JURNAL DEVICE, VOL. 12 NO 2, 160-168
ISSN (print) : 0216-9185

PENGUJIAN KEAMANAN JARINGAN MENGGUNAKAN METODE PENETRASI TES PADA JARINGAN SMK MUHAMMADIYAH 1 WONOSOBO

Muhamad Fuat Asnawi[1)], M. Agung Nugroho[2)]

[1,2)] Universitas Sains Al-Quran
Email : fuatasnawi@unsiq.ac.id [1)], agungmizima@gmail.com[2)]

ABSTRAK

Keamanan jaringan komputer yang ada di SMK Muhammadiyah 1 Wonosobo, belum pernah dilakukan pengujian. Maka dari itu di perlukan tindakan untuk menguji bagaimana keamanan jaringan komputer sekolah saat ini. Metode yang di gunakan adalah penetration testing. Proses simulasi serangan ke komputer server melalui port 80, 445 dan method TCP, HTTP dari hasil mapping sebelumnya hasilnya Failed. Sedangkan serangan ke Routerboard 1 kali hasilnya langsung Success. Dari kedua perangkat tersebut komputer server lebih baik keamanannya karena mempunyai Firewall yang selalu terupdate, sedangkan Routerboard yang jarang di update sangat mudah terkena serangan.

Kata Kunci : pentest, simulasi serangan, DDoS attack, keamanan jaringan

ABSTRACT

Computer network security in SMK Muhammadiyah 1 Wonosobo has never been tested. Therefore, action is needed to test how the security of the school's computer network is today. The method used is penetration testing. The process of simulating attacks on server computers via ports 80, 445 and the TCP, HTTP methods from the previous mapping results is Failed. Meanwhile, an attack on Routerboard 1 time results in immediate success. Of the two devices, the server computer has better security because it has a Firewall that is always updated, while the Routerboard, which is rarely updated, is very vulnerable to attacks.

Keywords: pentest, attack simulation, DDoS attack, network security.

1. PENDAHULUAN

Hampir setiap siswa sudah mahir dalam bidang teknologi, kemudian maraknya tentang hacker saat ini, dan belum pernah diuji keamanan jaringan. Keamanan jaringan komputer yang ada di SMK Muhammadiyah 1 Wonosobo, belum pernah dilakukan pengujian. Maka dari itu di perlukan tindakan untuk menguji bagaimana keamanan jaringan komputer sekolah saat ini. Dengan menggunakan metode Penetration Testing. Para hacker atau peretas melancarkan aksi illegalnya melalui jaringan wireless yang tersedia di SMK Muhammadiyah 1 Wonosobo. Karena jaringan wireless lebih rentan di banding dengan jaringan kabel (Sabdho, 2018). Oleh karena itu, kita membutuhkan sebuah metode untuk melakukan pengujian pada jaringan SMK Muhammadiyah 1 Wonosobo. Metode yang akan di gunakan adalah metode penetration testing (Ismail, 2020).

Namun dikarenakan perkembangan teknologi yang sangat pesat, terdapat berbagai tindakan cybercriminal yang dapat merugikan pihak tertentu atau perorangan. Sehingga tindakan ini sangat di cekam dikalangan masyarakat atau komunitas. Tindakan ini bisa dilakukan oleh perorangan atau organisasi, tindakan ini dinamakan hacker (Ketaren, 2016). Hacker melakukan berbagai macam kegiatan yaitu meneliti, menganalisis, memodifikasi, dan membobol sebuah sistem atau jaringan. Setelah data diambil, maka dapat di perjual belikan di dark web atau dapat di gunakan untuk tindak kejahatan atau penipuan (Kurniawan, 2022).

Metode penetration testing adalah metode yang digunakan untuk mengevaluasi keamanan sistem dan jaringan komputer (Bayu, 2017). Pengujian Penetration Testing adalah proses simulasi serangan pada sistem yang membutuhkan sertifikasi keamanan jaringan untuk mencegah peretas atau penyerang jaringan yang menyebabkan kerugian, baik data personal maupun data sebuah perusahaan (Sanjaya, 2020). Orang yang melakukan metode ini bisa juga disebut sebagai Pentester (Haeruddin, 2021). Saat pengujian ini perlu adanya persetujuan oleh pemilik sistem, jika tidak disetujui maka bisa disebut sebagai tindakan illegal atau hacking (Kurniawan, 2021). Hasil uji pentest ini sangat penting sebagai umpan balik untuk administrator sistem dan jaringan untuk memperbaiki tingkat keamanan sistem di sekolahan tersebut.

