PENINGKATAN KEAMANAN JARINGAN WIRELESS DI FAKULTAS KEDOKTERAN KAMPUS MADANG UNSRI

Aan Restu Mukti[1], Budiman[2], Syahril Rizal[3], Suryayusra[4]

[1,2,3,4] Fakultas Sains Teknologi, Universitas Bina Darma

[1]aanrestu@binadarma.ac.id, [2]budiman@unsri.ac.id, [3]syahril.rizal@binadarma.ac.id, [4]suryayusra@binadarma.ac.id

Abstrak

Teknologi nirkabel merupakan salah satu keutamaan sebagai faktor penunjang dunia informasi. Jaringan komputer menjadi jalur pengiriman data melalui intranet maupun distribusi internet, sehingga keamanannya menjadi prioritas. Beberapa kasus yangsering terjadi mengenai kebocoran informasi baik di lingkup institusi pemerintahan maupun pendidikan menjadi evaluasi serius dalam meningkatkan keamanan jaringan. Tujuan penelitian ini mengidentifikasi kerentanan untuk mengurangi risiko serangan, mengukur efektifitas tingkat keamanan terhadap jaringan nirkabel, membuat laporan hasil data yang bisa berguna bagi administrator dalam mengatur keamanan jaringan nirkabel, memotivasi administrator untuk bisa mencari hal-hal baru agar berguna bagi banyak orang, metode *penetrasi* menggunakan metode *OWASP Framework* menjadi metode yang diusulkan dalam penelitian ini. Berdasarkan hasil uji coba penetrasi jaringan *wireless* pada Fakultas Kedokteran Universitas Sriwijaya Kampus Madang menggunakan *tools* OWASP Testing Guide versi 4.1 dari modul yang telah diuji coba, didapatkan beberapa hasil menggunakan *tools* sebagai berikut *Wifi Analyzer (Scanning* SSID jaringan *Wireless* berhasil dilakukan), *Netcut (ARP Spoofing* terhadap *host* berhasil dilakukan), *Nmap (Scanning* jaringan berhasil dilakukan, *Brute Force* tidak berhasil), *Dirbuster (Brute Force* direktori server berhasil dilakukan). Dengan demikian dapat dilakukan audit keamanan jaringan secara berkala untuk mendeteksi dan memperbaiki potensi kelemahan sebelum dieksploitasi.

Kata kunci : Keamanan jaringan, *Netcut, Nmap, OWASP Dirbuster, Wifi Analyzer*

1. Pendahuluan

Teknologi nirkabel merupakan salah satu keutamaan sebagai faktor penunjang dunia informasi. Informasi di dunia jaringan tidak semua terbuka untuk umum. Karena jaringan nirkabel yang bersifat terbuka diperlukan keamanan yang terjamin. Namun, disisi lain tetap saja ada pihak-pihak yang berusaha untuk menembus sistem internal pada jaringan nirkabel itu. Salah satu sisi untuk membuat jaringan itu menjadi aman yaitu menggunakan *firewall* (Elizar, 2014).

Fakultas Kedokteran Unsri kampus madang menyediakan jaringan nirkabel *(WiFi)* untuk karyawan, mahasiswa, tamu dan lainnya. Terlebih lagi jaringan yang disediakan adalah untuk umum. Jaringan yang umum memiliki banyak sekali kekurangan sehingga menyebabkan keamanan pengguna serta ketahanan perangkat penyedia dalam penggunaannya sering kali menjadi masalah. Keamanan jaringan yag sudah terimplementasi masih dirasa kurang dikarenakan hanya pada sisi server utama sehingga diperlukan juga adanya keamanan berlapis yang perlu diimplementasikan pada sisi pengguna umum. (Informatika et al., 2022). Hal tersebut dapat disimpulkan bahwa berbagai macam sifat pengguna dalam menggunakan jaringan terbuka dapat dipelajari untuk membaca kebiasaan hingga membantu pengguna lain dalam mengamankan datanya (Arianto, 2009).

Meskipun disediakannya sebuah fasilitas yang berupa perangkat yang melindungi dalam jaringan kampus tersebut, penulis akan melakukan uji coba pada jaringan tersebut apakah benar perangkat pelindung yang tersedia itu dapat melindungi secara *high priority* atau tidak sama sekali. Dilihat dari hasil analisa dan bukti dari hasil percobaan pada jaringan apakah paket data yang dilewati itu apakah akan dianggap sebagai penyusup atau bukan, jika pedeteksian anomali pola paket tersebut dapat dibaca oleh mesin pengaman tersebut maka, akan di di arahkan degan *rules* yang sudah otomatis diatur oleh mesin *firewall* itu (Rijadi, 2021).

Pada saat ini sudah banyak persaingan dari *vendor* untuk membuat dan mengembangkan *firewall* baik berupa *hardware* ataupun *software* yang bersifat *realtime* aktif sehingga dapat melakukan tugas untuk melindungi jaringan itu dari serangan ketika terdeteksi, dengan menutupi celah-celah seperti *port* atau mem-filter beberapa *Internet Protocol (IP). Firewall* seperti ini pada umumnya disebut sebagai *Intrusion Prevention System (IPS)*. IPS merupakan suatu metode yang digunakan untuk mencegah aktifitas dan percobaan penyusup. Fungsi IPS ada 2 dalam kemapuan mendeteksi penyusupan dan kemampuan mencegah akses penyusupan.

Kemampuan inilah yang disebut *Interusion Detection System (IDS)* (Engineering et al., 2021).

