Jurnal Sistem Komputer dan Kecerdasan Buatan
Volume 5 Nomor 2 Maret Tahun 2022

Analisis Keamanan Jaringan Wpa2-Psk Menggunakan Metode *Penetration Testing* (Studi Kasus : Router Tp-Link Mercusys Mw302r)

Mochamad Adhari Adiguna[1], Bambang Wisnu Widagdo[2]

[1, 2] Program Studi Teknik Informatika, Universitas Pamulang
[1]dosen01864@unpam.ac.id , [2]dosen02092@unpam.ac.id

Diterima : 20 Februari 2022
Disetujui 27 Maret 2022

***Abstract*— Dengan berkembangnya teknologi komunikasi dan informasi melalui komunikasi data tanpa kabel yang dimana keamanan data pada lalu lintas data yang terjadi pada jaringan wireless LAN menjadi sangat penting dan menjadi perhatian, jaringan yang terkoneksi dengan internet pada dasarnya tidak akan aman dan selalu dapat dilakukan ekploitasi oleh cracker atau hacker. Ketika data berkomunikasi pada lalu lintas data dimana data dikirim dan melewati terminal untuk mencapai tujuan, maka pada saat itu pengguna lain yang tidak bertanggungjawab memiliki kesempatan untuk mengubah data dan atau menyadap. Oleh karena itu, merancang jaringan WLAN yang terhubung ke internet harus direncanakan dengan baik agar dapat meminimalisir vulnerability. Kelemahan dari jaringan nirkabel IEEE 802.11 yang menggunakan enkripsi WEP yaitu hacker atau cracker dapat mengetahui kode enkripsinya. Berdasarkan latar belakang tersebut di atas, kami melakukan penelitian ini. Adapun tujuan penelitian ini adalah untuk mengetahui vulnerability atau celah keamanan pada jaringan WPA2-PSK dan untuk mengetahui fitur sistem operasi kali linux dalam menganalisis Router TP-Link Mercusys MW302R dalam keamanan jaringan WPA2-PSK. Metode untuk ujicoba menggunakan metode penetration testing. Metode Penetration testing yang kami gunakan menggunakan sistem operasi kali linux dengan tahapan: Planning and Preparation, Reconnaissance, Discovery, Analyzing information and risk, Active intrusion attempts, Final analysis, Report preparation. Berdasar hasil analisis dan pengujian terhadap sistem operasi pada jaringan yang menggunakan router Tp-Link Mercusys Mw302r, maka dapat ditarik kesimpulan bahwa port http dapat dieksploitasi oleh meterpreter melalui msfconsole pada kali linux dan setiap lalu lintas data pada jaringan, jika dilakukan proses scanning dan discovering selalu dan besar kemungkinan didapat vulnerability atau celah keamanan melalui port yang terbuka.**

Keyword: Analisis Keamanan Jaringan WPA2-PSK, Penetration testing, Kali Linux

I. PENDAHULUAN

A. Latar Belakang Masalah

Sistem keamanan jaringan WLAN (wireless local area network) yang terkoneksi dengan internet harus dipahami dan direncanakan dengan baik agar dapat melindungi asset atau sumber daya yang berada dalam jaringan tersebut secara efektif. Jenis-jenis serangan yang dilakukan oleh para hacker yang biasa dilakukan adalah, Packet sniffer, probe, scan, ARP spoofing / ARP poisoning, Root compromise, Account compromise, Denial of service (Dos) [1].

Dengan pesatnya perkembangan teknologi komunikasi dan informasi melalui komunikasi data tanpa kabel yang dimana keamanan data pada lalu lintas data yang terjadi pada jaringan