Berdasarkan penjabaran diatas ini, penulis melakukan penelitian dengan judul "Pengujian Keamanan Jaringan Menggungakan Metode Penetration Testing Pada Jaringan Smk Muhammadiyah 1 Wonosobo."

2. METODE

a. Metode yang digunakan untuk *pentest* (Pohan, 2021) :
   1. *Planning and reconnaissance*
   2. *Scanning*
   3. *Gaining access*
   4. *Maintaining access*
   5. *Analysis*

b. Sasaran penelitian menargetkan jaringan komputer server sebagai bahan pengujian

c. Metode Pengumpulan Data dengan Dokumentasi, Studi Pustaka, Browsing Internet, dan Wawancara.

d. Analisa *system*
   Kebutuhan perangkat yang akan digunakan dalam pengujian keamanan jaringan di SMK Muhammadiyah 1 Wonosobo :
   1. Perangkat Keras (*Hardwere*)
      Perangkat keras yang di butuhkan :
      - Satu laptop dan satu komputer server, kemudian laptop yang terinstall *system* operasi Kali Linux guna untuk melakukan percobaan terhadap komputer server.
      -1 pcs hub sebagai penghubung jaringan.
   2. Perangkat Lunak (*Softwere*)
      Perangkat lunak yang di butuhkan dalam pengujian saat ini :
      - DDoS *Attack* sebagai *tools* untuk mengirim permintaan paket ke server secara banyak (*overload*).

- NMAP untuk megetahui IP *address* yang terbuka.
- Wireshark sebagai *tools* untuk memantau paket yang dikirim dan diterima.

Perangkat yang digunakan mempunyai spesifikasi sebagai berikut :

Laptop :
- Intel core i3 2,4Ghz
- Memori Ram 2Gb
- Hardis 500Gb sebagai penyimpan data
- Ssd 128Gb sebagai *system operasi*

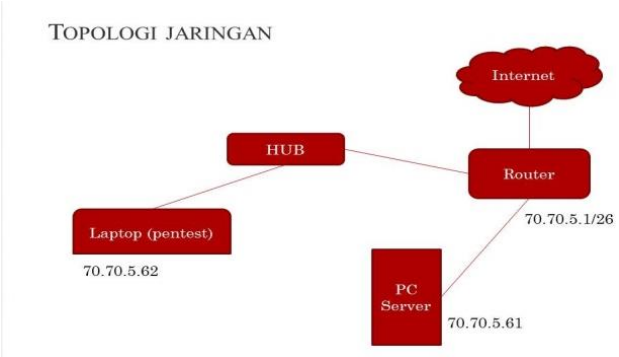
Komputer server
- Amd Ryzen 5 5300
- Memori ram 16Gb
- Ssd NvMe 128Gb (OS)
- Hdd 500Gb (data file internal)
- Hdd 1Tb (data sharing)
- Routerboard RB 750 r2

3. HASIL DAN PEMBAHASAN

Berikut adalah proses pengujian keamanan jaringan komputer di SMK Muhammadiyah 1 Wonosobo menggunakan metode pestest.

3.1 Implementasi Penelitian

Berikut adalah proses pengujian keamanan jaringan komputer di SMK Muhammadiyah 1 Wonosobo menggunakan metode *pestest*.



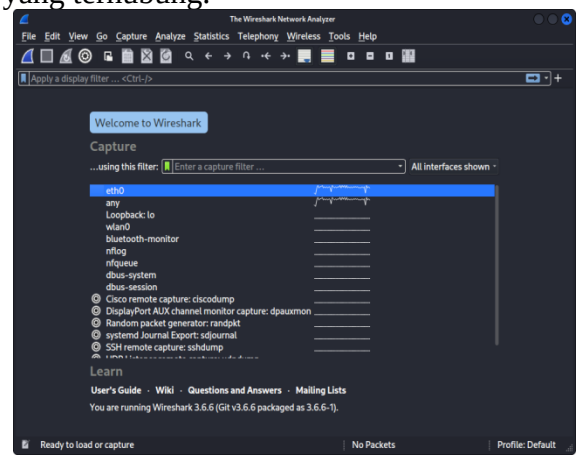
Gambar 1. Topology

3.2 Simulasi Pengujian

Metode pentesting yang akan penulis lakukan diantaranya *information gathering* dan *analysis* menggunakan *Wireshark, vulnerability detection* menggunakan NMAP, *penetration attempt* menggunakan LOIC *(Low Orbit Ion Cannon)*. berikut adalah penjelasan pengujian:

1. *Packet Sniffer (Wireshark)*

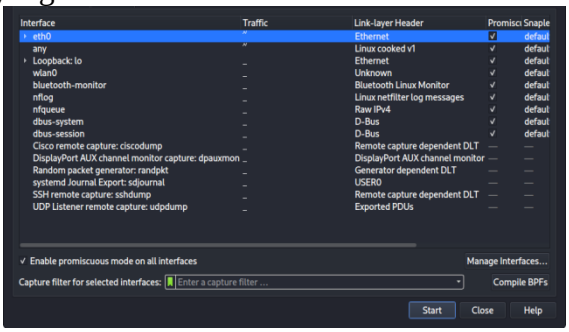
Tahap pertama, penulis menggunakan tools Wireshark untuk mendapatkan informasi dan analisa aktivitas perangkat yang terhubung.



Gambar 2. Tampilan awal *interface* yang aktif

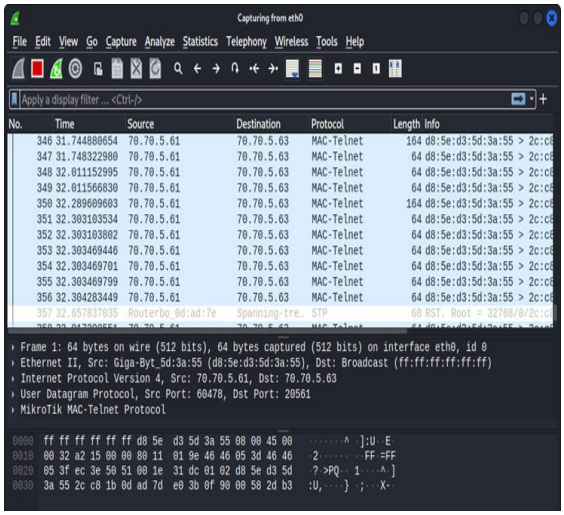
Pada tampilan awal ini, pengguna di suruh memilih interface yang akan di gunakan, bisa di perhatikan untuk tampilan interface nya lengkap, dari eth0, wlan, Bluetooth dll. Disini penulis menggunakan kabel lan jadi yang terdeteksi ada gelombang trafiknya yang Eth0.

Selanjutnya double klik pada Eth0 dan akan muncul tampilan sep-erti ini, disini pilih sesuai kebutuhan saja atau bisa semuanya. Kalau sudah klik tombol Start yang ada di bawah.



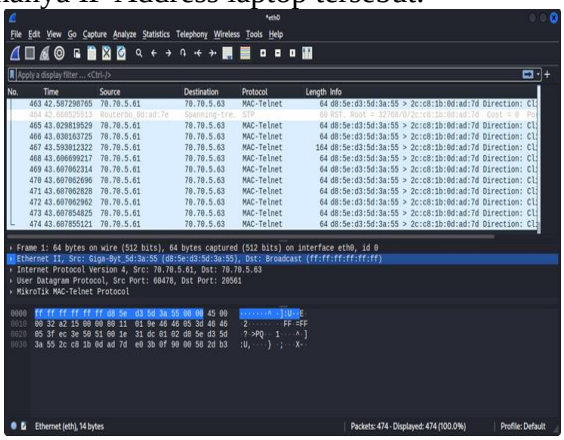
Gambar 3**.** klik *start*

Setelah klik Start akan masuk ke menu Capture, disini akan di tampilkan secara realtime secara terus menerus informasinya. Disini mac address, IP address dan packet data akan terlihat dari perangkat yang terhubung dan melakukan aktivitas akan terdeteksi.