Pada penelitian ini akan dilakukan ujicoba terhadap sistem jaringan nirkabel pada Fakultas Kedokteran Kampus Madang Universitas Sriwijaya, apakah mampu atau tidaknya untuk masala keamanan jaringan tersebut. Sistem ujicoba tersebu akan dilakukan dengan menggunakan metod *OWASP Framework* dengan secara acak, diman tahapan ujicoba serangan paket data denga menggunakan *tools-tools* apakah akan berhasil ata tidak.

2. Metode

2.1 *Wifi Analyzer*

Wifi Analyzer adalah aplikasi untu menganalisa jaringan *WiFi* di sekitar. Denga aplikasi ini kita bisa mendapatkan informasi kualita sinyal dan saturasi jaringan (Cetak & Online, 2022)

Pada dasarnya, fungsi dari *Wifi Analyzer* adala menganalisis jaringan *wifi. Wifi Analyze* menampilkan informasi kualitas sinyal dan saturas pada jaringan *wifi.* Fitur-fitur yang ditampilka dalam aplikasi *wifi analyzer* yaitu dapa menampilkan grafik kualitas jaringan *wifi* yan dijangkau, menampilkan urutan koneksi jaringan wi dengan skala nilai tertentu, dan juga sebaga pengukur yang menunjukkan saturasi setiap jaringa yang ditampilkan. *User* dapat melihat jaringan *wi* terbaik yang dapat digunakan(Vaniamosa et al 2023).

Scanning jaringan dengan menggunakan *Wifi Analyzer* yaitu agar penulis dapat mengetahui jaringan *wireless* yang ada pada Kampus Madang UNSRI *Wifi Analyzer* merupakan langkah preventif, yaitu membantu administrator dimana letak sinyal yang lemah dan letak *dead zone.* Hal ini sangat penting karena permasalahan jaringan *wireless* pastinya nilai produktivitas menurun (Penguat & Wireless, 2023).

Pengamatan frekuensi menggunakan aplikasi *Wifi Analyzer*, frekuensi yang dipakai yaitu 2,4 Ghz 5 Ghz. yaitu mencari SSID target yang akan dihubungkan dengan perangkat yang akan diujicoba. Pada frekuensi 2,4 Ghz nama SSID yang didapatkan saat melakukan scanning adalah *@net-unsri-newBB*. Kemudian pada frekuensi 5 Ghz juga didapatkan dengan nama SSID yang di dapatkan saat scanning yaitu sama yang diberikan nama *@net-unsri-newBB*.

Berikut daftar tabel hasil pengukuran sinyal yang disebarkan dari akses point *@net-unsri-newBB.*

2.2 *Network Mapper (Nmap)*

Network Mapper merupakan perangkat lunak yang digunakan dalam pemindaian jaringan open-source yang digunakan untuk menemukan perangkat dan layanan dalam jaringan, serta memeriksa kerentanannya.

Berikut merupakan rincian informasi yang didapatkan dari hasil pemindaian menggunakan *Net Mapper* pada Tabel 1 di bawah ini.

Tabel 1. Sinyal Akses Point SSID *@net-unsri-newBB*

No.	Lokasi	Jumlah Akses Point	SSID (@net-unsri-newBB)	
			2,4 Ghz (dBm)	5 Ghz (dBm)
1	Dekanat	10	-73	-51
			-75	-60
			-81	-71
			-65	-54
2	Kelas	9	-76	-51
			-69	-53
			-74	-49
3	Perpustakaan	10	-65	-67
			-73	-79
4	Gedung Anatomi	7	-67	-59
			-74	-63
5	Gedung Fisiologi	8	-71	-66
			-76	-67
			-74	-70
6	Gedung AA	5	-73	-50
			-84	-61
			-93	-74
7	Gedung PPDS	6	-78	-73
			-73	-68
8	Animal House	2	-64	-54
			-74	-67

Pada saat *scanning* jaringan *Wifi* sudah didapatkan *SSID* target yang akan dihubungkan yaitu *@net-unsri-newBB.* Penulis akan melanjutkan tahap ujicoba dengan menghubungkan pada frekuensi 5 Ghz yang terdekat agar proses pengerjaan akan berjalan dengan lancar.

2.3 *NetCut*

Netcut adalah aplikasi yang berfungsi untuk menguasai suatu jaringan *Wireless* yang sama sehingga dapat memanfaatkan sepenuhnya *bandwidth* yang di dapatkan dari jaringan tersebut. Dengan memanfaatkan Netcut, proses *download* dapat lebih cepat. Cara kerja *Netcut* cukup sederhana. *Netcut* akan membatasi akses semua perangkat pengguna lain di dalam jaringan tersebut. NetCut dapat menentukan perangkat apa saja yang terhubung untuk mengakses jaringan tersebut. Baik dari segi keuntungan dapat mencegah dari serangan *NetCut*, jika dari segi kekurangan *NetCut* sangat merugikan *host* lain, meskipun ada *netcut killer*, akan tetapi biasanya akan proses akan menjadi *lag* (Waliulu et al., n.d.).

Berdasarkan protokol *ARP* Operator / administrator juga dapat menggunakan *NetCut* untuk mengatur jaringan, dan berdasarkan dari *IP-MAC Netcut* dapat menghentikan dan menggunakan

jaringan terhadap perangkat manapun yang terkoneksi. *NetCut* juga dapat digunakan pada perangkat yang terkoneksi dibawah *router* atau didalam *switch/hub*. Selain itu, *NetCut* juga bisa digunakan untuk menjaga perangkat terhadap serangan *ARP spoof* (Sriwijaya, 2015).

Kekurangan *netcut* adalah merugikan orang lain, bisa di *counter attack* menggunakan *netcut killer* sehingga terjadi banyak proses kemudian akan menjadi *lag*, sering disalah gunakan.

