Pengelolaan Sistem Keamanan Jaringan dengan Adopsi Pola Kerja Hacker

Sasut Analar Valianta
Megister Teknik Informatika
Fakultas Ilmu Komputer
Univeristas Sriwijaya
kups@ivaley.com

Tasmi Salim
Megister Teknik Informatika
Fakultas Ilmu Komputer
Univeristas Sriwijaya
tasmi@ilkom.unsri.ac.id

Deris Stiawan
Program Studi Sistem Komputer
Fakultas Ilmu Komputer
Univeristas Sriwijaya
deris@ilkom.unsri.ac.id

Abstrak*—Keamanan pada sebuah jaringan bukanlah perkara yang mudah, seringkali sebuah server dalam jaringan dapat dengan mudahnya diretas padahal sistem keamanan yang dibuat sudah memenuhi standarisasi keamanan yang telah ditentukan secara umum. Seorang hacker atau peretas akan selalu mencari celah walau sekecil apapun untuk dapat masuk ke dalam sistem, teknik yang dilakukan para hacker umumnya sama, namun tidak ada publikasi secara detail bagaimana tahapan seorang hacker untuk dapat sukses melakukan peretasan pada sebuah sistem. Naskah ini akan membahas bagaimana seorang hacker berpikir dan mencari peluang, sehingga tehnik yang tepat untuk mengamankan suatu sistem jaringan dapat ditanamkan dalam sebuah konsep. Kedepan akan dirancang sebuah sistem jaringan dengan konsep otomatis.*

Kata kunci*—Network Security Management Sistem, Hacker Technique, Penetration Test, Vulnerable Object*

I. PENDAHULUAN

Suatu jaringan di bangun dengan sistem yang memilik standar keamanan. Semakin berkembangnya arsitektur jaringan para network developer dituntut untuk dapat membangun sebuat sistem jaringan dengan biaya rendah namun memiliki fitur keamanan yang baik.

Dalam studi kasus tertentu seringkali didapati bahwasanya sebuah server yang terhubung pada suatu jaringan mengalami serangan dari para hacker, dan lebih parah lagi hacker dapat mengambil alih sistem tanpa diketahui oleh administrator jaringan dan keamanan, padahal sistem telah dibangun dengan standarisasi keamanan yang dianggap ketat.

Hacker atau peretas digolongkan dalam beberapa tingkat keahlian, mulai dari level pemula sampai tingkat mahir. Hacker pada tingkatan pemula seringkali melakukan peretasan suatu server yang terbuka untuk public, tehnik yang dilakukan umumnya sama yaitu dengan mencoba kelemahan sytem yang dibangun para developer. Untuk tingkatan menengah, hacker akan menganalisa port-port yang terbuka dalam suatu jaringan dengan melakukan fingerprint request pada port yang terbuka untuk mengetahui platform apa yang digunakan, selanjutnya mencari celah kelemahan dari platform tersebut. Hacker dengan tingkat kemahiran yang lebih tinggi, akan mencari celah pada suatu jaringan untuk dapat masuk kedalam sistem atau sebuah server. Celah-celah inilah yang terkadang terabaikan oleh seorang developer keamanan jaringan, dengan kata lain hacker dengan level mahir akan menggunakan jaringan itu sendiri untuk dapat masuk kedalam sebuah server yang dituju dalam jaringan tersebut.

Penetration test atau tes penetrasi terhadap suatu sistem biasanya sering dilakukan para developer jaringan sebagai standarisasi sebelum jaringan dapat dijalankan, namun standarisasi ini hanya diambil berdasarkan konsep umum terhadap keamanan jaringan, tanpa mempertimbangkan bagaimana seorang hacker mencari celah dan bagaimana seorang hacker melakukan kegiatannya.

Dalam naskah ini, akan memaparkan bagaimana dan apa saja tehnik yang di lakukan seorang hacker untuk dapat sukses melakukan peretasan. Sehingga kedepan dapat dibangun sebuah platform yang lebih aman dengan biaya yang lebih rendah.

II. HACKER TECHNIQUE

Seperti yang sudah dijelaskan pada bagian sebelumnya, seorang hacker dengan tingkat mahir akan selalu mencari celah terkecil sekalipun dari suatu jaringan untuk setidaknya dapat terhubung pada jaringan tersebut. Pola kerja atau teknik yang digunakan hacker yang perlu diwaspadai antara lain seperti penjelasan berikut.

