PENETRATION TESTING DALAM FORENSIK DIGITAL PADA JARINGAN FAKULTAS TEKNIK UNIVERSITAS IBN KHALDUN BOGOR DENGAN *PING OF DEATH*

Denis Quroturohman
Program Studi S1 Sarjana Teknik Informatika
Teknik Informatika, Fakultas Teknik, Universitas Ibn Khaldun, Bogor
Email : denisq94@gmail.com

Abstrak

Ilmu pengetahuan tentang k eamanan k omputer yang terk ait dengan penyelidik an untuk menentuk an sumber serangan jaringan berdasark an data log buk ti, identifik asi, analisis, dan rek onstruk si k ejadian adalah Forensik Jaringan yang merupak an cabang dari Forensik Digital. Jenis serangan terhadap suatu k omputer atau server di dalam jaringan dengan cara menghabisk an sumber daya (resources) yang dimilik i oleh k omputer sampai k omputer tersebut tidak dapat menjalank an fungsinya dengan benar, sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh ak ses dari layanan jaringan yang diserang disebut dengan serangan Distributed Denial of Service (DDoS). Riset Forens ik Jaringan dilak uk an dalam Laboratorium Riset Magister Tek nik Informatik a Universitas Ahmad Dahlan Yogyak arta. Detek si serangan dilak uk an oleh Winbox RouterOS v3,6 dimana software tersebut menunjuk an resources, data penyerang (IP Address), jumlah pak et data, dan k apan terjadi serangan. Simulasi serangan dilak uk an dengan software LOIC untuk mengetahui k inerja sist em pengaman jaringan k omputer, sedangk an sistem pengaman jaringan k omputer berupa antisipasi terhadap bentuk serangan DDoS.

Kata kunci— *DDoS, router,* pengaman jaringan komputer.

Abstact

Network forensics is a computer security investigation to find sources of the attack s on the network by examining data log evidence, identifying, analyzing, and reconstructing the incidents. Types of attack s againist a computer or server on the network by spending resources that are owned by the computer until computer is not able to function properly, thus indirectly preventing other users to obtain access to network services that were attack ed is Distributed Denial of Service attack (DDoS). Network Forensics Research conducted in Research Laboratory of Information Engineering Master of Ahmad Dahlan University Yogyak arta. Detection of attacks carried out by Winbox RouterOS v3,6 where the software shows resources, attack er (IP Address), data pack ets, and when attack doing. Simulated attack s carried out by LOIC software to determine performance of safety system in computer network . To anticipate DDoS attack s,then developed a computer network security system.