Pengujian dilakukan dengan metode *ARP Spoofing scanning*, yaitu penulis akan melakukan *scanning* pada jaringan yang sama dan akan di dapatkan beberapa host target yang terhubung pada jaringan tersebut, selanjutnya penulis akan melakukan ujicoba untuk membatasi paket data target menggunakan aplikasi *Netcut.* Tujuannya adalah untuk membatasi pemakaian bandwidth terhadap target.

Saat pengujian scanning berlangsung *netcut* melaporkan ada 9 perangkat yang terhubung pada jaringan *Wireless* SSID *@net-unsri-newBB*

Tahap *ARP Spoofing scanning* dan menghentikan koneksi target, dilakukan dengan menggunakan Aplikasi *NetCut* yang beroperasi pada sistem operasi *Windows* 10, dan akan menunjukkan langkah tersebut apakah berhasil dilakukan.

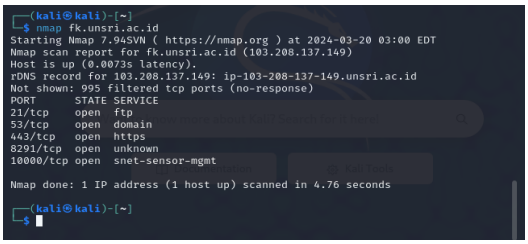
2.4 *Network Mapper (Nmap)*

Peran *Nmap* merupakan *tool* yang sangat berguna dalam mengaudit dan menganalisa kerentanan pada suatu jaringan. *Nmap* juga sangat bermanfaat bagi *administrator* jaringan untuk mengaudit. *Nmap* berfungsi untuk mendeteksi sistem operasi, melakukan proses *scanning-port*, *ping scan*, proses *ping scan* fungsinya melakukan ping ke setiap *host* untuk memastikan host tersebut aktif atau tidaknya.

Sniffing merupakan suatu aktivitas memantau dan menangkap data yang lewat pada suatu jaringan. Teknik ini biasanya dilakukan oleh pihak tidak bertanggung jawab untuk mencuri informasi dan data penting yang terjadi saat adanya komunikasi data pada jaringan internet (Kunci et al., 2023) .

Sebagian besar jenis pemindaian hanya tersedia untuk pengguna yang memiliki hak akses istimewa. Dikarenakan hal tersebut prosesnya dengan mengirim dan menerima *raw packets* yang memerlukan hak akses kedalam root pada Sistem Operasi Unix. Dianjurkan untuk menggunakan akun administrator pada Windows, meskipun Nmap terkadang berfungsi untuk pengguna yang tidak memiliki hak istimewa pada platform tersebut dimana saat *Npcap* telah dimuat ke dalam *OS*. Seperti kebanyakan dari pengguna hanya memiliki akses ke akun *shell* yang telah dibagikan untuk digunakan bersama. Sekarang, dunia berbeda. Harga komputer lebih murah, kebanyakan orang secara langsung mengakses Internet, dan sistem *desktop Unix* (termasuk *Linux* dan *Mac OS X)* merupakan hal yang sudah lazim. *Nmap* versi Windows kini tersedia, memungkinkan untuk dapat dijalankan dalam banyak perangkat *desktop*. Hal ini merupakan sebuah kemudahan, karena merupakan opsi pilihan yang istimewa membuat *Nmap* jauh lebih kuat dan *fleksibel*.

Banyak metode digunakan termasuk *sweep* terhadap *Internet Control Messaging* Protocol (ICMP), *Transmission Control Protocol* (TCP) dan *User Datagram Protocol (UDP). TCP/UDP ping* merupakan proses yang melibatkan *Acknowledgment* (ACK) atau *sinkronisasi* paket (SYN) ke *port-port* tertentu pada target *host.* Secara *default Nmap* menggunakan port 80, yang biasanya juga digunakan oleh protocol *Hypertext Transfer Protocol* (HTTP), akan tetapi batas dan fungsi Nmap bukan sampai disitu saja, Nmap juga dapat melakukan *scanning* pada port lain juga, seperti ditunjukkan pada Gambar 1. Dan juga tergantung pada koneksi ke *gateway*, dan *traffic* jaringan bisa tidak terdeteksi dan akan berhenti bahkan gagal. *Nmap* bisa mencari tahu layanan-layanan yang aktif pada *port* secara spesifik. Nmap juga dapat melakukan *fingerprinting* yang dapat membandingkan dan memperkirakan jenis sistem operasi target[o].



Gambar 1. Scanning *port* target *website*

Skenario yang dilakukan sebagai berikut:

1. *TCP Port Scan*
2. *UDP Port Scan*
3. *Scanning Sistem Operasi*
4. *Versi Daemon*
5. *CVE Detection*
6. *Brute Force*
7. *FTP Login*
8. *Combo Scanning*

2.4 Pengujian Menggunakan *DirBuster*

OWASP DirBuster ini adalah aplikasi Java yang dikembangkan oleh pihak OWASP. *DirBuster* adalah aplikasi java multi-thread yang dirancang untuk memaksa *(brute force)* direktori dan nama *file* di server web/aplikasi (Utama et al., 2022). Sekarang ini yang seringkali terjadi adalah apakah target instalasi default pada *server web* dalam keadaan sebenarnya atau tidak, dan apakah memiliki halaman dan aplikasi yang tersembunyi di dalamnya atau tidak. Maka dari itu *DirBuster* merupakan *tools* yang akan mencoba menemukannya. *DirBuster* mencari halaman dan direktori tersembunyi di *server web*.