wireless LAN menjadi sangat penting dan menjadi perhatian, jaringan yang terkoneksi dengan internet pada dasarnya tidak akan aman dan selalu dapat dilakukan ekploitasi oleh cracker atau hacker. Ketika data berkomunikasi pada lalu lintas data dimana data dikirim dan melewati terminal untuk mencapai tujuan, maka pada saat itu cracker atau hacker memiliki kesempatan untuk menyadap atau mengubah data. Oleh karena itu, merancang sistem keamanan jaringan wlan yang terkoneksi dengan internet harus dapat dipahami dan direncanakan dengan baik. Mekanisme keamanan jaringan wireless awalnya adalah WEP (Wireless Encryption Protocol). WEP merupakan algoritma enkripsi yang dirancang pada tahun 1999 dengan standar 802.11b untuk memberikan keamanan wireless [2]. Kelemahan dari jaringan nirkabel IEEE 802.11 yang menggunakan enkripsi WEP yaitu hacker atau cracker dapat mengetahui kode enkripsinya. Namun, hal tersebut bukan suatu yang tidak mungkin untuk membuat jaringan wireless yang mempunyai tingkat keamanan yang lebih baik melalui kombinasi keamanan standar terbuka dari jaringan wireless tersebut dan keamanan yang dimiliki perangkat itu sendiri. Untuk menyikapi kelemahan dari WEP telah dikembangkan suatu teknik pengamanan baru yang disebut WPA (Wi-FI Protected Access). Teknik WPA merupakan model dari keamanan yang kompatibel dengan draft standar 802.11i yang mana masih dalam proses pengembangan untuk menggantikan standar 802.11. Pada teknik keamanan WPA, selain pengembangan dari proses enkripsi juga menambahkan proses user authentication yang tidak ada pada pada WEP. Menurut Desi Maya Sari, dkk., Proses otentifikasi pada WPA menggunakan 802.1X dan EAP (Extensible Authentication Protocol) [3].

Meskipun sebagian pengguna tidak peduli dengan keamanan komunikasi data di tempat publik, dimana cracker melakukan uji coba illegal melalui jaringan wireless, kami tetap berusaha menganalisis celah keamanan yang kemungkinan terjadi pada jaringan wireless. Jaringan wireless lebih rentan dibanding jaringan kabel [4]. Karena Jaringan wireless lebih rentan dibanding jaringan kabel, maka diperlukan suatu metode yang dapat melakukan ujicoba apakah jaringan wireless yang telah terpasang sesuai standar atau belum. Karena hal tersebut berkaitan dengan kemanan jaringan wireless yang digunakan.

Metode untuk melakukan ujicoba tersebut disebut dengan metode pentest atau penetration testing. Metode pentest adalah metode dimana dilakukan proses percobaan menyerang pada sistem yang digunakan, yang dimana diperlukan sertifikasi keamanan jaringan untuk mencegah cracker dan atau hacker yang dapat menyebabkan kehilangan data dan asset sistem target. Pentester adalah sebutan orang yang melakukan metode tersebut [5]. Dalam setiap pengujian, diperlukan persetujuan dari pemilik sistem, jika hal tersebut tidak dilakukan maka pengujian tersebut disebut sebagai tindakan yang illegal atau di-hack. Hasil dari test pentest sangat penting bagi administrator jaringan untuk meningkatkan keamanan sistem melalui celah keamanan yang berhasil diketahui.

Metode Penetration testing yang akan kami gunakan menggunakan sistem operasi kali linux 2020.2. Kali linux merupakan sistem operasi distribusi Linux tingkat lanjut untuk melakukan pengujian keamanan, audit keamanan dengan penetration testing [6].

B. Rumusan Masalah

Berdasarkan latar belakang di atas maka kami merumuskan permasalahan dalam penelitian ini yaitu:

1. Bagaimana Metode Penetration testing dalam mengevaluasi pada analisis keamanan jaringan WPA2-PSK?
2. Bagaimana fitur sistem operasi kali linux dalam menganalisis Router TP-Link Mercusys MW302R untuk keamanan jaringan WPA2-PSK?

C. Tujuan

Berdasar dari rumusan masalah yang telah dipaparkan, tujuan penelitian ini adalah:

1. Untuk mengetahui vulnerability atau celah keamanan pada jaringan WPA2-PSK yang digunakan pada RT RW Net di perumahan Taman Rahmani, dimana router yang digunakan adalah Tp-Link Mercusys Mw302r.

2. Untuk dapat menggunakan dan mengetahui fitur sistem operasi kali linux dalam menganalisis Router TP-Link Mercusys MW302R untuk keamanan jaringan WPA2-PSK khususnya penggunaan msfconsole dan meterpreter pada msfconsole.

