Tugas
Keamanan Jaringan Komputer

Disusun Oleh :

Nama : Yonatan Riyadhi

NIM : 09011181419009

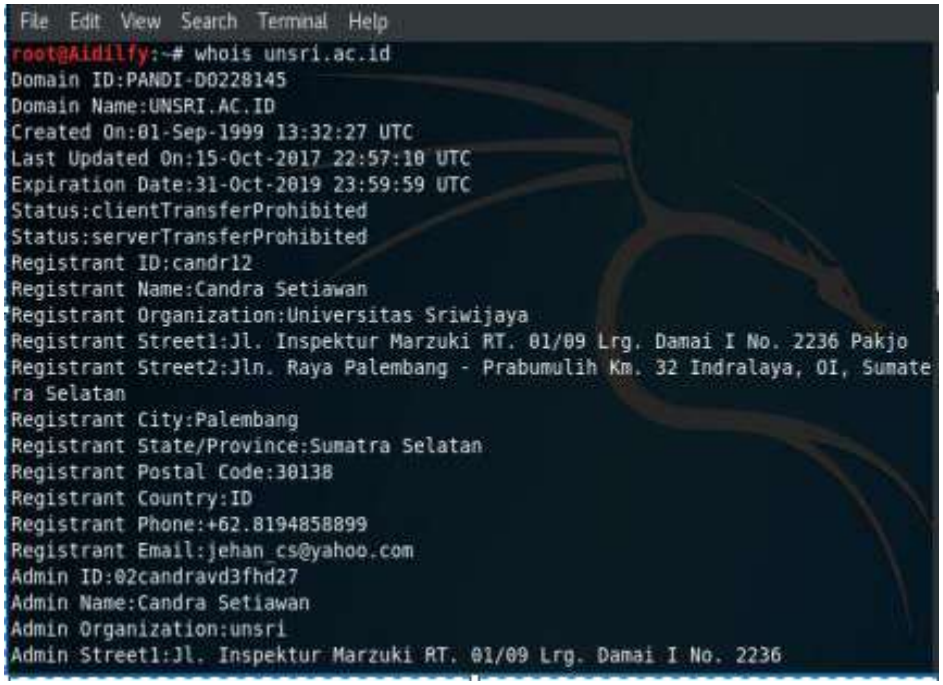
JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

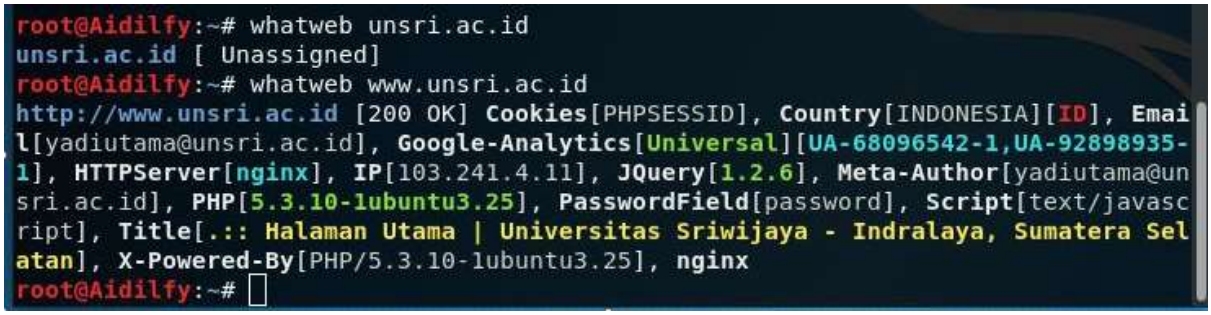
UNIVERSITAS SRIWIJAYA

2018

Dalam Hands on yang telah dilakukan, target percobaan yang dituju adalah www.unsri.ac.id. Adapun tahapan pertama yang dilakukan adalah dengan 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 nama domain. Contoh whois unsri.ac.id, kemudian akan menampilkan informasi-informasi mengenai web target.

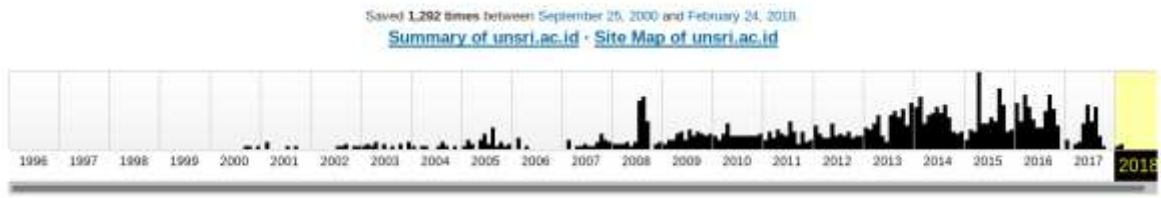


Kemudian mengetikkan whatweb unsri.ac.id di terminal yang telah ada, fungsi dari whatweb ini ialah untuk mengetahui informasi juga yang terdapat dalam web target namun whatweb ini lebih mengarah ke sisi web server yang digunakan, dari informasi tersebut didapat bahwa web server yang di pakai ialah web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