Terkadang pengembang membiarkan halaman dapat diakses, namun tidak tertaut. *DirBuster* dimaksudkan untuk menemukan potensi kerentanan (Purba et al., 2021).

DirBuster dapat membantu administrator meningkatkan keamanan aplikasi dengan menemukan konten di *server web* atau di dalam aplikasi yang tidak diperlukan (atau bahkan tidak boleh dipublikasikan) atau dengan membantu pengembang untuk memahami hanya dengan tidak menautkan ke sebuah halaman bukan berarti tidak bisa diakses.

OWASP DirBuster merupakan salah satu pilihan untuk melakukan penetrasi yang di khususkan untuk *server website* terhadap target yang akan diuji coba. Dengan metode *Brute-Force Server* direktori pada *server website*, yang bertujuan untuk mendapatkan informasi data-data yang didapatkan.

3. Hasil dan Pembahasan

3.1 *Scanning* Jaringan Menggunakan W*ifi Analyzer*

Pada bab ini dimaksudkan untuk mengetahui keseluruhan SSID yang di scan oleh Wifi Analyzer. Dengan demikian akan diketahui SSID yang akan di tangkap dan akan dilakukan tahap ujicoba dimana *Wifi Analyzer* dengan metode Riset Lapangan (Field Research) dan Riset Kepustakaan (Library Research) untuk mengumpulkan data dan sebagai acuan tahap ujicoba pada jaringan WLAN dan penmganalisaan konsep implementasi penguat jaringan WLAN pada objek yang di teliti, apakah mengacu pada model pengembangan Network Development Life Cycle (NDLC). Dimana perencanaan dari hasil ujicoba penetrasi yang dilakukan meliputi pengujian dan analisis penyerangan dengan melakukan *Scanning* dan *Probing* (Jivthesh et al., 2022).

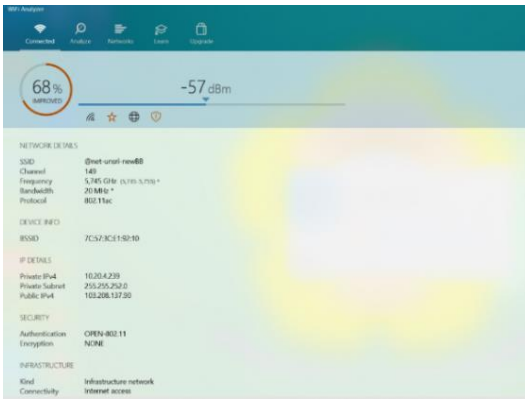
Pada tahap ini penulis mengidentifikasi konsep sistem *wireless* akses *point Alcatel* yang terhubung ke *WLC (Wireless Lan Controller)* sebagai jalur layanan internet dari UNSRI pusat dan *Alcatel* sebagai pemancar jaringan *WLAN* yang ada di Fakultas Kedokteran Universitas Sriwijaya Kampus Madang (Rijadi, 2021). Pada tahap ini penulis megidentifikasi kekuatan sinyal dan juga bahwa ada beberapa lokasi yang didapatkan dalam kondisi kualitas sinyal yang lemah dan titik spot yang didapatkan *blank-spot*, serta penulis juga mendapatkan kurangnya jarak cakupan sinyal koneksi *WLAN* pada Kampus Madang UNSRI dimana kekuatan sinyal yang lemah tersebut didapatkan pada beberapa tempat seperti yang ditujukkan pada tabel 2 berikut ini.

Tabel 2. Tabel pengukuran sinyal di kampus Madang

No.	Gedung	Frekuensi 2,4 (dBm)	Frekuensi 5Ghz (dBm)
1.	Area Parkir Dekanat	-93 dbm	-71 dbm
2.	Kantin	-95 dBm	-91 dBm

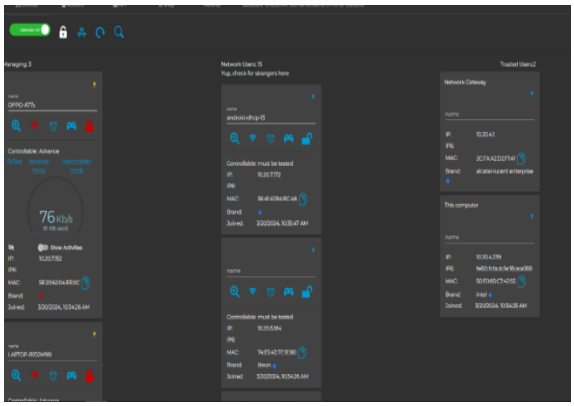
3.2 Pengujian Jaringan *Wireless* Menggunakan Aplikasi *Netcut*

Pada tahap berikut penulis menggunakan aplikasi *Netcut*, yaitu metode *ARP Spoofing ARP Spoofing* pembatasan koneksi terhadap *host* yang *IP Address* yang beroperasi pada system operasi Windows 10. Setelah Sinyal *Wifi* terhubung ke SSID *@net-unsri-newBB*.