D. Manfaat

1. Manfaat Teoritis

   Secara teoritis hasil penelitian ini akan menambah wawasan dan ilmu pengetahuan khususnya bagi para administrator jaringan dalam perancangan keamanan sistem jaringan WPA2-PSK, khususnya pada Router TP-Link Mercusys MW302R.

2. Manfaat Praktis

   Manfaat secara praktis dari penelitian ini yakni diharapkan mampu memberikan manfaat: Bagi praktisi administrasi jaringan, penelitian ini diharapkan mampu memberikan pengetahuan celah keamanan pada jaringan WPA2 –PSK. Bagi peneliti selanjutnya, hasil penelitian ini dapat dijadikan literasi dalam mengembangkan penelitian-penelitian lain yang sejenis.

II. KAJIAN PUSTAKA

A. Keamanan Jaringan WLAN

Penelitian yang terkait keamanan jaringan telah berkembang dari beberapa aspek referensi yang berkaitan dengan subjek pertanyaan telah diperoleh. Penelitian tersebut meliputi:

Penelitiannya yang berjudul "Penetration testing Pada Jaringan Wifi Menggunakan Kali Linux" menjelaskan bahwa dikarenakan kemudahan untuk instalasi jaringan nirkabel, sangat rentan terhadap gangguan keamanan eksternal. Enkripsi ganda ini telah diterapkan untuk melindungi kemanan jaringan wireless ini. Namun, enksripsi ini mudah dipecahkan oleh cracker atau hacker. Berdasar hal tersebut, maka perlu ditingkatkan keamanan jaringan di perusahaan tersebut [6].

Pada penelitannya yang berjudul "Analisis Sistem Keamanan Jaringan Wireless (WEP,WPAPSK/WPA2PSK) MAC Address, Menggunakan Metode Penetration testing" menjelaskan bahwa sebuah jaringan bisa dikatakan aman harus memenuhi enam persyaratan, yaitu kerahasiaan yang hanya bisa diakses oleh pihak yang berwenang dan cegah pihak yang tidak berwenang membaca informasi rahasia dan harus aman. Lalu integritas yang pastikan data yang diterima tetap tidak berubah selama transmisi, baik itu dimodifikasi, didpulikasi atau dikembalikan. Layanan keamanan disediakan memerlukan otentikasi, untuk memastikan identitas pengguna yang berkomunikasi di jaringan yang benar. Kemudian memerhatikan kejadian yang tidak terjadi penyangkalan, ketersedian dan akses kendali [3].

Penelitannya yang berjudul "Analisis Keamanan Jaringan WLAN Dengan Metode Penetration testing" menggunakan metode penetration testing sebagai bentuk simulasi serangan yang akan terjadi atau mencari celah keamanan di jaringan wireless [7]. Dimana, tujuan dari penetrasi testing adalah untuk melindungi organisasi yang diuji. Karena dengan hasil uji penetrasi yang didapat, organisasi tersebut dapat mengurangi dan mengidentifikasi kerentanan yang terdeteksi. Tahapan pertama dari metode ini adalah planning, pada tahapan ini, selain mendapatkan persetujuan dari manajemen atas proses pengujian, penyelesaian ruang lingkup pengujian dan catatan yang terdokumentasi, aturan dalam pengujian juga diidentifikasi, dan akhirnya target pengujian ditentukan [4]. Tahap planning menetukan berhasil tidaknya uji penetrasi yang akan dilakukan dan belum ada uji teknis. Tahapan penetration testing yang dibahas dalam penelitian ini adalah planning, Discovery, attack and reporting.

Penelitiannya yang berjudul "Metode Penetration testing pada Keamanan Jaringan Wireless Wardriving PT. Puma Makmur Aneka Engineering Bekas" menjelaskan bahwa mengidentifikasi kerentanan keamanan dalam keadaan terkendali, sehingga dapat menghapusnya. Para pentester sistem menggunakan pengujian pentesting untuk memecahkan masalah yang ada dan melekat

dalam penilaian kerentanan, dengan fokus sensitivitas terhadap tingkat vulnerability yang tinggi. Pengujian penetrasi adalah alat penilaian nilai yang bermanfaat bagi bisnis dan operasinya [8].

