

# **Tugas Keamanan Jaringan Komputer**

## **Hands-on Port Scanning with Nmap**



Nama : Aidil Fitri Yansya  
NIM : 09011281419054  
Kelas : SK8 PIL  
Dosen Pembimbing : Deris Stiawan, M.T., Ph.D

**JURUSAN SISTEM KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS SRIWIJAYA**

Tahapan yang dilakukan :

- A. Scanning Network
- B. Scanning Source
- C. Scanning Type Os

Dalam percobaan ini website target yang akan di scanning ialah [www.unsri.ac.id](http://www.unsri.ac.id)

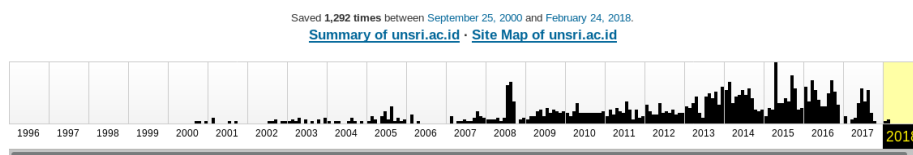
Pertama yang dilakukan ialah melakukan identifikasi website tersebut menggunakan “whois” yang berfungsi untuk mendapatkan data informasi domain tertentu seperti nama pemilik domain, ip address, name server, no telepon, alamat email, kapan domain ini di daftarkan dan kapan domain ini akan expired. Untuk mencari informasi mengenai web tersebut tinggal mengetikkan whois namadomain. Contoh whois unsri.ac.id, kemudian akan menampilkan informasi-informasi mengenai web target.

```
root@Aidilfy: ~  
File Edit View Search Terminal Help  
root@Aidilfy:~# 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:candri2  
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, 01, Sumate  
ra 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
```

Kemudian mengetikkan whatweb unsri.ac.id di terminal yang telah ada, fungsi dari whatweb ini ialah untuk mengetahui informasi juga yang terdapat dalam web target namun whatweb ini lebih mengarah ke sisi web server yang digunakan, dari informasi tersebut didapat bahwa web server yang di pakai ialah web server nginx dan os yang digunakan ialah linux.

```
root@Aidilfy:~# whatweb unsri.ac.id  
unsri.ac.id [ Unassigned]  
root@Aidilfy:~# whatweb www.unsri.ac.id  
http://www.unsri.ac.id [200 OK] Cookies[PHPSESSID], Country[INDONESIA][ID], Email  
[yadiutama@unsri.ac.id], Google-Analytics[Universal][UA-68096542-1,UA-92898935-  
1], HTTPServer[nginx], IP[103.241.4.11], JQuery[1.2.6], Meta-Author[yadiutama@un  
sri.ac.id], PHP[5.3.10-lubuntu3.25], PasswordField[password], Script[text/javasc  
ript], Title[.: Halaman Utama | Universitas Sriwijaya - Indralaya, Sumatera Sel  
atan], X-Powered-By[PHP/5.3.10-lubuntu3.25], nginx  
root@Aidilfy:~#
```

Lalu mencari domain yang web server nya sama dengan web target . Seperti contoh web target yg digunakan ialah unsri.ac.id seperti yang telah di lakukan di awal menggunakan web target unsri.ac.id terdapat beberapa domain yang sama dengan web server unsri.ac.id yaitu bse-diknas.unsri.ac.id, kemahasiswaan.unsri.ac.id, pustaka.unsri.ac.id dan masih banyak lagi, ada 22 domain. Kemudian kita melihat arsip-arsip yang ada pada web unsri.ac.id dari pertama kali dibuat hingga sekarang dengan melakukan membuka browser lalu mengetikan <https://web.archive.org> di kolom pencarian, kita cari web target yang ingin dilihat.