Gambar 2. Status kuat sinyal perangkat jaringan yang terhubung

Dengan aplikasi *Wifi Analyzer* ditunjukkan pada Gambar 2, yang sudah mendapatkan IP *Address* 10.20.4.239 pada halaman utama aplikasi *Netcut* akan menampilkan beberapa perangkat *host* yang telah terhubung pada jaringan *wireless* yang sama, dapat dibaca jenis perangkat yang terhubung seperti laptop dan *smartphone.*

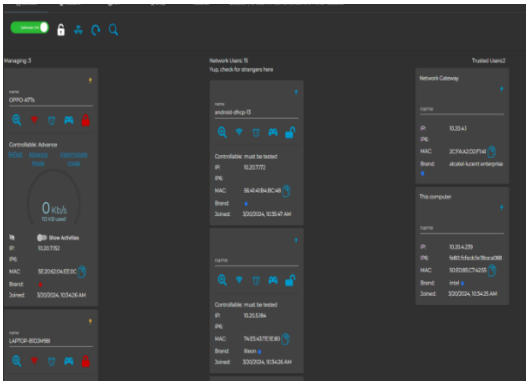


Gambar 3. Ujicoba Penetrasi *terhadap host*

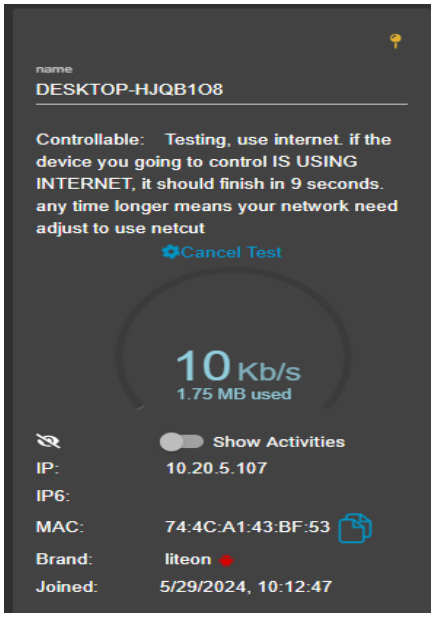
Selanjutnya penulis akan melakukan uji coba seperti ditunjukkan pada Gambar 3 untuk pembatasan *bandwidth* terhadap perangkat yang telah terhubung dengan IP 10.20.7.152. Pembatasan *bandwidth* pada perangkat OPPO-A77s yang sebelumnya terbaca *bandwitdh* sebesar 76 Kb/detik, kemudian saat dilakukan *speed control*, *bandwidth* yang terbaca pada aplikasi *Netcut* yaitu 0 Kb/s, serta log report dari aplikasi *Netcut*.

Tahap selanjutnya pengujian aplikasi *netcut* akan dilakukan pada tempat yang berbeda, penulis akan melakukan ujicoba terhadap target IP 10.20.5.107, saat dilakukan pembatasan kecepatan internet pada target, hanya mendapatkan kecepatan

sekitar yang bervariasi antara 2 Kb/s sampai dengan14 Kb/s. Gambar 4 dan Gambar 5 mengilustrasikan proses ini.

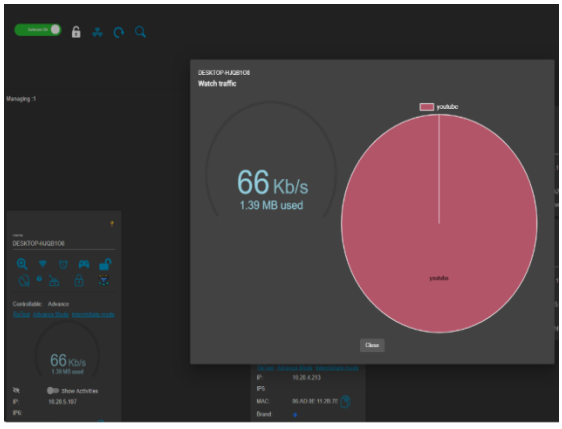


Gambar 4. *Scanning* jaringan *wireless* menggunakan aplikasi *Netcut*



Gambar 5. speed control target 10.20.5.107 menggunakan *netcut*

Monitoring target 10.20.5.107 saat akses *www.yotube.com* diperlihatkan bahwa dengan kecepatan 66 Kb/s dan penggunaan *bandwidth* 1.39 MB. Gambar 6 mengilustrasikan hasil yang dimaksud.



Gambar 6. *Monitoring* target 10.20.5.107 menggunakan *netcut*

Aplikasi *Netcut* menampilkan bahwa beberapa perangkat yang terhubung dapat dilakukan memutuskan internet dan membatasi *bandwidth* target yang terhubung.

3.3 Pengujian *Scanning* menggunakan *Nmap*

3.3.1 *TCP scanning Nmap*

Tahap pertama penulis akan *scanning* target website *fk.unsri.ac.id* dengan mengetikkan perintah di terminal:

"*nmap fk.unsri.ac.id*"

Fungsi tersebut adalah untuk mendapatkan *IP* address dari *website fk.unsri.ac.id*. Dan hasil *scan Nmap IP Public* yang didapat adalah 103.208.137.149. serta menampilkan beberapa *port* yang terbuka dari *IP* target, seperti ditunjukkan pada Gambar 7.

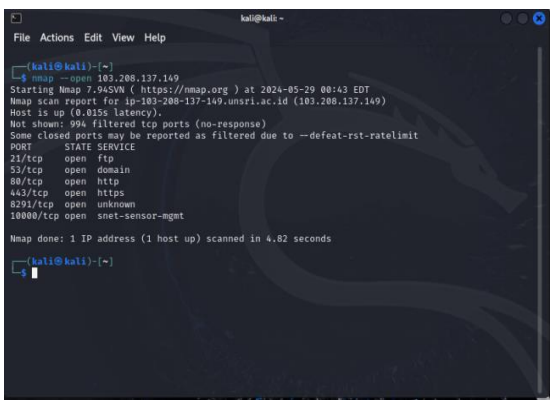
Gambar 7. *tcp scanning nmap target websit*

PORT STATE SERVICE
21/tcp open ftp
53/tcp open domain
80/tcp open http
443/tcp open https
8291/tcp open unknown
10000/tcp open snet-sensor-mgmt

Selanjutnya akan mengetikkan perintah:

"*—open 103.208.137.149*"

Fungsi dari perintah diatas adalah untuk menampilkan *port-port* berapa saja yang terbuka.



