IMPLEMENTASI USB HID KEYBOARD ATTACKS DENGAN REMOTE PENETRATION TEST PADA KALI NET HUNTER

IMPLEMENTATION USB HID KEYBOARD ATTACKS WITH REMOTE PENETRATION TEST ON KALI NET HUNTER

Muhammad Dzulkarnaen[1], Mochammad Fahru Rizal [2], Setia Juli Irzal Ismail [3]

[1,2,3]Prodi D3 Teknik Komputer, Fakultas Ilmu Terapan, Universitas Telkom

[1]mdzulkarnaen@student.telkomuniversity.ac.id, [2]mfrizal@tass.telkomuniversity.ac.id
[3]julismail@tass.telkomuniversity.ac.id

Abstrak

Linux dapat dikatakan biasa digunakan untuk melakukan kegiatan pengujian penetrasi pada suatu sistem. Pada proyek akhir ini akan diperkenalkan cara baru untuk melakukan hacking atau pengujian penetrasi pada sebuah sistem dengan menggunakan smartphone. Smartphone yang biasa menggunakan system operasi android tersebut akan di flash ulang sehingga dapat menggunakan sistem operasi yang hampir sama dengan Linux yaitu Kali Net Hunter. Kemudian jika Kali Net Hunter telah ter-install pada smartphone tersebut akan dilakukan pengujian dengan menggunakan HID keyboard attack, yaitu penyerangan untuk merekam keylogger pada sebuah browser. Penyerangan dilakukan dengan cara menghubungkan smartphone dengan laptop korban dengan kabel USB dan menanamkan exploit pada laptop korban, kemudian penyerangan dilakukan dengan menggunakan metasploit. Ketika korban mengetikkan username dan password saat melakukan login maka akan terekam.

Kata Kunci: ***Kali Net Hunter, HID Keyboard Attack, Metasploit, penetration***

Abstract

Linux also can be used to perform penetration testing on a system. Remember if a hacker or someone who wants to doing a penetration test require needs a laptop to do such activities on a site adjacent to the target will give rise to suspicion, then that is considered less effective way to conduct such activities, so there is this final project will be introduced a new way to perform penetration testing or hacking on a system by using smartphone. The usual Smartphone using the android operating system in flash reset so can use almost the same operating system with Linux i.e. Kali Net Hunter. Then if the Kali Net Hunter has been installed on a smartphone will be testing using the HID keyboard attack, that assault to record a keylogger on a browser. The assault was conducted by way of a connecting victims with laptop with smartphone USB cable and embed code on the victim's laptop, then attacks is done using metasploit. When victims type in the username and password during login it will be recorded.

Keywords: Kali Net Hunter, HID Keyboard Attack, Metasploit, penetration test..

1. Pendahuluan

1.1. Latar Belakang

Linux adalah sistem operasi yang didistribusikan secara open source. Sistem operasi Linux kebanyakan digunakan untuk melakukan uji penetrasi pada keamanan suatu sistem yang telah dibuat. [1].

Mengingat pada saat ini uji penetrasi atau proses hacking terkadang sulit untuk mencari alamat IP target yang diinginkan dan harus menggunakan laptop. Teknologi terbaru yang ada yaitu dapat membawa Kali Linux hanya dalam genggaman tangan dengan cara menerapkan sistem operasi Kali Linux pada sebuah smartphone Android. Sistem operasi tersebut adalah Kali Net Hunter[1]. Secara garis besar Kali Net Hunter setara dengan sistem operasi Kali Linux, Kali Net Hunter juga memiliki banyak tools untuk proses hacking, seperti yang akan diangkat pada topik proyek akhir ini yaitu USB HID keyboard attacks. Singkatnya, HID keyboard attacks merupakan tools yang disediakan kali net hunter untuk melakukan beberapa proses hacking dengan cara menghubungkan smartphone penyerang pada laptop korban dengan kabel USB dengan berpura-pura charge smartphone tersebut di laptop korban, kemudian memberikan exploit didalamnya dan exploit akan menanamkan payload untuk memasang backdoor pada komputer target, salah satu proses hacking yang akan digunakan adalah keyscan atau merekam kegiatan keyboard pada saat korban mengakses suatu web browser tertentu di komputer target [2]. Kemudian akan dilakukan remote penetrasi dengan menggunakan Real VNC untuk jika ingin melakukan kegiatan tersebut dari jarak yang tidak berdekatan dengan laptop target[3].

Berdasarakan permasalahan diatas, maka akan dibuatlah sebuah alat yang dapat menjaga kondisi kolam dan pemberian makan yang sesuai. Jika kolam berada pada kondisi yang tidak baik maka sistem ini akan melakukan tindakan agar kondisi kembali ke kondisi netral. Sistem ini juga dapat memberikan pakan ikan secara otomatis, yang dapat diatur pemberian pakannya.

Pada proyek akhir ini akan mengimplementasikan USB HID keyboard attacks dengan penetration test pada Kali Net Hunter ini sebagai bahan penelitian dan pembelajaran. Bukan untuk mengajarkan suatu kejahatan atau hal buruk lainnya. Karena diharapkan juga untuk waspada terhadap apapun yang berhubungan dengan keamanan.