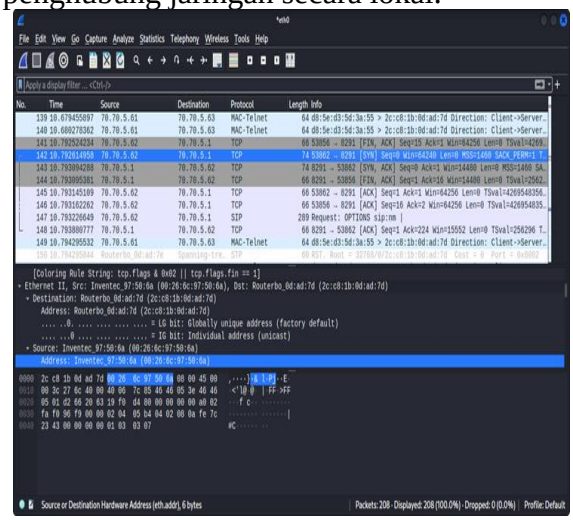
Gambar 4**.** Tampilan *interface client*

Ketika laptop yang digunakan masih berada di mode stanby. Dan belum di gunakan untuk Mapping. Yang terlihat hanya IP Address laptop tersebut.



Gambar 5. Routerboard yang terdeteksi

Salah satu perangkat yang terdeteksi disini Routerboard, karena sebagai penghubung jaringan secara lokal.



Gambar 6. Ketika proses Mapping berjalan

Ketika proses Mapping berjalan di laptop, kemudian PC server sebagai targetnya, maka akan muncul aktivitas yang dilakukan.

Dari kegiatan pertama ini, dapat di analisa aktivitas pada jaringan komputer yang berjalan. Termasuk informasi dari komputer server yang tersedia.

Kesimpulannya adalah penggunaan Wireshark untuk analisis dan mendapatkan informasi di komputer server yang terhubung itu cukup mudah tanpa harus membuka komputer servernya.

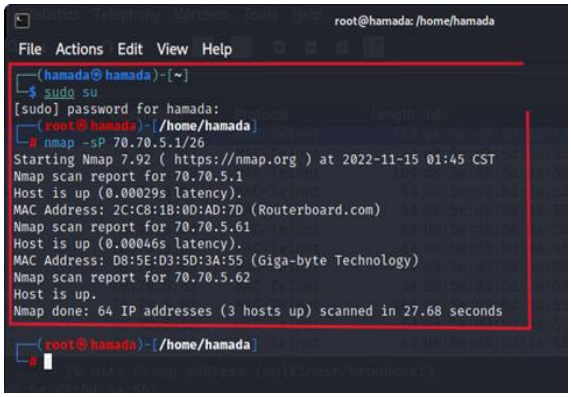
Tabel 1. Kesimpulan penggunaan Wireshark

Keterangan	**Hasil**
Tampilan awal *Wireshark*	**ok**
Setting interface yang akan di gunakan (silahkan centang yang di butuhkan)	**ok**
Interface setelah di jalankan (laptop)	**ok**
Contoh salah satu perangkat yang terdeteksi, disini yang terdeteksi routerboard	**ok**
Wireshark mendeteksi adanya *mapping* yang berjalan pada *protocol* TCP (targetnya PC Server)	**ok**

2. Network Mapper (NMAP)

Tahap kedua penulis menggunakan tools NMAP untuk mencari celah pa-da port yang terbuka. Berikut penjelasannya :

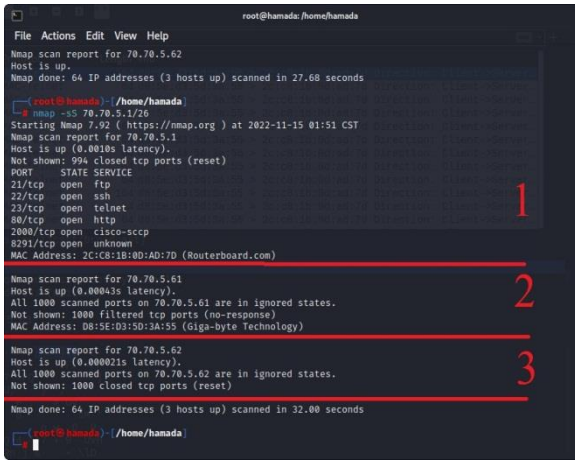
Pertama, buka terminal kemudian masuk sebagai administrator (super user), kemudian ketik perintah nmap –sP 70.70.5.1/26 untuk melakukan scanning pada range IP tersebut guna mendapatkan informasi perangkat yang terhubung.