A. Network Scan

Network scanning dilakukan untuk mencari atau mengetahui gateway utama pada sebuah target, sehingga dapat dilanjutkan untuk scanning terhadap IP *(Internet Protocol)* Address dalam jaringan tersebut untuk mengetahui berapa banyak jumlah server bekerja pada jaringan tersebut, dan atau mengetahui berapa banyak server yang dapat diakses secara langsung.

B. TCP dan UDP Scan

TCP *(Transmission Control Protocol)* dan UDP *(User Datagram Protocol)* scan adalah tehnik untuk mengetahui berapa banyak port yang terbuka pada target yang dituju. Seringkali karna terbatasnya public IP address, dalam sebuah jaringan dilakukan forwarding port dari sebuah gateway public IP address ke local IP Address. Tehnik ini dapat mengetahui apakah port yang terbuka digunakan oleh server yang sama, atau server yang berbeda dalam jaringan tersebut. Dan jika port yang terbuka tidak dapat ditembus, maka akan ada kemungkinan untuk dapat menembus melalui port lainnya,

Annual Research Seminar (ARS) Fakultas Ilmu Komputer Unsri 2015

dan melakukan penetrasi terhadap port atau server yang dituju melalui port server yang berhasil ditembus, tehnik ini disebut spoofing, karena hacker melakukan serangan dari dalam jaringan melalui server yang ditembusnya.

C. *Fingerprints Request Scan*

Finggerprint request dapat mengetahui platform apa yang sedang berjalan pada port server yang terbuka secara public. Tehnik ini digunakan untuk menentukan tools yang digunakan untuk melakukan penetrasi secara langsung terhadap target server yang dituju.

D. *Server Penetration*

Setelah diketahui apa saja platform yang sedang berjalan pada suatu server, maka hacker akan mencoba melakukan penetrasi baik itu secara langsung ataupun spoofing. Keberhasilan dalam tehnik ini akan menyebabkan hacker dapat melakukan kegiatan apapun di dalam server tersebut.

Setelah hacker dapat masuk kedalam sistem, umumnya mereka akan berusaha untuk mendapatkan hak akses tertinggi pada sistem sehingga dapat ditanam sebuah aplikasi otomatis seperti *worm*, untuk mengirimkan data kepada hacker.

E. *Phishing dan Scamming*

Tehnik ini dilakukan untuk mendapatkan hak akses baik itu user maupun administrator. Hacker akan mengarahkan user pada platform palsu, untuk mengindari kecurigaan hacker akan memforward request data ke platform aslinya.informasi yang didapatkan umunya berupa hak akses, berupa informasi hak akses ke platform bahkan ada juga yang berupa informasi hak akses ke email user.

F. *Tampering*

Tampering dilakukan untuk mendapatkan informasi apa saja proses yang sedang bekerja saat permintaan dieksekusi oleh server atau user, Ada beberapa tipe dalam teknik tampering diantaranya;

- Local Network Tampering
  Tampering dilakukan pada local network untuk mendapatkan informasi apa saja proses yang dieksekusi antara server dan user.
- Direct Data Tampering
  Informasi yang diharapakan tidak berbeda dengan Local network tampering, namun teknik ini dilakukan langsung terhadap server atau gateway dengan berpura-pura sebagai user biasa.

G. *DDoS Attack*

DDos (*Distributed Denial of Service*) Attack seringkali diartikan sebagai flooding pada sebuah jaringan atau server. Serangan ini dapat mengakibatkan overload pada jaringan yang berarti padatnya lalulintas pada jalur transmisi jaringan. seorang administrator jaringan yang tidak paham apa yang sedang terjadi akan akan menyimpulkan bahwa server yang atau gateway yang mengalami overload telah mendapatkan serangan DDoS dan melakukan restart pada gateway atau server tersebut, seringkali restart atau reboot akan di lakukan pada server yang terindikasi mendapatkan serangan DDoS, padahal si hacker sangat mengharapkan hal itu terjadi.

