992 closed ports
PORT      STATE      SERVICE
21/tcp    open      ftp
22/tcp    filtered  ssh
53/tcp    filtered  domain
80/tcp    open      http
111/tcp   open      rpcbind
443/tcp   open      https
8000/tcp  open      http-alt
10000/tcp open      snet-sensor-mgmt
Device type: general purpose|firewall
Running (JUST GUESSING): Linux 3.X|2.6.X|4.X (93%), WatchGuard Fireware 11.X (88%)
OS CPE: cpe:/o:linux:linux_kernel:3.8 cpe:/o:watchguard:fireware:11.8 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:4
Aggressive OS guesses: Linux 3.8 (93%), Linux 3.2 - 3.8 (89%), WatchGuard Fireware 11.8 (88%), Linux 3.0 (88%), Linux 3.0 - 3.2 (88%), Linux 2.6.32 - 2.6.39 (87%), Linux 3.5 (87%), Linux 3.1 - 3.2 (86%), Linux 2.6.32 (85%), Linux 2.6.32 or 3.10 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 18 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 81.33 seconds
backbox@backbox:~$
```


Dari data diatas, prediksi terhadap sistem operasi yang digunakan dimana ia memprediksi 93% menggunakan Linux versi 3.8. sehingga kita perlu mencari CVE nya untuk mengetahui lebih detail.

3. Common Vulnerabilities and Exposures

Linux 3.8

<https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Linux+3.8>

Search Results

There are 9 CVE entries that match your search.

Name	Description
CVE-2013-2548	The crypto_report_one function in crypto/crypto_user.c in the report API in the crypto user configuration API in the Linux kernel through 3.8.2 uses an incorrect length value during a copy operation, which allows local users to obtain sensitive information from kernel memory by leveraging the CAP_NET_ADMIN capability.
CVE-2013-2547	The crypto_report_one function in crypto/crypto_user.c in the report API in the crypto user configuration API in the Linux kernel through 3.8.2 does not initialize certain structure members, which allows local users to obtain sensitive information from kernel heap memory by leveraging the CAP_NET_ADMIN capability.
CVE-2013-2546	The report API in the crypto user configuration API in the Linux kernel through 3.8.2 uses an incorrect C library function for copying strings, which allows local users to obtain sensitive information from kernel stack memory by leveraging the CAP_NET_ADMIN capability.
CVE-2013-1763	Array index error in the __sock_diag_rcv_msg function in net/core/sock_diag.c in the Linux kernel before 3.7.10 allows local users to gain privileges via a large family value in a Netlink message.
CVE-2013-0343	The ipv6_create_tempaddr function in net/ipv6/addrconf.c in the Linux kernel through 3.8 does not properly handle problems with the generation of IPv6 temporary addresses, which allows remote attackers to cause a denial of service (excessive retries and address-generation outage), and consequently obtain sensitive information, via ICMPv6 Router Advertisement (RA) messages.
CVE-2013-0290	The __skb_rcv_datagram function in net/core/datagram.c in the Linux kernel before 3.8 does not properly handle the MSG_PEEK flag with zero-length data, which allows local users to cause a denial of service (infinite loop and system hang) via a crafted application.
CVE-2013-0231	The pciback_enable_msi function in the PCI backend driver (drivers/xen/pciback/conf_space_capability_msi.c) in Xen for the Linux kernel 2.6.18 and 3.8 allows guest OS users with PCI device access to cause a denial of service via a large number of kernel log messages. NOTE: some of these details are obtained from third party information.
CVE-2012-4542	block/scsi_ioctl.c in the Linux kernel through 3.8 does not properly consider the SCSI device class during authorization of SCSI commands, which allows local users to bypass intended access restrictions via an SG_IO ioctl call that leverages overlapping opcodes.
CVE-2005-4351	The securelevels implementation in FreeBSD 7.0 and earlier, OpenBSD up to 3.8, DragonFly up to 1.2, and Linux up to 2.6.15 allows root users to bypass immutable settings for files by mounting another filesystem that masks the immutable files while the system is running.

<https://www.cvedetails.com/version/142711/Linux-Linux-Kernel-3.8.0.html>

Linux » Linux Kernel » 3.8.0 : Vulnerability Statistics

[Vulnerabilities \(231\)](#) [Related Metasploit Modules](#) (Cpe Name:cpe:/o:linux:linux_kernel:3.8.0)

[Vulnerability Feeds & Widgets](#)

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2013	89	52	3	24	9					8	18	14			3
2014	83	51	2	10	6					8	21	14			8
2015	10	5		1	1					2	1	2			
2016	24	17		10	6					1		12			
2017	20	9	1	3						1	3	3			
2018	5	4		1	1										
Total	231	138	6	49	23					20	43	45			11
% Of All		59.7	2.6	21.2	10.0	0.0	0.0	0.0	0.0	8.7	18.6	19.5	0.0	0.0	

Memungkinkan pengguna lokal mendapatkan informasi sensitif dari memori kernel dengan memanfaatkan kemampuan CAP_NET_ADMIN.

Web yang digunakan “unsri.ac.id”

IP yang digunakan 103.241.4.11

celah: Low