Lalu nmap -sP 103.241.4.1/24 untuk mengecek ip yang digunakan dimulai dari 103.241.4.1 - 103.241.4.255 : dari 256 IP ada 74 hosts up ip .

```
root@Aidilfy: ~  
File Edit View Search Terminal Help  
root@Aidilfy:~# nmap -sP 103.241.4.1/24  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 22:55 WIB  
Nmap scan report for ip-103-241-4-1.unsri.ac.id (103.241.4.1)  
Host is up (0.039s latency).  
Nmap scan report for ns1.unsri.ac.id (103.241.4.2)  
Host is up (0.040s latency).  
Nmap scan report for talangkelapo.unsri.ac.id (103.241.4.4)  
Host is up (0.042s latency).  
Nmap scan report for lahat.unsri.ac.id (103.241.4.6)  
Host is up (0.043s latency).  
Nmap scan report for demanglebardaun.unsri.ac.id (103.241.4.8)  
Host is up (0.045s latency).  
Nmap scan report for ns4.unsri.ac.id (103.241.4.11)  
Host is up (0.049s latency).  
Nmap scan report for lpse.unsri.ac.id (103.241.4.13)  
Host is up (0.039s latency).  
Nmap scan report for muaro.unsri.ac.id (103.241.4.14)  
Host is up (0.039s latency).  
Nmap scan report for dadarjiwo.unsri.ac.id (103.241.4.15)  
Host is up (0.039s latency).  
Nmap scan report for elearning.unsri.ac.id (103.241.4.18)  
Host is up (0.045s latency).  
Nmap scan report for ip-103-241-4-23.unsri.ac.id (103.241.4.23)
```

Kemudian melakukan nmap -sV 103.241.4.1 untuk Memeriksa service yang berjalan pada port target .

```
root@Aidilfy: ~
File Edit View Search Terminal Help
Host is up (0.042s latency).
Nmap done: 256 IP addresses (74 hosts up) scanned in 17.31 seconds
root@Aidilfy:~# nmap -sV 103.241.4.1

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 23:06 WIB
Nmap scan report for ip-103-241-4-1.unsri.ac.id (103.241.4.1)
Host is up (0.052s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  tcpwrapped
23/tcp    open  tcpwrapped
25/tcp    filtered smtp
80/tcp    open  nagios-nasca Nagios NSCA
179/tcp   open  tcpwrapped
2000/tcp  open  bandwidth-test Mikrotik bandwidth-test server
8181/tcp  open  http         Mikrotik router config httpd
8291/tcp  open  unknown
9090/tcp  filtered zeus-admin
Service Info: OS: RouterOS; Device: router; CPE: cpe:/o:mikrotik:routeros

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 162.99 seconds
root@Aidilfy:~#
```

Dari gambar diatas dapat diketahui bahwa port yang terbuka ialah port 22 ialah untuk ssh, 23 untuk tcp/udp, 80 untuk http, port 179, port 2000, dan port 8181. Namun disini kita tidak bisa membrute force ssh username dan password yang ada dengan memanfaatkan port 22 yang telah terbuka dikarena kan waktu yang diperlukan cukup lama tergantung dari kerumitan password yang telah dibuat.

Lalu melakukan nmap -O unsri.ac.id untuk mengidentifikasi sistem operasi mesin yang digunakan.

```
root@Aidilfy: ~
File Edit View Search Terminal Help
root@Aidilfy:~# nmap -O unsri.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 23:28 WIB
Nmap scan report for unsri.ac.id (103.241.4.11)
Host is up (0.040s latency).
Other addresses for unsri.ac.id (not scanned): 2001:df1:7000::a2
rDNS record for 103.241.4.11: ns4.unsri.ac.id
Not shown: 989 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    filtered ssh
25/tcp    filtered smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
443/tcp   open  https
8080/tcp  open  http-alt
8080/tcp  filtered http-proxy
9090/tcp  filtered zeus-admin
10000/tcp open  snet-sensor-mgmt
Device type: general purpose|firewall
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), WatchGuard Firewall 11.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:3.8 cpe:/o:watchguard:fireware:11.8 cpe:/o:linux:linux_kernel:2.6
Aggressive OS guesses: Linux 3.8 (92%), Linux 3.0 (89%), Linux 3.2 - 3.8 (87%), WatchGuard Firewall 11.8 (87%), Linux 3.1 - 3.2 (86%), Linux 2.6.32 - 2.6.39 (85%), Linux 3.5 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 8 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.59 seconds
```

Dari gambar tersebut diketahui bahwa OS yang digunakan ialah linux, dalam gambar tersebut banyak versi dari linux yang digunakan. Disini untuk mencari celah nya saya

menggunakan Linux 2.6.32 karena memiliki nilai persentase yang kecil dibandingkan dengan linux versi lainnya.