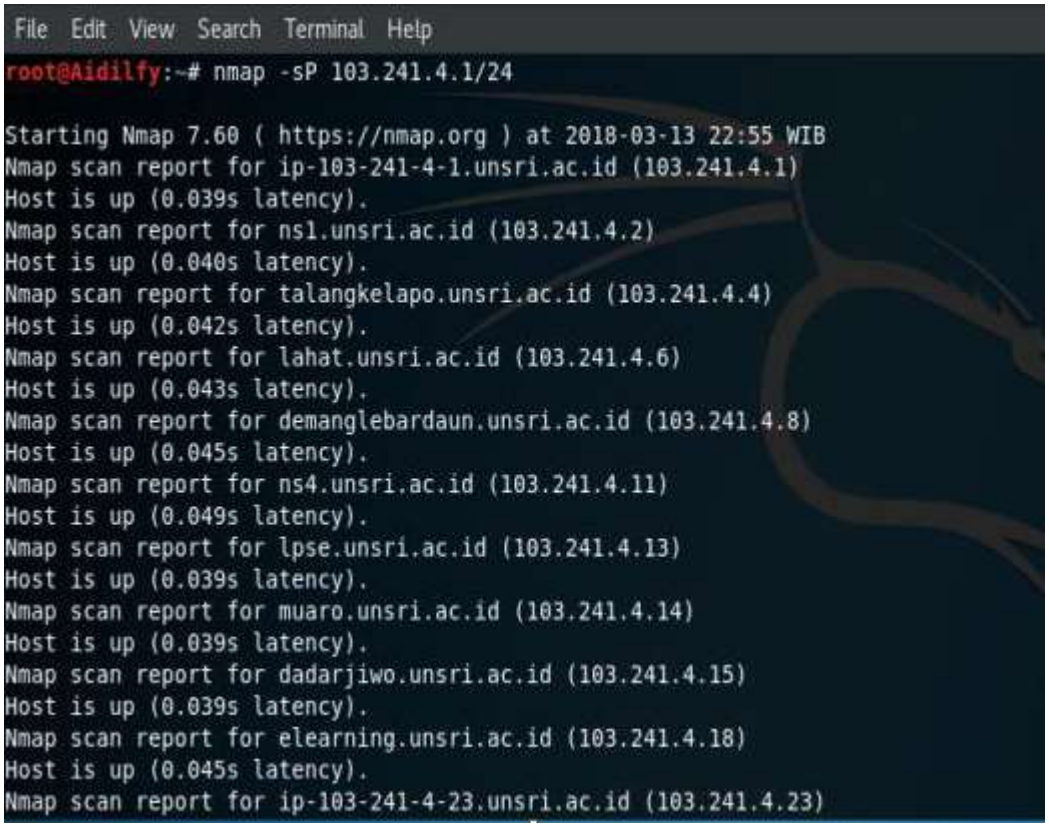


Lalu mencari domain yang web server nya sama dengan web target . Seperti contoh web target yg digunakan ialah unsri.ac.id seperti yang telah di lakukan di awal menggunakan web

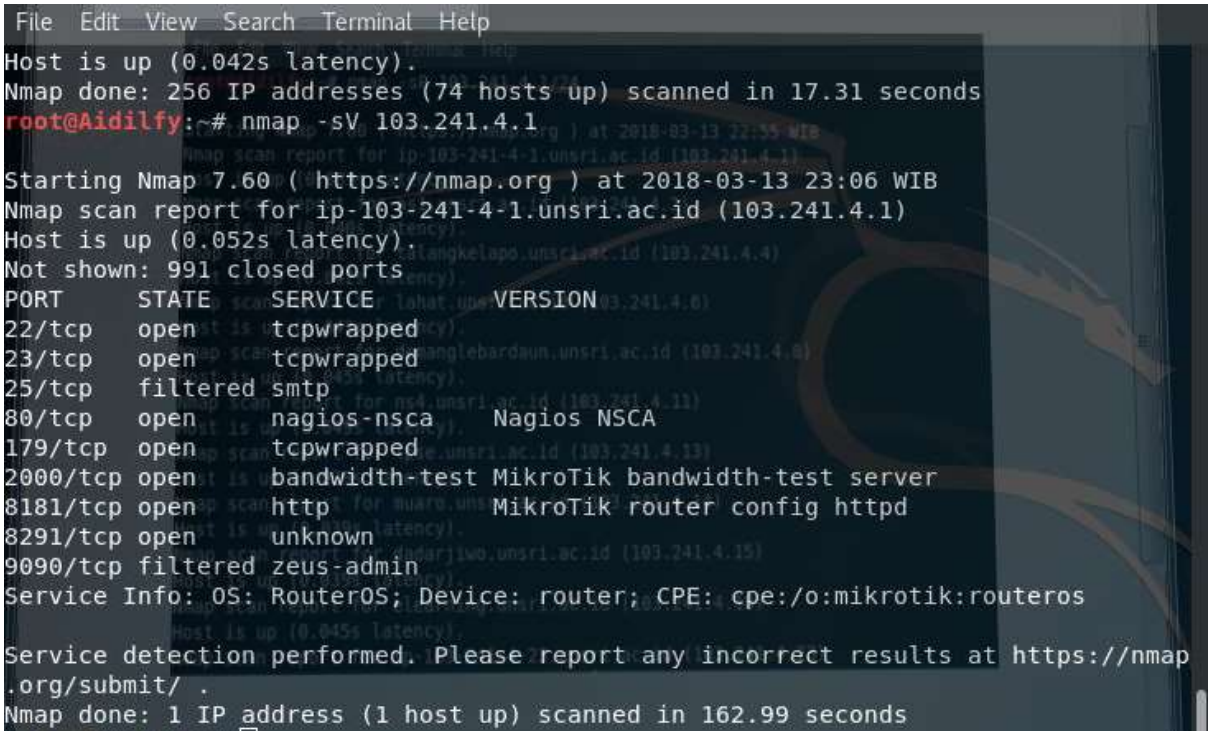
target unsri.ac.id terdapat beberapa domain yang sama dengan web server unsri.ac.id yaitu bse-diknas.unsri.ac.id, kemahasiswaan.unsri.ac.id, pustaka.unsri.ac.id dan masih banyak lagi, ada 22 domain. Kemudian kita melihat arsip-arsip yang ada pada web unsri.ac.id dari pertama kali dibuat hingga sekarang 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 .