Gambar 7. identifikasi perangkat yang terhubung

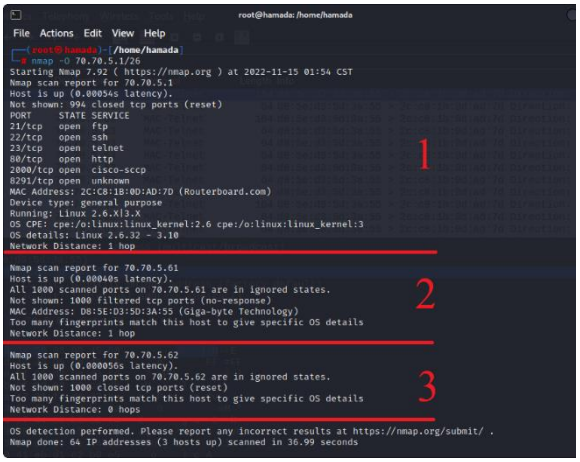
Disini yang terbaca ada tiga perangkat yaitu Routerboard, Giga-byte (PC server) dan laptop.

Selajutnya adalah scanning port pada perangkat yang aktif untuk melihat port yang terbuka. Ketik perintah "nmap –sS 70.70.5.1/26" akan terlihat port yang terbuka.



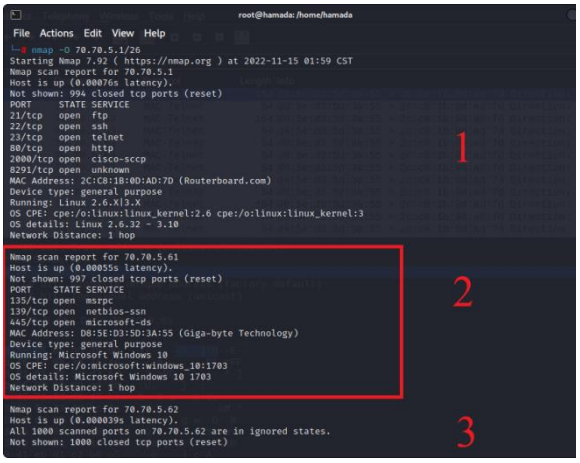
Gambar 8. *scan port* yang terbuka

Setelah melakukan scanning port maka akan terlihat port yang ter-buka. Selanjutnya untuk mengetahui system operasi yang di gunakan pa-da masing-masing perangkat yang terhubung ketik perintah “nmap –O 70.70.5.1/26”.



Gambar 9. Informasi OS pada PC server

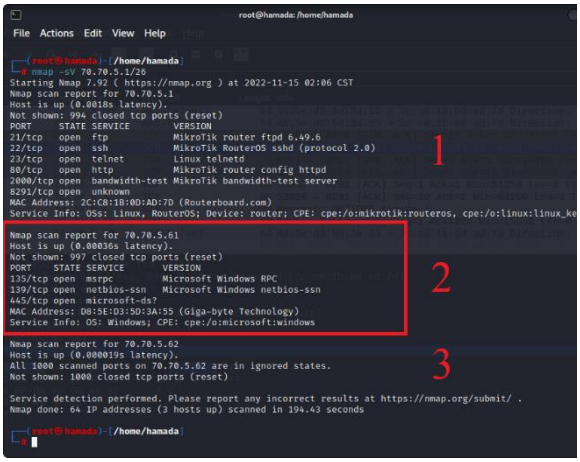
Nomor 1 Routerboard, nomor 2 PC *server*, nomor 3 laptop. Target nya PC *Server* untuk ditest keamanannya.



Gambar 10. Server mematikan *Firewall*

Pada bagian proses pengumpulan informasi menentukan sistem operasi apa yang berjalan pada perangkat yang aktif untuk mengetahui tipe sistem yang sedang ditest security nya. Namun disini server masih mengaktifkan Firewall sehingga informasi OS tidak akan terdeteksi (per-hatikan gambar 4.8). Berikutnya server mematikan Firewall maka akan terlihat informasi OS yang digunakan (perhatikan gambar 4.9).

Ketika Nmap tidak dapat mendeteksi OS secara tepat, ia terkadang memberikan kemungkinan terdekat. Tebakan yang cocok akan dilakukan oleh Nmap. Dengan option ini membuat Nmap menduga dengan lebih agresif.



Gambar 11. *Scan port* yang terbuka

Kemudian setelah *port* yang *open* diketahui dengan menggunakan salah satu metode *scan* diatas, hal selanjutnya adalah deteksi versi dari *service* yang sedang berjalan.