Penelitannya yang berjudul "Keamanan Jarıngan WLAN Terhadap Serangan Wireless Hackıng Pada Dınas Komunıkası & Informatıka DIY" pengujian ini didasarkan pada konsep nirkabel serangan peretasan, termasuk spoofing ARP dan cracking WPA2-PSK. Hasil dari pengujian di Biro Komunikasi dan Informasi DIY pada jaringan WLAN berkesimpulan bahwa sistem keamanan jaringan yang digunakan memiliki celah keamanan yang masih ada dibeberapa jaringan Wi-Fi yang harus ditingkatkan dan juga perlu mengaktifkan fungsi ARP [9]. Berdasarkan penelitian yang telah dilakukan oleh peneliti sebelumnya maka kami berencana melaksanakan penelitian mengenai "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration testing". Selanjutnya kami harus memenuhi enam persyaratan sebagai syarat dalam keamanan jaringan seperti pada [3]. Pengujian keamanan jaringan ini dilakukan untuk menghindari jenis-jenis serangan yang ada pada [8]. Pengujian ini dilakukan pada WPA2-PSK untuk mengetahui celah-celah keamanan yang masih ada pada jaringan wireless seperti di penelitian [9]. Lalu kami melakukan pengujian, menggunakan tools yang tersedia di sistem operasi kali linux pada Router TP-Link Mercusys MW302R.

B. Kali Linux

Kali Linux merupakan operating system berbasis linux debian yang dikembangkan oleh offensive Security. User interface dari Kali Linux memiliki tampilan graphical user interface (GUI) yang sederhana dan tidak terlalu mencolok. Kali Linux, Selain terdapat di PC, juga dapat diinstalasi dan konfigurasi pada sistem Android yang disebut Kali Nethunter yang memiliki fungsi dan fitur yang sama. Kali Linux adalah salah satu distribusi Linux tingkat lanjut untuk melakukan Penetration testing dan audit keamanan. Kali Linux merupakan pengembangan dari sistem operasi BackTrack. BackTrack adalah distro Linux yang diciptakan secara khusus untuk memenuhi keperluan dalam pengujian dan penetration testing pada sebuah sistem serta keamanan pada komputer. Offensive Security, lembaga yang mengembangkan dan mendanai Kali Linux. Backtrack merupakan pendahulunya kali linux. Saat ini ada lebih dari 300 tools yang harus di penetration testing dalam Kali Linux [6]. Fitur-fitur dari Kali Linux adalah sebagai berikut:

1) Tools penetration testing > 300
2) Free Licensed
3) Mengikuti FHS compliant
4) Support perangkat wireless
5) IDE yang aman
6) Support dengan banyak bahasa

Banyak tools security dan pentest dalam Kali Linux, seperti: Nmap, Metasploit Framework, Aircrack-ng, wifite, routerSploit, Kismet, Wireshark, Burp suite, John the Ripper, OWASP ZAP, Ettercap, Maltego, dan Social Engineering Toolkit.

C. Router TP-Link Mercusys MW302R

Router Mercusys MW302R adalah sub-brand dari TP-Link yang kelebihan utamanya adalah mampu menyediakan koneksi WiFi dengan kecepatan hingga 300 Mbps dan Multi-Mode.

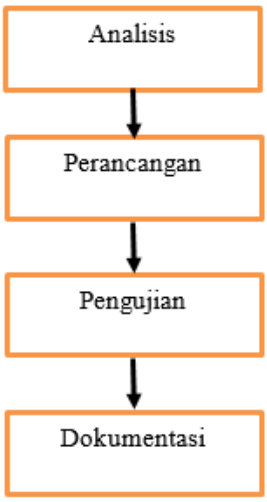
Hardware dari perangkat memiliki dimensi 11,4 x 9,4 x 2,6 cm terdiri dari panduan instalasi singkat, power adaptor dan kabel ethernet. Mercusys MW302R dilengkapi dua antena eksternal high-gain dengan 5dBi untuk mengirimkan sinyal WiFi yang kuat, sehingga tidak ada lagi ruangan yang tidak terkena sinyal WiFi. Router memiliki port di bagian belakang yang terdiri dari Ethernet Ports, yakni dua port 10/100Mbps LAN Ports dan satu port 10/100Mbps WAN Port. Lalu Reset Button serta External Power Supply 5V/0.6A.