Keywords: *DDoS, Router, Safety system of Security Network*

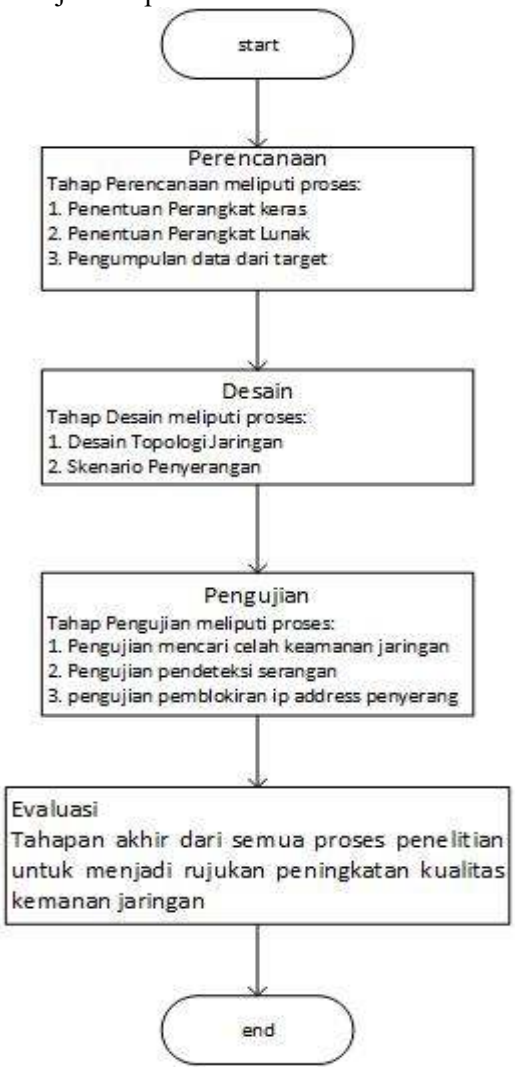
1. PENDAHULUAN

Teknologi informasi telah berkembang dengan pesat pada saat ini, terutama dengan adanya jaringan internet yang dapat memudahkan dalam melakukan komunikasi dengan pihak lain[1]. Dua dekade terakhir, jaringan komputer telah menjadi bidang revolusioner untuk berimprovisasi[2]. Keamanan jaringan merupakan tugas penting yang harus serius dipertimbangkan ketika merancang jaringan. Keamanan jaringan didefinisikan sebagai kebijakan dan prosedur diikuti oleh administrator jaringan untuk melindungi perangkat jaringan dari ancaman, hal ini sangat penting bahwa mekanisme keamanan dari suatu sistem yang dirancang untuk mencegah akses tidak sah[3]. Perlunya model simulasi *penetration testing* dalam sebuah sistem jaringan yang dapat membantu administrator sebagai bahan evaluasi dalam mendapatkan kualitas jaringan,yang aman dari serangan pihak yang tidak bertanggung jawab sehingga *administrator* dapat menanggulangi ancaman secara cepat dan jaringan dapat beroperasi kembali secara optimal. Penerapan sistem pengamanan jaringan yang mampu mendeteksi dan memblokir serangan dapat dilakukan dan

pelaksanaan pencegahan dengan metode forensik digital sehingga *administrator* dengan mudah dapat mendeteksi, menganalisis dan melakukan penangulangan terhadap serangan pada jaringan. Metode Forensik melakukan pendeteksian serangan berdasarkan tahapan yang sesuai. Adapun tujuan yang ingin dicapai pada penelitian ini adalah: (1) Memperoleh IP *Address* dari penyerang.(2) Mengetahui kekuatan keamanan jaringan dengan metode *penetration testing.*

2. METODE PENELITIAN

Metode pada penelitian ini terdiri dari lima tahapan yaitu perencanaan, desain, pengujian,laporan dan evaluasi seperti ditunjukkan pada Gambar 1 berikut:



Gambar 1 Metode Penelitian

Tahap Penelitian:

Tiap tahapan pada metode penelitian pada Gambar 1 akan dijelaskan sebagai berikut:

I. Perencanaan

Pada tahap ini yang dilakukan adalah menentukan perangkat lunak dan perangkat keras dan data seperti IP *Address* dan celah keamanan jaringan agar penelitian bisa berjalan dengan semestinya.

II. Desain

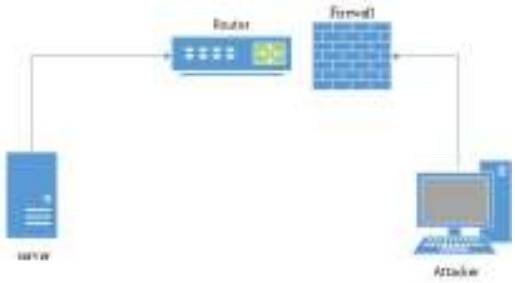
Dalam tahap desain yaitu membuat pola terstruktur untuk menentukan sistem berdasarkan pada rancangan penelitian dimana terdapat beberapa Topologi dalam menggambarkan desain struktur yang akan dibangun.

III. Pengujian

Pengujian simulasi serangan terhadap sistem dilakukan pada tahap ini dimana penulis selaku penguji penetrasi melakukan deteksi terhadap celah-celah kerentanan. Rincian tahap pemindaian (*scanning)* dan simulasi penyerangan meliputi *Ping of death.*

IV. Evaluasi

Tahap ini adalah tahapan akhir dari semua proses penelitian yang bisa menjadi rujukan untuk meningkatkan kualitas kemanan jaringan pada Fakultas Teknik Universitas Ibn Khaldun Bogor.



Gambar 2 Topologi *Penetration Testing*

3. HASIL DAN PEMBAHASAN

Hasil dari pengukuran kinerja sistem dengan pemberian 1 (satu) serangan, yaitu *Ping of death* melalui 4 (empat) tahap, yaitu pemberian serangan, deteksi, identifikasi pada log,dan pemblokiran. Sehingga menghasilkan pencegahan serangan agar tidak terlalu masuk menembus jaringan komputer yang ada, Sehingga menghasilkan pencegahan. Dan mengahasilkan berupa (empat) jenis informasi, yaitu waktu serangan, jenis serangan, IP tujuan dan IP sumber, dan serangan dapat terblokir dengan konfigurasi di *routerOs*.