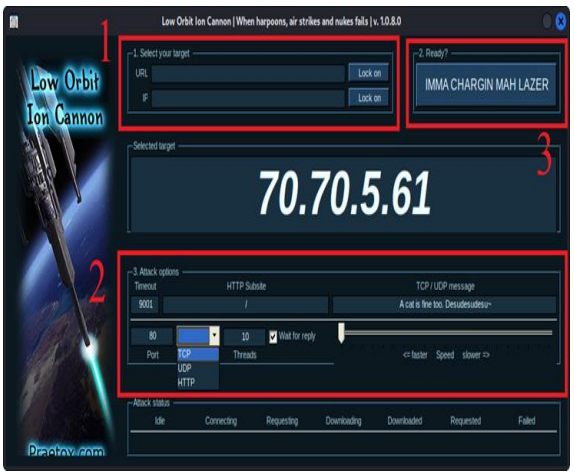
Maka dapat di simpulkan jika computer server menghidupkan *Firewall* maka tidak akan terlihat informasi terkait OS nya, tetapi jika *Firewall* di matikan maka akan terlihat. Berikut tabel keterangan :

Tabel 2 kesimpulan penggunaan NMAP

Keterangan	Hasil
melakukan scanning pada range IP guna mendapatkan informasi perangkat yang terhubung.	Ok
scanning port pada perangkat yang aktif untuk melihat *port* yang terbuka.	Ok
untuk mengetahui sistem operasi yang di gunakan pada masing-masing perangkat yang terhubung tetapi PC *server* masih mengaktifkan *Firewall.*	Ok
untuk mengetahui system operasi yang di gunakan pada masing-masing perangkat yang terhubung PC *server* menonaktifkan *Firewall.*	Ok
Untuk deteksi versi dari *service* yang sedang berjalan.	Ok

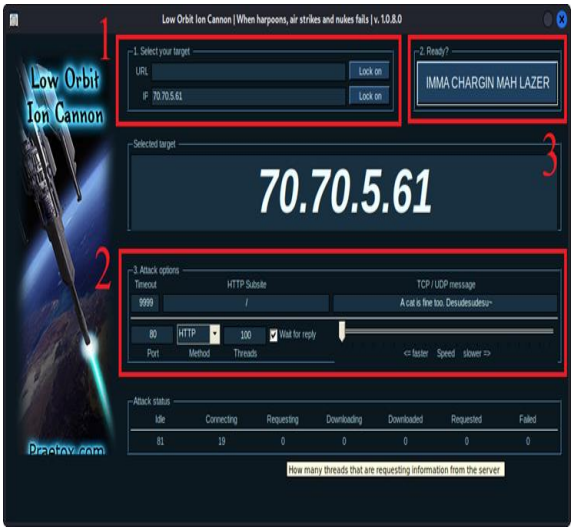
3. *Attacking the Infrastructure (DDoS)*

Tahap ketiga dalam melakukan pengujian adalah dengan melakukan stressing, yaitu mensimulasikan serangan pada komputer *server*. Disini penulis menggunakan *softwere* LOIC *(Low Orbit Ion Can-non).*



Gambar 12. tampilan *interface softwere*

Keterangan pada gambar 12 no 1 untuk mengisi alamat atau IP target. Setelah terisi kemudian klik *Lock on* untuk mengunci target. Kemudian no 2 untuk *Attack options* fitur apa saja yang akan di serang sesuai kebutuhan. Dan no 3 untuk mengeksekusi jika konfigurasi sudah selesai.

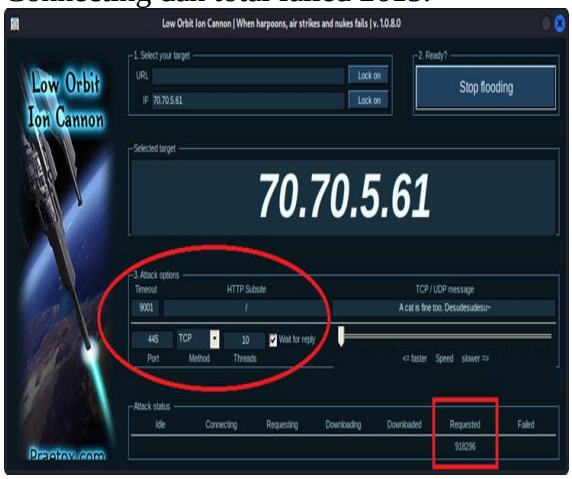


Gambar 13. *Preparation*

Pada gambar 13 masukkan ip *address* target 70.70.5.61 kemudian *lock on* akan muncul di tengah secara jelas, kemudian di no 2 coba untuk di sesuaikan *port* mana yang akan di serang, kemudian klik IMMA CHARGIN MAH LAZER jika sudah *ready*.