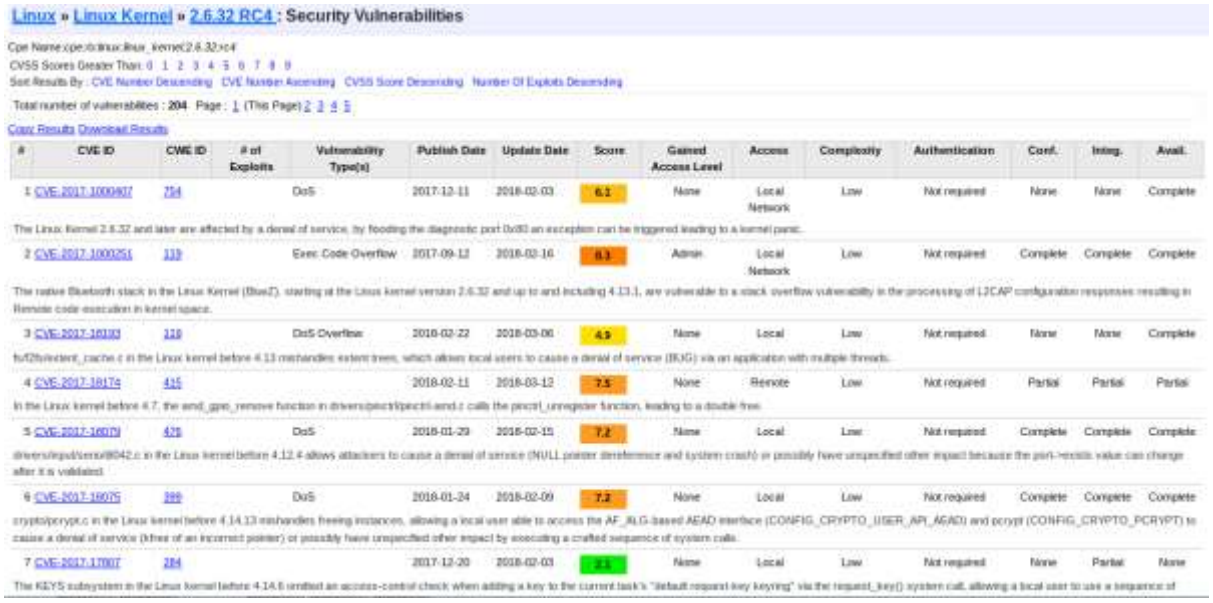
Kemudian melakukan nmap -sV 103.241.4.1 untuk Memeriksa service yang berjalan pada port target .



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.

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	CVE-2017-1000407	754		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	CVE-2017-1000251	119		Exec Code Overflow	2017-09-12	2018-03-16	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	CVE-2017-16939	119		DoS Overflow	2018-02-22	2018-03-06	4.9	None	Local	Low	Not required	None	None	Complete
	fs/f2fs/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	CVE-2017-18174	415			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	CVE-2017-16879	476		DoS	2018-01-29	2018-02-15	7.2	None	Local	Low	Not required	Complete	Complete	Complete
	drivers/input/serio/i8042.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	CVE-2017-16075	399		DoS	2018-01-24	2018-02-09	7.2	None	Local	Low	Not required	Complete	Complete	Complete
	crypto/pcrypt.c 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 pcrypt (CONFIG_CRYPTO_PCRYPT) 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	CVE-2017-17807	284			2017-12-20	2018-02-03	7.2	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													

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 codeyang bisa diperbaiki, tersedia di:https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=e860d2c904d1a9f38a24eb 44c9f34b8f915a6ea3 .