Gambar 8. *Scanning port-port* yang terbuka

Hasil pada lampiran Gambar 8 diatas yang ditampilkan hampir sama seperti yang ditampilkan pada Gambar 6 hanya saja dijelaskan:

"Some closed ports may be reported as filtered due to --defeat-rst-ratelimit"

Penjelasan diatas dapat kita artikan bahwa kemungkinan beberapa port yang di tutup oleh administrator (Beardsley, 2010).

Selanjutnya penulis akan mengetikkan perintah "*–reason"* yang artinya penulis akan mengetahui alasan mengapa port-port tersebut terbuka dengan perintah:

nmap –reason 103.208.137.149"

Alasan *port* tersebut terbuka dengan kode *REASON* nya *"syn-ack"* bahwa *port* tersebut tersedia dan siap untuk menanggapi respon terhadap jaringan.

Gambar 9. Status reason pada nmap port-port yang terbuka

3.3.2 *Scanning TCP dan UDP Nmap*

Tampilan dari sisi penyerang setelah melakukan penyerangan menggunakan *Nmap* dengan melakukan *TCP Port scan* terhadap IP 103.208.137.149 dengan mengetikkan perintah pada terminal, seperti ditunjukkan pada Gambar 10.

" nmap –sT 103.208.137.149"

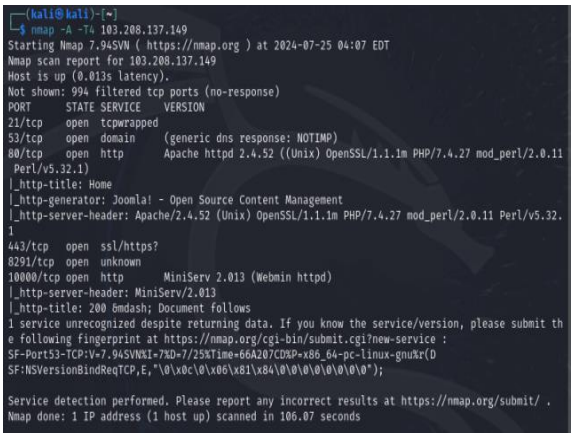
Gambar 10. pemindaian TCP dengan perintah –sT

3.3.3 Pemindaian Target Mendeteksi Sistem Operasi dan Layanan Service

Disini penulis akan melakukan pemindaian target dengan perintah pada termina:

"Nmap –A –T4 103.208.137.149 "

Dengan menggunakan perintah pada terminal parameter "-A" berguna untuk meperlihatkan sistem operasi dan mendeteksi *service* layanan pada waktu bersamaan akan dikombinasikan dengan mengetikkan perintah pada terminal "–T4", untuk tingkat kecepatan agresif *scanning*, dan hasilnya akan diperlihatkan pada Gambar 11.



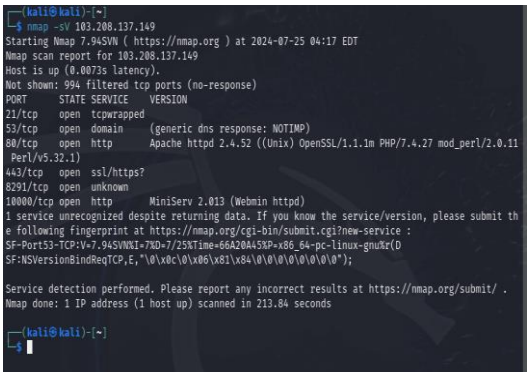
Gambar 11. Perintah pada terminal –A dan T4

3.3.4 Mendeteksi layanan atau versi daemon Nmap

Disini penulis akan mendeteksi layanan yang ada terhadap target dengan mengetikkan perintah pada terminal:

"nmap –sV 103.208.137.149"

Perintah diatas untuk mengetahui layanan yang berjalan pada port yang akan di tampilkan. Hasil yang didapat sama persis dengan perintah yang dilakukan sebelumnya dengan perintah –A dan –T4. Gambar 12 memberikan ilustrasi dari hasil proses ini.



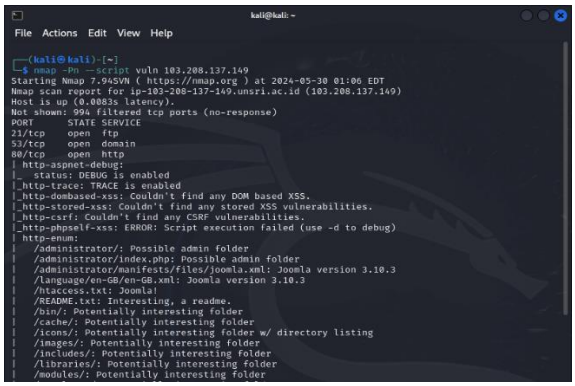
Gambar 12. Mendeteksi versi Daemon target server website

3.3.5 *CVE detection Nmap*

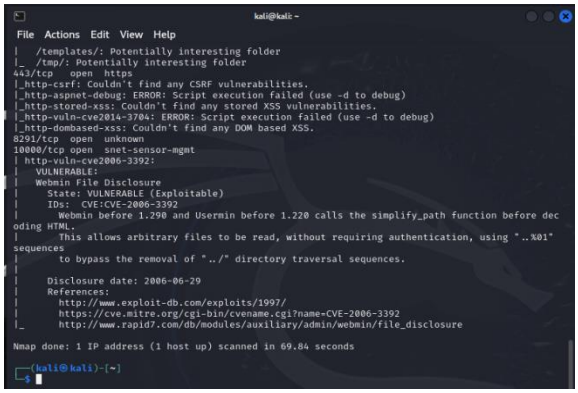
CVE Detection adalah metode yang dilakukan penulis untuk pendeteksian terhadap target dimana fungsi dari perintah tersebut agar memungkinkan untuk menggunakan serangkaian *script* yang telah ditentukan sebelumnya(Engineering et al., 2021). Dengan mengetikkan perintah pada terminal:

"nmap -Pn --script vuln"

Fungsi perintah diatas adalah mencari celah *port service* yang dapat disusupi. Gambar 13 dan Gambar 14 memberikan ilustrasi dari proses ini.