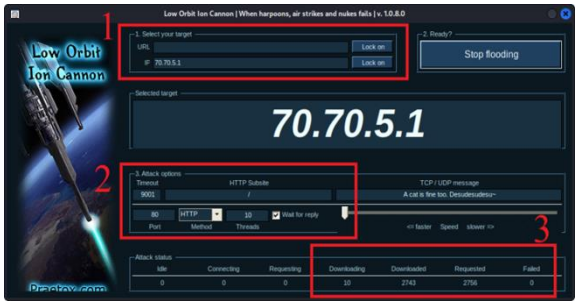
Gambar 14. Hasil serangan pertama PC server

Dari serangan pertama dari port 80 ,method HTTP, Threads 1000 dapat diketahui pada kolom Attack Status. Dari 1000 treads yang menyerang 972 sisanya Connecting dan total failed 2615.



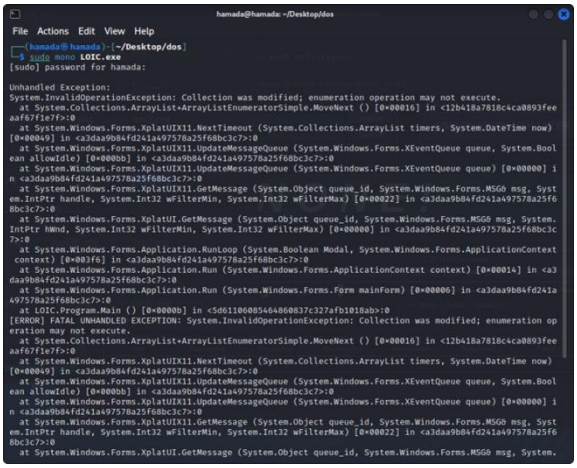
Gambar 15. Percobaan serangan kedua PC server

Dari serangan kedua ini, *Attack options* nya (*port* 445, *method* TCP, *Threads* 10). Hanya menghasilkan *Requested* sebanyak 918296 pada *Attack status*. Artinya serangan ini juga tidak tembus.



Gambar 16. Hasil serangan ketiga ke Routerboard

Hasil serangan ketiga dicoba ke ke *Router* dengan *options* yang sama (*port* 80, *method* HTTP, *threads* 10). Dan berhasil *Download* 2743 sedang di *download* 10.



Gambar 17 hasil serangan ketiga setelah selesai

Ini hasil dari serangan yang ketiga ke *Routerboard* yang ada di jaringan yang sama. Dari ketiga serangan tersebut 2 kali PC *server* dan 1 kali ke Routerboard.

Maka dapat di simpulkan bahwa serangan ke komputer *server* melalui *port* 80, 445 dan *method* TCP, HTTP hasilnya ***Failed***. Sedangkan serangan ke *Routerboard* 1 kali hasilnya langsung *Success*. Dari kedua perangkat tersebut komputer *server* lebih baik keamanannya karena mempunyai *Firewall* yang selalu terupdate, sedangkan *Routerboard* yang jarang di update sangat mudah terkena serangan.

Tabel 3. Tabel serangan *DDoS attack*

Keterangan	**Hasil**
Hasil serangan I *port* 80 ,*method* HTTP, *Threads* 1000 dapat diketahui pada kolom *Attack Status*. Dari 1000 *treads* yang menyerang 972 sisanya *Connecting* dan total *failed* 2615.	Failed
Hasil serangan II (*port* 445, *method* TCP, *Threads* 10). Hanya menghasilkan *Requested* sebanyak 918296 pada *Attack status*. Artinya serangan ini juga tidak tembus.	Failed

Hasil serangan III ke Routerboard (*port* 80, *method* HTTP, *threads* 10). Dan berhasil *Download* 2743 sedang di *download* 10.	Berhasil

4. *Maintaining access* (mempertahankan akses)

Pada *routerboard* ada beberapa celah yang terbuka seperti port 80 , port 139, 135, dan port TCP, HTTP. Sebaiknya untuk meningkatkan keamanan perlu adanya konfigurasi sendiri tetapi secara detail agar port yang tidak digunakan tertutup.