Mercusys MW302R memiliki keunggulan empat mode dalam satu perangkat. Yakni, Mode Router , Mode Access Point, Mode Range Exterder, dan Mode WISP. Selain itu, Mercusys MW302R dilengkapi Parental Control untuk memantau penggunaan internet [10].

III. METODE PENELITIAN

Metode adalah kerangka berfikir atau kerangka kerja untuk melakukan tindakan dalam menyusun suatu hipotesa dan gagasan yang terarah dan sesuai maksud dan tujuan dari latar belakang penelitian. Metode penelitian yang sesuai dapat terasa pada proses penelitian dan hasil yang didapat.

A. Metode Pengumpulan Data



Gambar 1. Prosedur Penelitian

Pada prosedur penelitian, proses pengumpulan data digunakan untuk mendapatkan data yang relevan, agar hasil yang dicapai sesuai dengan maksud dan tujuan dari penelitian. Kami melakukan langkah penelitian sebagai berikut:

1. Analisa

   Analisa merupakan metode awal dalam melakukan penelitian, analisa digunakan untuk menganalisis rancangan jaringan yang ada pada lokasi penelitian.

2. Perancangan

   Perancangan merupakan metode kedua, dimana tahap ini mampu menerjemahkan spesifikasi kebutuhan perangkat lunak sistem operasi kali linux untuk diimplementasi pada metode analisa.

3. Pengujian

   Metode ketiga, yakni tahap pengujian penetration testing untuk mendapatkan hasil dan menemukan celah keamanan.

4. Dokumentasi

   Metode selanjutnya adalah dokumentasi, pada proses ini, yakni melakukan studi pustaka, mempelajari jurnal yang relevan serta sumber lain yang berkaitan dengan penelitian untuk dijadikan referensi.

B. Metode Penetration Testing

Penetration testing adalah serangan jaringan yang disimulasikan pada sistem komputer untuk menemukan kerentanan, ancaman, dan resiko dalam sistem dan aplikasi perangkat lunak, jaringan atau aplikasi web yang dapat digunakan penyerang. Dalam keamanan jaringan wireless, pentesting sering digunakan untuk menambahkan firewall pada router. Vulnerability atau kerentanan adalah sebuah resiko resmi bahwa penyerang dapat mengganggu atau mendapatkan sistem dan data apapun yang ada pada sumber daya target. Dalam tahap pengembangan dan implementasi sistem, Vulnerability sering kali dimasukkan secara tidak sengaja. Vulnerability umum termasuk kesalahan desain atau konfigurasi, kesalahan perangkat lunak dan lainnya.

Tujuannya untuk menemukan kemungkinan celah resiko keamanan yang ada pada sistem. Kesalahan yang sering terjadi terdapat pada kesalahan konfigurasi, kesalahan perangkat lunak dan lainnya. Pengujian penetrasi dapat mengevaluasi kemampuan perlindungan sistem jaringan dan user dari ancaman eksternal dan internal. Penetration testing dilakukan dalam kondisi ketika sistem keamanan menemukan ancaman baru dari cracker atau hacker, memperbarui sistem dan mempersiapkan program startegi kebijakan baru atau end-user. Langkah-langkah yang kami ambil dalam kegiatan penetration testing adalah sebagai berikut:

Gambar 2. Metode Penetration testing

1. Planning and Preparation

   Tentukan ruang lingkup dan tujuan dari pengujian, termasuk didalamnya sistem yang akan diuji dan metode yang digunakan. Kumpulkan data(misalnya nama jaringan dan domain server, server email) untuk lebih memahami cara kerja target dan pontensi kerentanan. Langkah pertama adalah selama proses pengujian dalam rencana awal dan pekerjaan persiapan berfokusk pada menentukan kerentanan dan melakukan perbaikan keamanan secara bertahap.