Gambar 13. Perintah *vuln* terhadap target 1



Gambar 14. Perintah *vuln* terhadap target 1

3.3.6 *Brute Force Attack Nmap*

*M*etode yang dilakukan untuk ujicoba pada target *IP* Public 103.208.137.149, dengan mengetikkan perintah pada terminal:

"nmap –script ftp-brute –p 21 103.208.137.149"

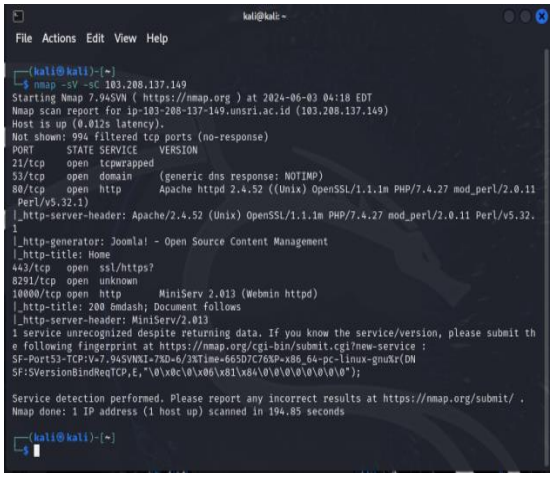
Brute Force tersebut diarahkan pada target IP tujuan dan port tujuan untuk mendapatkan informasi terhadap target. Gambar 15 menampilkan visualisasi proses ini.

Gambar 15. brute force target ip 103.208.137.149

3.3.7 *Nmap FTP login*

FTP Login adalah metode untuk melakukan ujicoba *Anonymous Login* dari *FTP*, jika uji coba *anonymous* tersebut diizinkan, akan daftar *directory* dari *directory* root selanjutnya akan memberikan sorotan file yang akan ditulis seperti Gambar 16.

"nmap -sV -sC 103.208.137.149"



Gambar 16. Nmap *FTP login*

Hasil dari scanning mengindikasikan bahwa pada port 21 menjelaskan servicenya tcpwrapped, yang artinya pada port 21 dilindungi.

"http://103.208.137.149:80"

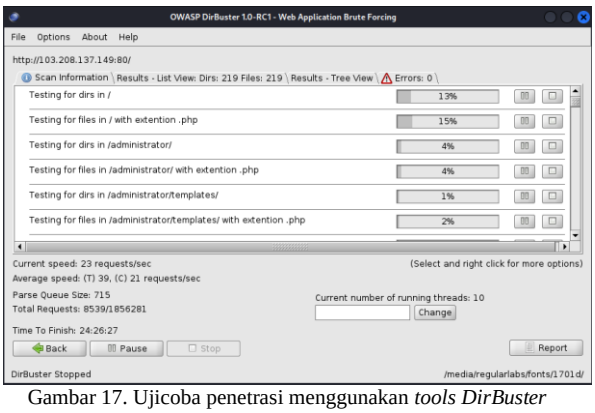
3.3.8 *Combo Scanning Nmap*

Berikut penulis akan menggunakan *flag* –sS untuk melakukan *stealth port scan, "*–sV " yaitu menebak layanan yang sedang berjalan pada *port* yang terbuka dan " –O " untuk menebak system operasi dari target atau juga disebut OS *fingerprinting.*

3.3.9 *OWASP DirBuster*

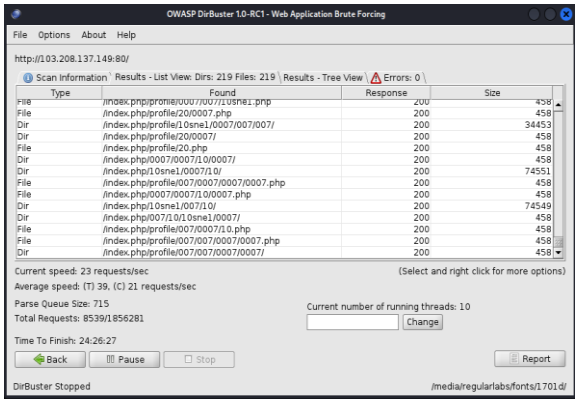
Penulis akan melakukan *Brute Force* menggunakan *tools DirBuster* ke target 103.208.137.149. dan hasilnya akan menampilkan isi dari direktori pada target, seperti diilustrasikan pada Gambar 17.