Dan komputer server mempunyai celah ketika Firewall tidak di aktifkan, tetapi jika di aktifkan port yang menjadi celah akan tertutup.

5. *Analysis* (analisa)
   1. Celah keamanan yang dapat di serang
      - Pada routerboard port 21/tcp (ftp), 22/tcp (ftp), 23/tcp (telnet), 80/tcp (http)
      - Pada komputer server port 135/tcp (msrpc), 139/tcp (netbios-ssn), 445/tcp (Microsoft-ds)
   2. Data yang dapat diambil atau diakses
      - Pada *routerboard* data yang dapat di ambil pada port 80/tcp (http)
      - Pada komputer *server* tidak ada data yang bisa diambil
   3. Waktu yang digunakan untuk menerobos ke dalam sistem.
      - Pada *routerboard* saat ada aktivitas yang berjalan
      - Pada komputer *server* saat komputer menerima *packet* dari *routerboard*

Untuk mengamankan di *router* perlu konfigurasi sendiri jangan menggunakan *default setting*, dan komputer *server* selalu cek *Firewall* secara berkala dan terupdate *system*.

4. PENUTUP

4.1. Kesimpulan

Berdasarkan "Pengujian Keamanan Jaringan Menggungakan Metode *Penetration Testing* Pada Jaringan Smk Muhammadiyah 1 Wonosobo." Penulis menyimpulkan, dalam kegiatan mencari celah dengan NMAP, komputer server diuji serangan *DDoS* sebanyak 2 kali melalui *port* 80, 445 dan *method* TCP, HTTP hasilnya *Failed*. Sedangkan serangan *DDoS* ke *Routerboard* 1 kali hasilnya langsung *Success*. Dari kedua perangkat tersebut komputer *server* lebih baik keamanannya karena mempunyai *Firewall* yang selalu terupdate, sedangkan *Routerboard* yang jarang di *update* sangat mudah terkena serangan *DDoS*.

4.2. Saran

Setelah melakukan observasi, pengamatan, dan pengujian selama di SMK Muhammadiyah 1 Wonosobo. Ada beberapa saran dapat penulis sampaikan, yaitu meningkatan keamanan jaringan dengan konfigurasi sendiri jangan menggunakan konfigurasi *default* dari sistem. Dikarenakan penyerangan tidak hanya menggunakan tiga tahapan tersebut dan juga jenis serangan sangat banyak. Sedangkan keamanan jaringan komputer server itu sendiri sudah baik jika *Firewall* selalu aktif dan selalu terupdate.

5. DAFTAR PUSTAKA

Sabdho, H. D., & Ulfa, M. (2018). Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor PT. Mora Telematika Indonesia Regional Palembang. In *Prosiding Seminar Hasil Penelitian Vokasi (Semhavok)* (Vol. 1, No. 1, pp. 15-24).

Ismail, R. W., & Pramudita, R. (2020). Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT. Puma Makmur Aneka Engineering

Bekasi. *Jurnal Mahasiswa Bina Insani*, *5*(1), 53-62.

Ketaren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. *Jurnal Times*, *5*(2), 35-42.

Kurniawan, D., & Syah, A. M. (2022). The Impact of Bjorka Hacker on the Psychology of the Indonesian Society and Government in a Psychological Perspective. *CONSEILS: Jurnal Bimbingan dan Konseling Islam*, *2*(2), 53-60.

Bayu, I. K., Yamin, M., & Aksara, L. F. (2017). Analisa Keamanan Jaringan Wlan Dengan Metode Penetration Testing (Studi Kasus: Laboratorium Sistem Informasi dan Programming Teknik Informatika UHO.

Sanjaya, I. G. A. S., Sasmita, G. M. A., & Arsa, D. M. S. (2020). Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, 113-124.

Haeruddin, H., & Kurniadi, A. (2021, March). Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6). In *CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences* (Vol. 1, No. 1, pp. 508-515).

Kurniawan, A. (2021). *Ethical Hacker–Menjadi Peretas yang Beretika*. PENERBIT KBM INDONESIA.

Pohan, Y. A., Yuhandri, Y., & Sumijan, S. (2021). Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar. *Jurnal Sistim Informasi dan Teknologi*, 1-6.