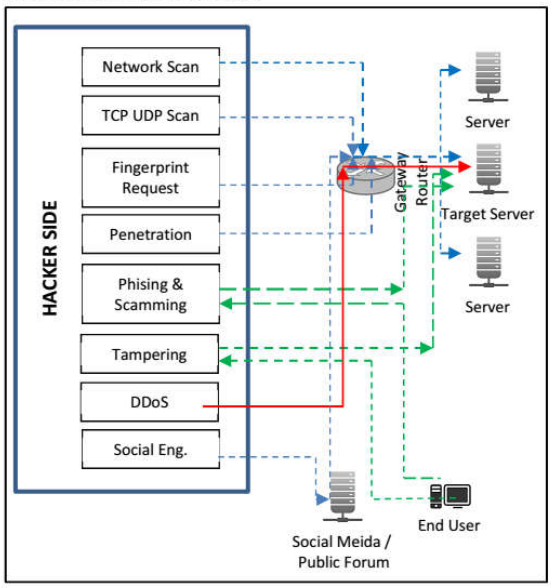
Sebagai gambaran umum, bahwa tehnik ini digunakan oleh hacker tingkat mahir, dimana si hacker telah berhasil menguasai server atau jaringan dan telah menanamkan suatu *backdoor / shellcode / tools* pada server atau jaringan tersebut, agar tools yang ditanam dapat berjalan secara permanent pada sistem si hacker mengharapkan reboot pada sistem tersebut, hacker bisa saja melakukan reboot secara langsung, namun kegiatan ini akan mengakibatkan kecurigaan dari administrator, oleh karena ini bantuan dari administrator itu sendiri sangat dinantikan.

Gambaran lainya, hacker menyakini ada celah pada service yang sedang berjalan pada server atau gateway, namun sistem terlindungi oleh firewall yang di pasang pada sistem, sedangkan firewall tersebut hanya menggunakan cache memory, dengan melakukan DDoS hacker mengharapkan sistem akan di *reboot* dan pengaturan firewall menjadi default, dan si hacker dapat melakukan cracking pada sistem untuk mendapatkan hak akses tertinggi.

H. *Social Engenering*

Suatu hal yang sangat dilupakan oleh para developer adalah social engineering, tehnik ini digunakan para hacker jika menemukan jalan buntu, atau kekurangan informasi terhadap server yang dituju. Hacker akan mencari apa saja informasi yang tersedia secara public yang berhubungan dengan kata kunci dari server atau jaringan yang dituju. Informasi ini kadang tidak sengaja terekspos oleh developer secara public. Informasi ini diantaranya seperti ; si developer mambahas sebuah platform pada sebuah social media. Informasi mengenai developer, email address, nomer telepon, alamat. file konfigurasi jaringan atau server yang dapat diakses secara public, dan sebagainya.

Gbr. 1 Flow Chart Pola Kerja Hacker



ISBN: 979-587-573-6

III. PENANGANAN JARINGAN

Bermacam-macam standarisasi dalam keamanan jaringan diterapkan, namun tetap saja dianggap kurang mampu dalam memproteksi serangan dari para hacker. Keamanan dalam suatu jaringan adalah pekerjaan yang dianggap cukup berat, karena harus dikerjakan secara real-time.

Sistem firewall sering kali digunakan untuk melindungi jaringan dari serangan para hacker, namun terbatasnya pengetahuan terhadap pola pikir hacker mengakibatkan konfigurasi pada firewall hanya terbatas pada proteksi secara umum.

Beberapa macam konfigurasi penting yang dapat melindungi jaringan dari serangan hacker antara lain :

A. Echo Reply

Manipulasi pada echo reply sangat penting, karena informasi ini dapat melindungi server atau gateway dari serangan lanjutan hacker, ada beberapa model reply yang dapat dikonfigurasi seperti droping dan reject. Echo reply dapat dikonfigurasi melalui gateway maupun firewall server, penggabungan keduanya dapat menghasilkan sistem yang lebih aman.

B. TCP dan UDP SYN Protect

Konfigurasi dapat dilakukan dengan menggunakan script dimana apabila terjadi request port yang dinamis dan konstan maka firewall akan segera melakukan droping terhadap requester.

Untuk jaringan local, pembatasan komunikasi antara server sebaiknya dilakukan, untuk menghindari jika terjadi kebocoran pada salah satu server, maka tehnik spoofing dapat dihindari antara server dalam suatu jaringan.

C. Fingerprint Manipulation

Fingerprint dapat memberikan informasi pada public mengenai platform yang digunakan baik itu sistem operasi maupun service yang digunakan. Konfigurasi dapat dilakukan dengan memanipulasi informasi header reply dari sebuah server maupun router gateway.