1.2. Rumusan Masalah

Dari berbagai uraian diatas maka ditarik rumusan masalah antara lain :

1. Bagaimana mengimplementasikan kali net hunter pada *smartphone* Android?
2. Bagaimana cara kerja dari USB HID *Keyboard attacks*?
3. Bagaimana melakukan *remote penetration test* dengan VNC viewer?

1.3. Tujuan

Adapun tujuan dari pembuatan proyek akhir antara lain :

1. Dapat mengaplikasikan kali net hunter pada *smartphone* Android.
2. Dapat mengetahui cara kerja dari USB HID *keyboard attacks*.
3. Dapat melakukan *remote penetration test* dengan menggunakan VNC viewer.

1.4. Batasan Masalah

Adapun batasan masalah dari proyek akhir ini, yaitu :

1. Hanya membahas tentang USB HID *keyboard attacks* dan *remote penetration test* pada kali net hunter.
2. Menggunakan kali net hunter 3.15.
3. Menggunakan *smartphone* nexus 5.
4. Semua perangkat berada dalam satu jaringan yang sama.
5. Melakukan perekaman keylogger pada suatu web browser.
6. Exploitasi hanya dilakukan dengan metasploit.
7. Laptop atau komputer target dalam kondisi menyala dan tidak melakukan *reboot* .

2. Dasar Teori /Material dan Metodologi/perancangan

2.1. Anotomi Hacking

Anotomi hacking adalah langkah – langkah yang dilakukan dalam hacking, urutan anatomi hacking adalah footprinting, scanning, gaining access, escalating privilege, creating backdoor, DOS.

2.2. Kali Net Hunter

Kali Net Hunter merupakan salah satu sistem operasi terbaru yang dimiliki kali linux untuk beroperasi pada *smartphone*. Kali Net Hunter tersebut merupakan *project* pertama *open source android platform* yang difungsikan sebagai *penetration testing*. *Smartphone* yang biasa digunakan untuk menjalankan Kali Net Hunter ini adalah *smartphone* keluaran google Nexus dan One Plus. Kali Net Hunter dapat dikatakan sebagai Kali Linux mini karena kemampuannya setara dengan Kali Linux dan memungkinkan untuk diterapkan pada Android

2.3. Metasploit

Metasploit adalah *software security* yang digunakan untuk menguji coba ketahanan suatu sistem dengan cara mengeksploitasi kelemahan dari susatu sistem. Metasploit juga digunakan untuk melakukan penyerangan pada *application layer* dengan 0 day *attack* yang merupakan suatu metode penyerangan pada *software* yang belum di *patch*. Selain itu metasploit biasa dikaitkan dengan istilah *remote exploitation* atau dapat diartikan teknik penyerangan dari jarak jangkauan yang cukup jauh yang dapat mengendalikan komputer korban dengan cara penyerangan yang dilakukan metasploit mengirimkan exploit pada komputer korban. Exploit merupakan *software* yang berfungsi memanfaatkan kelemahan pada *software* (*Web Browser*), kemudian exploit akan menanamkan payload pada memori komputer korban. Payload adalah sebuah *executable* milik penyerang yang akan dijalankan pada komputer korban bertujuan untuk melakukan beberapa hal, seperti memasang *backdoor*, Trojan, virus, worm, dan lainnya.

2.4. Real VNC

Real VNC adalah *software* yang digunakan untuk *remote* komputer lain secara jarak jauh menggunakan koneksi jaringan Internet, dimana real VNC ini dapat digunakan disemua sistem operasi yaitu Windows, Linux maupun Macintosh maupun Android. *Software* ini terdiri dari 2 yaitu realVNC Server (untuk membuat server VNC) dan VNC *Viewer* (untuk *remote* VNC server).

2.5. Keylogger

Keylogger merupakan *software* yang dapat melakukan perekaman sinyal yang diperoleh dari proses pengetikan secara langsung yang berhubungan dengan DMA (*derect memory access)* atau *interrupt.* Contohnya dapat berupa angka

heksadecimal yang dikirimkan pada *processor* untuk di proses atau dieksekusi, dapat melakukan *capture* setiap *keystroke* yang ditransmisikan oleh OSK (*on screen keyboard*) kepada aplikasi tujuan dengan cara merekam *pointer* yang ditujukan pada *pixel* atau gambar yang terdapat pada OSK

2.6. Windows

Sistem operasi Windows adalah sistem operasi yang dikembangkan oleh Microsoft Coporation dengan berbasis GUI (*Graphical User Interface*) atau tampilan antarmuka bergrafis. Sistem operasi Windows telah berevolusi dari MS-DOS, sebuah sistem operasi berbasis modus teks dan *command-line*.