3.1 *Scanning* dengan Nmap

Pengujian untuk mencari celah keamanan jaringan yang ada, dengan menggunakan Nmap

Gambar 3 *Scanning* dengan Nmap

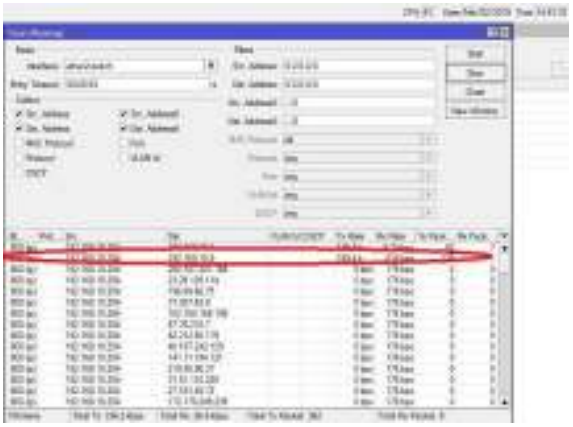
3.2 Pengujian *Penetration Testing*

Setelah mendapatkan port atau celah yang terbuka, kemudian di mulai lah proses *penetration testing* untuk melakukan pengujian, Pengujian di lakukan dengan LOIC, dengan memasukan IP target yang akan di uji.

Gambar 4 Pengujian *Penetration Testing*

3.3 Deteksi

Deteksi serangan *DDoS* dalam hal ini menggunakan *Software Winbox RouterOS* yang menunjukan identitas dari penyerang., warna merah menunjukan akses ilegal dalam jaringan komputer Fakultas Teknik UIKA Bogor.



Gambar 5 Akses ilegal

Selain mendapatkan barang bukti, dibuat sistem antisipasi yaitu dengan memblokir IP *Address* dari penyerang agar tidak terjadi serangan yang sama dikemudian waktu.IP *Addre*ss 192.168.10.9 diblokir supaya dilain waktu tidak dapat melakukan serangan.. Menunjukan, proses terhentinya *request* serangan setelah diblokir dan paket data yang dikirim oleh penyerang akan terhenti.

4. KESIMPULAN

Hasil dari tahapan pembuatan sistem *Penetration Testing* melalui 4 (empat) tahapan, yaitu perencanaan, desain, pengujian dan evaluasi,. Sehingga dapat memperoleh IP *Address* dari penyerang, Hasil pengukuran kinerja keamanan jaringan dengan model penetrasi dan berbantu forensik digital menghasilkan kombinasi untuk menemukan kesalahan dalam sebuah jaringan dan menidentifikasi masalah dalam sistem jaringan

DAFTAR PUSTAKA

[1] Kusumawati, Monika, *Implementasi IDS (Intrusion Detection System) Serta Monitoring Jaringan Dengan Interface WEB Berbasis BASE Pada Keamanan Jaringan*, Universitas Indonesia, Depok. 2010

[2] Boob, Snehal, Priyanka Jadhav, 2010, "Wireless Intrusion Detection System" in *International Journal of Computer Applications*, Volume 5– No.8, August 2010, pp. 9-13.

[3] Taluja, Sachin, Pradeep Kumar Verma, Rajeshwar Lal Dua, 2012, "Network Security Using IP firewalls" in *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 2 Issue 8, August 2012, pp. 348-354.

[4] Suyatno Budiharjo, dan Faisal Riyadi,"Forensik Jaringan Pada Lalu Lintas dalam jaringan *Honeynet* Di Indonesia *Security Insident Respone Team On Internet Infrastructure/Coordination Center"* November 2014

[5] Eka Leonardus Dian Suradji, dan Dian Widiyanto Chandra,S.kom., M.cs "*Penetration Testing* Sistem Jaringan Komputer Untuk Mengetahui Kerentanan Kemanan *Server* Dengan Menggunakan Metode *Penetration Testing Execution Standart (PTES)* Studi Kasus Rumah Sakit Santa Clara Madiun" Oktober 2014

[6] Goel, Rohit, Durgesh Kumar, Abhishek Raja, 2014, "A Packet Filtering Firewall" in *International Journal of Emerging Technology and Advanced Engineering*, Vol. 4 Special Issue 1, February 2014, pp. 362-363.

[7] Tejvir Kaur, Vimmi Malhotra, Dr. Dheerendra Singh, 2014, "Comparison of network security tools- Firewall Intrusion Detection System and Honeypot" in *International Journal of Enhanced Research in Science Technology & Engineering*, Vol. 3 Issue 2, February 2014, pp. 201-202.

[8] Kumar, Ashish, Ajay K. Sharma, Arun Singh, Dr. B. R. Ambedkar, 2012, "Performance Evaluation of Centralized Multicasting Network over ICMP Ping Flood for DdoS" in *International Journal of Computer Applications*, Vol. 37, January 2012, pp. 3.

[9] https://nmap.org/