[Linux](#) » [Linux Kernel](#) » [2.6.32 RC4](#) : Security Vulnerabilities

Cpe Name: `cpe:/o:linux:linux_kernel:2.6.32:rc4`  
 CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9  
 Sort Results By: [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

Total number of vulnerabilities : 204 Page : 1 (This Page) 2 3 4 5

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	<a href="#">CVE-2017-1000407</a>	<a href="#">754</a>		DoS	2017-12-11	2018-02-03	6.1	None	Local Network	Low	Not required	None	None	Complete
The Linux Kernel 2.6.32 and later are affected by a denial of service, by flooding the diagnostic port 0x80 an exception can be triggered leading to a kernel panic.														
2	<a href="#">CVE-2017-1000251</a>	<a href="#">119</a>		Exec Code Overflow	2017-09-12	2018-02-16	8.3	Admin	Local Network	Low	Not required	Complete	Complete	Complete
The native Bluetooth stack in the Linux Kernel (BlueZ), starting at the Linux kernel version 2.6.32 and up to and including 4.13.1, are vulnerable to a stack overflow vulnerability in the processing of L2CAP configuration responses resulting in Remote code execution in kernel space.														
3	<a href="#">CVE-2017-18193</a>	<a href="#">119</a>		DoS Overflow	2018-02-22	2018-03-06	4.9	None	Local	Low	Not required	None	None	Complete
fs/2fs/extent_cache.c in the Linux kernel before 4.13 mishandles extent trees, which allows local users to cause a denial of service (BUG) via an application with multiple threads.														
4	<a href="#">CVE-2017-18174</a>	<a href="#">415</a>			2018-02-11	2018-03-12	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
In the Linux kernel before 4.7, the amd_gpio_remove function in drivers/pinctrl/pinctrl-amd.c calls the pinctrl_unregister function, leading to a double free.														
5	<a href="#">CVE-2017-18079</a>	<a href="#">476</a>		DoS	2018-01-29	2018-02-15	7.2	None	Local	Low	Not required	Complete	Complete	Complete
drivers/input/serial/8042.c in the Linux kernel before 4.12.4 allows attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact because the port->exists value can change after it is validated.														
6	<a href="#">CVE-2017-18075</a>	<a href="#">399</a>		DoS	2018-01-24	2018-02-09	7.2	None	Local	Low	Not required	Complete	Complete	Complete
crypto/pkcs11 in the Linux kernel before 4.14.13 mishandles freeing instances, allowing a local user able to access the AF_ALG-based AEAD interface (CONFIG_CRYPTO_USER_API_AEAD) and pccrypt (CONFIG_CRYPTO_PCCRYPT) to cause a denial of service (kfree of an incorrect pointer) or possibly have unspecified other impact by executing a crafted sequence of system calls.														
7	<a href="#">CVE-2017-17807</a>	<a href="#">284</a>			2017-12-20	2018-02-03	2.1	None	Local	Low	Not required	None	Partial	None
The KEYS subsystem in the Linux kernel before 4.14.6 omitted an access-control check when adding a key to the current task's "default request-key keyring" via the request_key() system call, allowing a local user to use a sequence of crafted system calls to add keys to a keyring with only Search permission (not Write permission) to that keyring, related to construct_net_keyring() in security/keys/request_key.c														

Dari 7 CVE tersebut saya mengambil yang no 2 dikarenakan score cvss nya besar yaitu 8.3, seperti yang saya ketahui bahwa apabila score cvss nya besar maka cve tersebut sangat rentan terhadap serangan, dan juga memiliki banyak hole. Dari vulnerability Details : CVE-2017-1000251 dapat diketahui bahwa vulnerability type nya ialah Execute Code dan Overflow. CVE tersebut menjelaskan bahwa Kerentanan dilaporkan terjadi di kernel Linux. Pengguna jarak jauh pada jaringan nirkabel dapat mengeksekusi kode acak pada sistem target. Pengguna jarak jauh pada jaringan nirkabel Bluetooth dapat mengirim parameter Logical Link Control and Adaptation Layer Protocol (L2CAP) yang dibuat khusus untuk memicu stack overflow dalam implementasi Bluetooth kernel dan mengeksekusi kode sembarang pada sistem target. Kode akan berjalan dengan hak istimewa tingkat kernel. Dampaknya ialah Pengguna jarak jauh pada jaringan nirkabel dapat mengeksekusi kode acak pada sistem target.

Solusinya ialah Vendor telah mengeluarkan source code yang bisa diperbaiki, tersedia di: <https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=e860d2c904d1a9f38a24eb44c9f34b8f915a6ea3> .