2. Reconnaissance

   Reconnaissance atau biasa disebut sebagai aktivitas mengumpulkan data yang selanjutnya diklarifikasikan sebagai data pasif dari pengujian penetrasi karena mengumpulkan data secara manual, melalui dokumen terkait atau informasi publik atau bertanya langsung kepada pihak-pihak yang terlibat langsung dengan sistem.

3. Discovery

   Discovery adalah langkah mengumpulkan informasi menggunakan alat otomatis untuk memindai sistem untuk menemukan kerentanan, termasuk memindai jaringan, server, perangkat dan data. Langkah selanjutnya adalah memahami bagaimana target akan merespon berbagai upaya intrusi.

4. Menganalisis informasi dan risiko (Analyzing information and risk)

   Merupakan tahapan analisis informasi secara detail resiko yang diperoleh sebelumnnya(fase Reconnasisssance dan Discovery) dan celah keamanan yang mungkin disebabkan oleh kerentanan pada sistem yang di-install.

5. Upaya intrusi aktif (Active intrusion attempts)

   Tahapan ini adalah tahap dimana beberapa intruksi diberikan secara aktif dari sisi keamanan sistem, sehingga vulnerability yang ditemukan dapat diperbaiki atau ditingkatkan.

6. Analisis Akhir

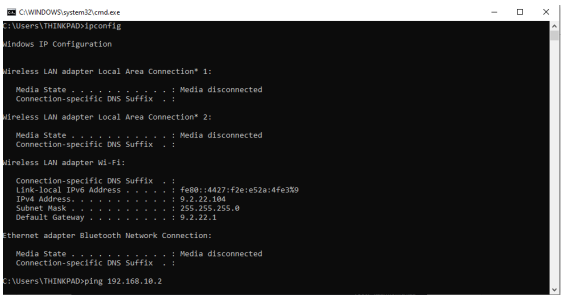
   Analisis akhir secara keseluruhan menggambarkan semuaa temuan dan setelah adanya rencana analisis yang sistematis, petunjuk teknis untuk meningkatkan keselamatan.

7. Persiapan laporan

   Tahapan terakhir dari kegiatan penetrasi testing ini adalah memberikan laporan hasil dari investigasi yang diberikan kepada semuaa pihak yang terkait dan bertanggung jawab atas sistem yang digunakan sebagai acuan untuk meningkatkan sistem keamanan.

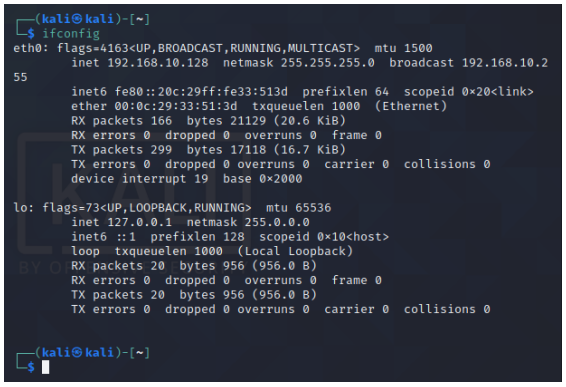
IV. IMPLEMENTASI DAN EVALUASI

Sesuai dengan metode penelitian yang digunakan, tahapan awal yang kami lakukan adalah metode pengumpulan data yang dilanjutkan dengan metode penetration testing melalui pengecekan alamat ip (internet protokol) yang dimiliki setiap perangkat yang dilanjutkan dengan proses scanning dan discovering untuk identifikasi port-port yang terbuka dan services yang berjalan pada port tersebut yang melibatkan system port pada TCP dan UDP. Adapun status port yang dikenali scanning oleh Nmap, yakni: open, open|filtered, closed, closed|filtered, filtered, unfiltered. Cek ip windows dan untuk mengetahui ip router:



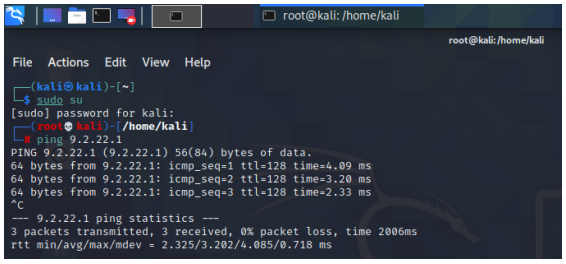
Gambar 3. Cek ip windows dan router

Dari pengecekan ip yang dilakukan dengan perintah ipconfig pada sistem operasi windows, didapat ip window 9.2.22.104 dengan subnet mask 255.255.255.0, sedangkan ip router 9.2.22.1. Selanjutnya mengecek ip kali linux:



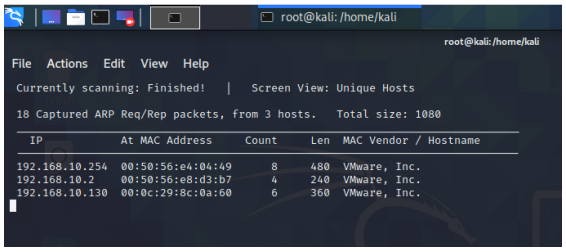
Gambar 4. Cek ip Kali Linux

Melalui pengecekan tersebut didapatkan ip dari kali linux adalah 192.168.10.128 dengan netmask 255.255.255.0, hal ini menyebabkan kami mengetahui jenis jaringan yang digunakan, yakni jaringan kelas C. Untuk bukti koneksi, kami buktikan dengan perintah ping.

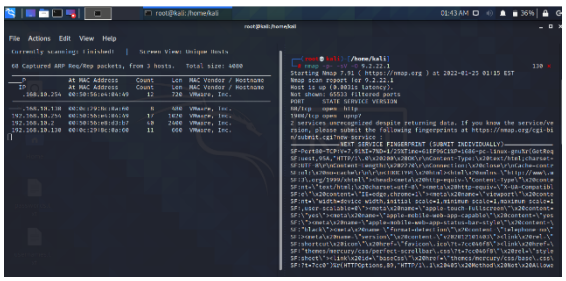


Gambar 5. Ping ke ip router

Setelah diketahui ip dari perangkat-perangkat dan jaringan terkoneksi, kami lanjutkan dengan proses scanning dan discovering jaringan yang dilewati dengan perintah sudo netdiscover –r 9.2.22.0/24 dan perintah nmap -p- -sV –O 9.2.22.1.



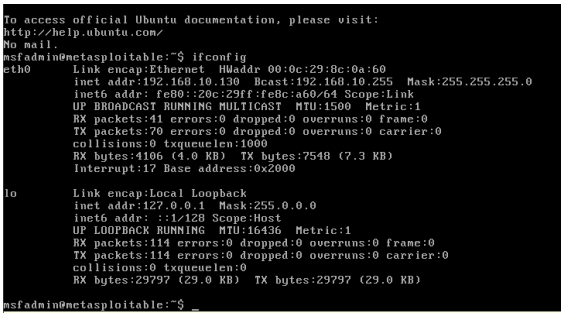
Gambar 6. Proses Discovery



Gambar 7. Proses Scanning

Dari gambar tersebut didapat analisa bahwa port http port 80/tcp dan port upmp 1900/tcp statusnya open.

Setelah dilakukan proses scanning dan discovering, kami lanjutkan dengan pengujian port http yang ada pada sistem operasi metasploitabe, dimana ip dari metasploitable adalah 192.168.10.130 netmask 255.255.255.0.



Gambar 8. Ipconfig metsploitable

untuk mengeksploitasi PORT 80 HTTP, kami gunakan kode berikut:

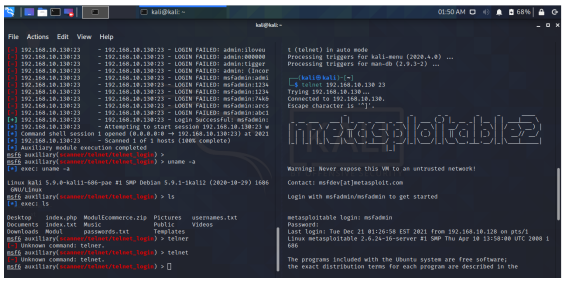
```
cek ip target di browser
cek phpinfo
cek akun password
cek robots.tx
masuk kali:
cek service postgresql status
msfconsole
use auxiliary/scanner/http/http_version
show options
set RHOSTS <<ip_target>>
run
searchsploit <<versi apache>> | grep php
grep cgi search php 5.4.2
use 1
show options
set RHOSTS <<ip_target>>
run

sysinfo
pwd
getuid
```

