KEAMANAN JARINGAN KOMPUTER

White Paper

Disusun Oleh :

Nama : Yen Mey Sutedja

NIM : 09011181621030

Kelas : SK7A

Dosen Pengampuh : Deris Stiawan, M.T., Ph.D

PROGRAM STUDI SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA 2019

World of Black Hat Hacker

Yen Mey Sutedja

Introduction

Perentas komputer digital yang memiliki teknologi negatif yang disebut hacker/black hat hacker. Black hat hacker adalah mereka yang melakukan hacking dengan cara meretas sistem atau program secara ilegal. Tujuannya pun tidak bisa dibilang baik karena mereka melakukan hacking untuk mengambil data pribadi pengguna internet seperti password hingga nomor telepon. Mereka juga terkadang menyebarkan virus pada perangkat lain. Dari data pribadi yang dicuri tersebut mereka bisa mendapatkan keuntungan yang besar. Data-data tersebut jika dijual bisa memiliki harga yang sangat tinggi karena memang banyak yang menginginkannya.

Tindakan tersebut jelas merugikan dan membahayakan sistem yang diretas. Kekhawatiran, ambisi dan modi operan pada peretas jahat ditampilkan sebagai media komunikasi utama mereka sehubungan dengan praktik khusus intrusi jaringan dan komputer. Sangat mendalam memahami faktor-faktor ini akan membantu deteksi dini serangan cyber dan memungkinkan untuk identifikasi ancaman cyber masa depan.

Background

Banyak orang di balik operasi cyber yang berasal dari luar yang menjalankan lab atau perintah militer mengandalkan komunitas peretas yang signifikan, lebih disukai berinteraksi melalui berbagai forum online (sebagai sarana untuk tinggal keduanyaanonim dan untuk menjangkau kolaborator yang tersebar secara geografis).

Distribusi dari Trojan Akses Remote MegalodonHTTP (RAT) memanfaatkan topi hitam amatir platform, HackForum. Lima orang yang dituduh membuat malware dan / atau distribusi tinggal di tiga negara Eropa yang membutuhkan penegakan hukum untuk bekerja sama internasional dalam mengejar penangkapan peretas jahat.

Internasional sifat domain-cyber organisasi yang bekerja sama dengan peretas jahat serta target internasional mereka melampaui tidak hanya kekuatan eksekutif teritorial, tetapi menambah pentingnya platform komunikasi virtual

1.1 Black Hat Hacker

Seorang hacker adalah orang yang dengan sengaja mengutuk jaringan komputer untuk menembus jaringan yang bukan haknya. Hacker adalah seorang peretas yang mendapatkan akses tidak sah ke sistem komputer untuk keuntungan pribadi. Tujuannya biasanya untuk mencuri data perusahaan, melanggar hak privasi, mentransfer dana dari rekening bank, dll.

1.2 Tujuan Black Hat Hacker

Melakukan hacking untuk mengambil data pribadi pengguna internet seperti password hingga nomor telepon. Mereka juga terkadang menyebarkan virus pada perangkat lain.Dari data pribadi yang dicuri tersebut mereka bisa mendapatkan keuntungan yang besar. Data-data tersebut jika dijual bisa memiliki harga yang sangat tinggi karena memang banyak yang menginginkannya. Tindakan tersebut jelas merugikan dan membahayakan sistem yang diretas.

1.3 Menghindari Serangan Hacker

1. Jangan Membagikan Data Pribadi Kamu Sembarangan

2. Gunakan VPN

VPN (Virtual Private Network) adalah sebuah layanan koneksi yang memungkinkan kamu untuk mengunjungi sebuah website dengan aman dan private.VPN bekerja dengan cara mengubah jalur koneksi melalui server dan menyembunyikan pertukaran data yang terjadi.

3. Matikan Jaringan WiFi atau Bluetooth Ketika Tidak Digunakan

4. Gunakan Jawaban Pertanyaan Keamanan Palsu

Kebanyakan orang akan membuat jawaban *Security Question* yang benar agar mudah untuk diingat.membuat *Security Question* yang mudah diketahui jawabannya, seperti nama orang tua, nama sekolah, dan lain-lain.

5. Aktifkan Enkripsi Disk Penuh Pada Komputer

Full Disk Encryption (FDE) adalah sebuah metode untuk mengenkripsi *hard drive* sedemikian rupa sehingga semua data pada *drive* selalu dienkripsi, tanpa menggunakan solusi enkripsi pihak ketiga.

6. Gunakan password yang kompleks

Gunakan password yang kompleks seperti campuran angka, huruf kapital, maupun simbol agar resiko terkena serangan hacker semakin rendah.

7. Jangan Gunakan Password yang Sama untuk Semua Akun

8. Periksa Permissions Aplikasi Sebelum di-Install

Cek apa saja izin akses yang diberikan dan pastikan aplikasi yang ingin kamu install tersebut tidak mengakses informasi yang tidak diperlukan.Misalnya, aplikasi mewarnai yang kamu akan install meminta akses ke kontak handphone kamu, maka harus kamu curigai.

2.1 Malicious Hackers

Peretas jahat menjadi semakin sadar akan metode analisis forensik. Akibatnya mereka sering menerapkan langkah-langkah balasan untuk mencegah penyelidik mengambil bukti yang berguna. Praktek ini disebut sebagai anti-forensik, atau kadang-kadang kontra forensik. Pada intinya praktik tersebut melibatkan menghilangkan atau mengaburkan bukti yang berkaitan dengan aktivitas kriminal atau

niat jahat. Dengan mengingat hal ini, fokus utama dari bagian ini adalah untuk membahas forensik penyimpanan media hard disk, dengan fokus pada pengidentifikasian tempat mengungkap bukti yang tersimpan di area media yang diformat secara tidak jelas; daerah yang kebal terhadap anti-forensik atau yang mungkin tidak dipertimbangkan oleh tersangka. Teknik analisis forensik yang khas juga dibahas secara singkat di bagian ini, dan karena meningkatnya toleransi pengadilan dalam menerima analisis RAM sebagaimana diizinkan, hal ini juga dibahas

3.2 Konsep protokol perentasan utama

1. Tetap legal, dapatkan persetujuan yang tepat sebelum mengakses dan melakukan penilaian keamanan.

2. Tentukan ruang lingkup, tentukan ruang lingkup penilaian sehingga pekerjaan peretas etis tetap legal dan dalam batas yang disetujui organisasi.

3. Laporkan kerentanan, beri tahu organisasi semua kerentanan yang ditemukan selama penilaian. Berikan saran perbaikan untuk mengatasi kerentanan ini.

4. Hormati sensitivitas data, bergantung pada sensitivitas data, peretas etis mungkin harus menyetujui perjanjian non-pengungkapan, di samping syarat dan ketentuan lain yang disyaratkan oleh organisasi yang dinilai.

DAFTAR PUSTAKA

[1] Conrad, J. (2012). Seeking help : the important role of ethical. *Network Security*, *2012*(8), 5–8. https://doi.org/10.1016/S1353-4858(12)70071-5

[2] Levy, S.: Hackers: Heroes of the Computer Revolution. Doubleday, New York, NY, USA 1984)

[3] Macdonald, M., Frank, R., Mei, J., Monk, B.: Identifying digital threats in a hacker web forum. In: Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015, ASONAM '15, pp. 926–933. ACM, New York, NY, USA (2015)

[4] Stallings, W., and Brown, L. 2008. Computer Security: Principles and Practice, Upper Saddle River, NJ: Prentice Hall.

[5] The Honeynet Project. *Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community*. Addison-Wesley, Boston, 2002.