D. Development Coordination

Sebuah jaringan tentu saja berisi layanan-layanan yang dapat diakses baik public maupun intern, seringkali service developer membangun platform tanpa koordinasi dengan administrator jaringan terlebih dahulu, sehingga kelemahan yang berupa celah tidak dapat diketahui, akibatnya layanan servis berjalan dengan tingkat keamanan yang tidak diuji coba terlebih dahulu. Kemungkinan adanya celah sangat besar apalagi jika service dibangun dengan platfrom opensource., dan hindari diskusi pada social media atau forum, jika mengalami kendala dalam membangun sebuah sistem

E. Data Encryption

Sebaiknya data yang diteruskan dari sebuah platform mengunakan enkripsi, sehingga walaupun hacker dapat melakukan tampering data namun data tersebut tidak dengan mudah dapat dibaca.

F. Think Before Decission

Suatu hal yang harus diwaspadai jika terjadi kejanggalan pada sistem, analisa terlebih dahulu apa yang terjadi. Terkadang keputusan yang diambil adalah kehendak dari si penyerang atau hacker.

IV. PERENCANAAN MENDATANG

Dengan adopsi dari pola kerja dan pola pikir hacker, kami akan merencanakan untuk membuat sebuah platform firewall yang dapat mengatasi masalah pada jaringan secara otomatis, baik itu analisa maupun keputusan terhadap jaringan. Setiap data yang ditransmisikan oleh server dan router ditampung dan dianalisa dalam sebuah platform khusus sebelum diteruskan kepada public. Diharapkan dengan mempelajari pola kerja hacker sistem firewall dapat dibangun dengan biaya rendah.

V. KESIMPULAN

Hacker akan selalu mencoba untuk mencari celah terhadap suatu sistem pada jaringan, hacker umumnya akan mempelajari teknik-teknik yang umumnya di publikasi secara umum, namun untuk level yang lebih mahir mereka akan mengembangkan sendiri teknik mereka bahkan adapula yang membangun tools untuk memudahkan proses kerja mereka dan mempersingkat proses waktu.

Penetration test tidak sepenuhnya dapat mengatasi masalah sebelum sebuah platform di jalankan. Dengan mempelajari pola kerja dari hacker, kemungkinan terekspos nya informasi yang diharapkan oleh para hacker dapat dicegah.

Koordinasi antara developer merupakan hal yang sangat penting, mengingat banyak developer yang membangun suatu platform dengan sistem opensource.

VI. REFERENSI

[1] "*Ten Deadly Sins of Cyber Security*" EC-Council, August 2010.

[2] "*Certified Ethical Hacking - The 5 phases Every Hacker Must Follow*" EC-Council.

[3] Xue Qiu, Shuguang Wang, Qiong Jia, Chunhe Xia, Qingxin Xia "*An Automated Method of Penetration Testing*", IEEE Computing, Communications and IT Applications Conference (ComComAp), 2014

[4] Dr. Daniel Geer and John Harthorne, "*Penetration Testing: A Duet*", IEEE 18th Annual Computer Security Applications Conference, 2002

[5] Darrien Rushing, Jason Guidry, Ihssan Alkadi *"Collaborative Penetration-testing and Analysis Toolkit*", IEEE Aerospace Conference, 2015

[6] Matt Bishop, Deborah A. Frincke*, "About Penetration Testing",* IEEE Security & Privacy, (Vol:5, Issue: 6), P84-87, Dec 2007

[7] R. Shanmugapriya, "*A Study of Network Security Using Penetration Testing",* International Conference on Information Communication and Embedded Sistems (ICICES), Feb. 2013.

[8] Sergey Bratus, Anna Shubina, Michael E. Locasto, "Teaching the Principles of the Hacker Curriculum to Undergraduates" SIGCSE'10, March 10–13, 2010

[9] Christian S. Fötinger, Wolfgang Ziegler *"Understanding a hacker's mind – A psychological insight into the hijacking of identities",* a White Paper by the Danube-University Krems, Austria

[10] Deris Stiawan, Mohd. Yazid Idris, Abdul Hanan Abdulah, 2013. Threat and Vulnerability Penetration Testing: Linux. Journal of Internet Technology. Vol 15 (3) pp. 333-342