Selanjutnya setelah diketahui uid dan pwd meta, eksploitasi dilakukan oleh program

meterpreter, meterpreter biasa disebut daemon/setan dimana sebuah kode shell yang digunakan oleh cracker atau hacker untuk membuat trojan atau shell untuk menyusup masuk ke dalam sistem, dalam hal ini meterpreter digunakan untuk mengambil akses administrator.

Dari hasil analisa dan pengujian yang kami lakukan, sistem operasi metasploitable dapat dieksploitasi.



Gambar 9. Proses Eksploitasi

V. SIMPULAN

Berdasar hasil analisis dan pengujian terhadap sistem operasi pada jaringan yang menggunakan router Tp-Link Mercusys Mw302r, maka dapat ditarik kesimpulan sebagai berikut:

1. Setiap lalu lintas data pada jaringan, jika dilakukan proses scanning dan discovering selalu dan besar kemungkinan didapat vulnerability atau celah keamanan melalui port yang terbuka.
2. Port http dapat dieksploitasi oleh meterpreter melalui msfconsole pada kali linux.

DAFTAR PUSTAKA

[1] I. M. S. Achmad Rizal Fauzi, "Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids," *Jurnal Manajemen Informatika Volume 8 Nomor 2,* pp. 11-17, 2018.

[2] A. S. Y. I. Muhammad Farhan Fauzan, "Wireless Attack : Menggunakan Tools Aircrack Pada Kali Linux Untuk Melakukan Wpa Attack," *Jurnal Lentera Vol. 20 No. 1,* pp. 63-74, 2021.

[3] M. Y. L. B. A. Desi Maya Sari, "Analisis Sistem Keamanan Jaringan Wireless (Wep, Wpapsk/Wpa2psk) Mac Address, Menggunakan Metode Penetration Testing," *semanTIK volume 3 no 2 ISSN : 2502-8928,* pp. 203-208, 2017.

[4] A. K. Haeruddin, "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : TP-Link Archer A6)," *CoMBInEs Volume 1 No 1,* pp. 508-515, 2021.

[5] R. F. I. W. Muhammad Mushlih, "Penetration Testing Tool Untuk Menguji Kerentanan Sql Injection Secara Otomatis Berbasis Web," in *Prosiding Seminar Nasional Riset Terapan (SNRT) Vol 4*, Banjarmasin, 2019.

[6] D. P. M. I. Rusdi, "Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux," *Seminar Nasional Teknologi Informasi dan Komputer (SEMANTIK),* pp. 260-269, 2019.

[7] M. Y. L. F. A. Imam Kreshna Bayu, "Analisa Keamanan Jaringan Wlan Dengan Metode Penetration Testing (Studi Kasus: Laboratorium Sistem Informasi dan Programming Teknik Informatika UHO," *semanTIK, Vol.3, No.2 ISSN : 2502-8928,* pp. 69-78, 2017.

[8] R. P. R.W. Ismail, "Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT . Puma Makmur Aneka Engineering Bekasi," *Jurnal Mahasiswa Bina Insani Vol 5 No 1,* pp. 53-62, 2020.

[9] J. T. E. S. M Gilang Hari Wibowo, "Keamanan Jaringan Wlan Terhadap Serangan Wireless Hacking Pada Dinas Komunikasi & Informatika Diy," in *PROSIDING SENSEI 2017 Vol 1 No 1*, Jember, 2017.

[10] F. Hidayat, "TP-Link Kenalkan Tiga Teknologi Baru untuk Memperluas Sinyal Internet," 30 Oktober 2021. [Online]. Available: https://www.beritasatu.com/digital/847423/tplink-kenalkan-tiga-teknologi-baru-untuk-memperluas-sinyal-internet.