"http://103.208.137.149:8"



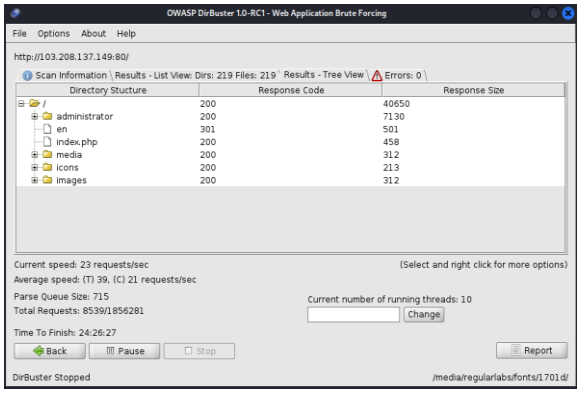
Gambar 17. Ujicoba penetrasi menggunakan *tools DirBuster*

Selanjutnya hasil yang di *scanning* yang ditampilkan adalah *direktori* dan *file* yang didapat, seperti terlihat pada Gambar 18.



Gambar 18. List hasil *scanning* direktori dan *file* target

Dan pada tab *tree direktori* akan menampilkan hasil yang ada pada Gambar 19.



Gambar 19. *Tree View OWASP Dirbuster*

4 Kesimpulan dan Saran

Berdasarkan hasil dari uji coba penetrasi jaringan *wireless* pada Fakultas Kedokteran Kampus Madang Universitas Sriwijaya dengan OWASP Testing Guide versi 4.1 dari modul yang telah di ujicoba, didapatkan beberapa hasil menggunakan tools yang diusulkan dan beberapa ujicoba yang dilewati untuk dilakukan karena tidak memenuhi kriteria pengujian. Pengujian yang berhasil dilakukan kemudian dipilih untuk untuk dilaporkan penulis dapat dilihat pada Tabel 2 di bawah ini.

Tabel 2. Hasil uji coba penetrasi jaringan *wireless*

No	*Software/Tools*	Status	Keterangan
1.	*Wifi Analyzer*	Berhasil	*Scanning* SSID jaringan *Wireless* berhasil dilakukan
2.	*Netcut*	Berhasil	*ARP Spoofing* terhadap *host* berhasil dilakukan
3.	*Nmap*	Berhasil	*Scanning* jaringan berhasil dilakukan, *Brute Force* tidak berhasil
4.	*Digbuster*	Berhasil	*Brute Force* direktori server berhasil dilakukan

Dengan demikian disarankan dalam dilakukan audit keamanan jaringan secara berkala untuk mendeteksi dan memperbaiki potensi kelemahan sebelum dieksploitasi serta mengurangi risiko terhadap berbagai serangan yang berhasil dideteksi melalui tools seperti Wifi Analyzer, Netcut, Nmap, dan Dirbuster sehingga dapat menjaga jaringan tetap aman dari berbagai ancaman.

Daftar Pustaka:

Elizar, A. (2014). IEEE 802.11ac sebagai standar pertama untuk Gigabit Wireless LAN. *Jurnal Teknologi Informasi*, *11*(1), 36–44.

Gustav, M. A., & Pranata, M. (2022). Perancangan dan implementasi jaringan komputer LAN dan WLAN dengan quality of service. *STRING (Satuan Tulisan Riset dan Inovasi Teknologi*, *7*(2), 197.

Arianto, T. (2009). Implementasi Wireless Local Area Network dalam RT/RW Net. *Jurnal Teknologi Informasi*, *XIV*(2), 152–157.

Rijadi, B. B. (2021). Optimasi jaringan Wireless Local Area Network (WLAN) pada model lingkungan perkantoran. *Jurnal Teknologi Informasi*, *1*(1), 1–9.

Jufri, M., Fakultas Ilmu Komputer, & Universitas Internasional Batam. (2021). Peningkatan keamanan jaringan wireless dengan menerapkan that network security is very influential on the prevention of attacks carried out by attackers. *Jurnal Teknologi Informasi*, *5*(2), 98–108.

Cetak, I., & Online, I. (2022). *DECODE: Jurnal Pendidikan Teknologi Informasi*, *2*(1), 1–7.

Vaniamosa, S. K., et al. (2023). Analisis walk test pada cakupan area. *Jurnal Teknologi Informasi*, no. 6, 87–99.

Alfarisi, T. D., & Fatoni. (2023). Analisis dan Implementasi Penguat Jaringan Wireless Local Area Network (WLAN). *JUPITER: Jurnal Penelitian Ilmu Dan Teknologi Komputer*, *15*(1c), 434–443. https://doi.org/10.5281./5510/15.jupiter.2023.04

Waliulu, R. F., Jurusan Teknologi Informatika, & Universitas Dian Nuswantoro. DARI PENGGUNA NETCUT DI JARINGAN LOCAL DENGAN.

Sriwijaya, P. N. (2015). (Ichsan, Putra, Wibisono, dan Studiawan, 2013), 0–5.

Kunci, K., et al. (2023). Penetration Testing Berbasis OWASP Testing Guide Versi 4.2 (Studi Kasus: X Website).

Utama, I. M. P., Putri, K. R., Agung, A., Wirayuda, E., & Tyora, V. A. (2022). Analisis perbandingan kinerja tool website directory brute force dengan target website DVWA. *Jurnal Teknologi Informasi*, *4221*, 278–285.

Purba, W. W., Efendi, R., Fakultas Teknologi, Universitas Satya Negara Indonesia. (2021). Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT. *Jurnal Teknologi Informasi*, *17*(2), 143–158.

Jivthesh, M. R., G. M. R. A. P., H. N. Gd, & Rao, S. N. (2022). A comprehensive survey of WiFi analyzer tools. In *Proceedings of the IEEE Global Conference on Advanced Technologies*. https://doi.org/10.1109/GCAT55367.2022.9972040

Beardsley, T. (2010). The TCP split handshake: Practical effects on modern network equipment. *Jurnal Teknologi Informasi*, *2*(1), 197–217.

Halaman ini sengaja dikosongkan