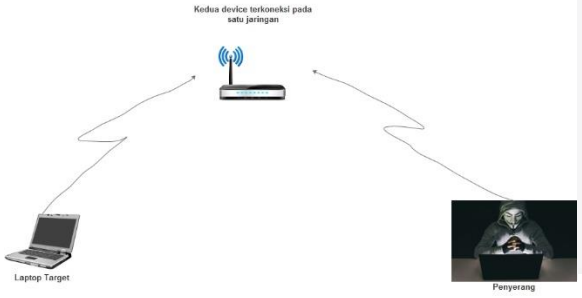
3. Analisis dan Perancangan

3.1. Analisis

Pada bagian analisis ini akan dijelaskan bagaimana gambaran system saat ini, blok diagram beserta cara kerjanya. Juga menganalisis kebutuhan apa saja yang digunakan oleh system.

3.2. Gambaran Sistem Saat Ini

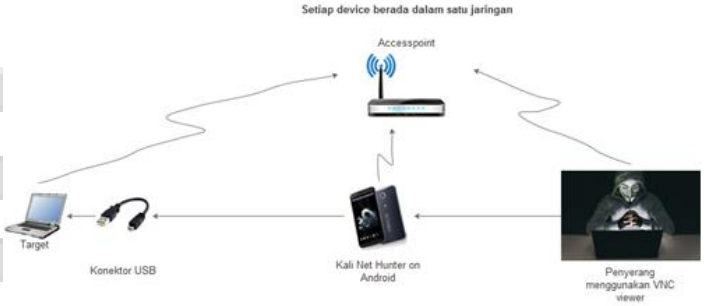
Saat ini kebanyakan orang untuk melakukan *penetration test* atau proses *hacking* masih mengunakan komputer atau laptop *device* utama penyerangan, dengan dukungan sistem operasi berbasis Kali Linux. Melakukan *penetration test* dan *hacking* dilakukan dengan jarak yang tidak berdekatan dari laptop korban, tetapi jika kondisinya melakukan *penetration test* dan *hacking* pada ruang lingkup yang kecil maka akan sangat merepotkan penyerangan dan dapat menimbulkan kecurigaan dari target.



Gambar 3-1 Sistem saat ini

3.3. Perancangan

Adapun konsep pembangunan sistem baru usulan yang akan dibuat adalah sebagai berikut :



Gambar 3-2 Sistem usulan

3.4. Cara Kerja Sistem

Cara kerja sIstem USB HID *Keyboard Attack* ini sebagai berikut, ketika menghubungkan *Smartphone* dengan laptop korban menggunakan kabel USB sebagai *social engineer*, kemudian mengeksekusi *tools* yang terdapat pada kali net hunter yaitu HID *Attack*. Setelah di eksekusi maka exploit akan ditanamkan pada laptop korban, kemudian payload akan membuat *backdoor* pada laptop korban. Setelah itu penyerangan akan dilakukan dari laptop Lain dengan menggunakan VNC *viewer* sehingga penyerangan dapat dilakukan dari jarak yang tidak berdekatan dari target agar mengurangi rasa curiga dari *victim*.

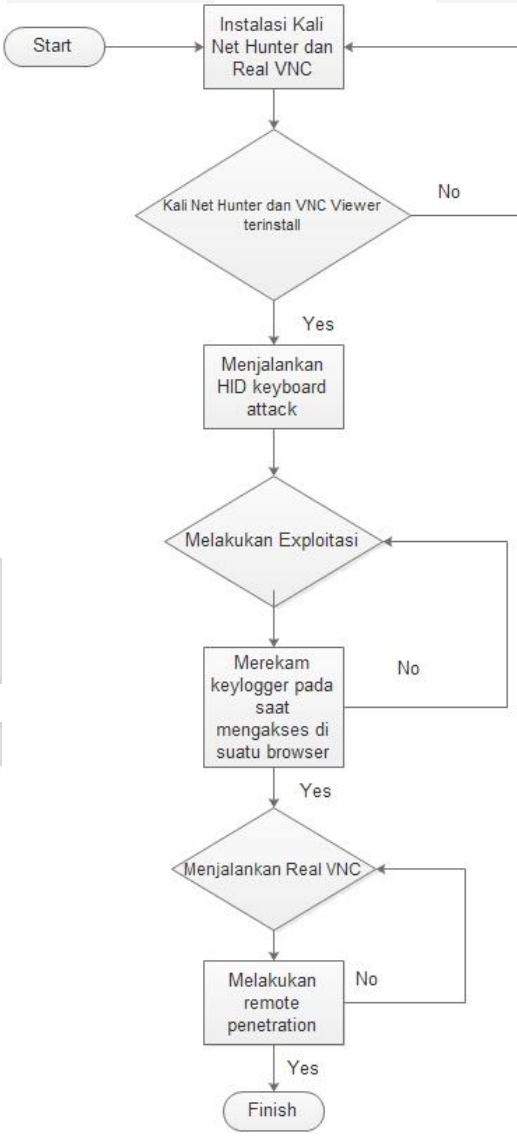
3.5. Kebutuhan Sistem

Adapun kebutuhan Perangkat Peras & Perangkat Lunak yang dibutuhkan ialah sebagai berikut :

Tabel 3.1 Kebutuhan Sistem

Perangkat Keras	Perangkat Lunak
• Laptop	• Kali Net Hunter
• Smartphone Nexus 5	• Windows
• USB kabel	• Real VNC

3.6. Flowchart Sistem Usulan

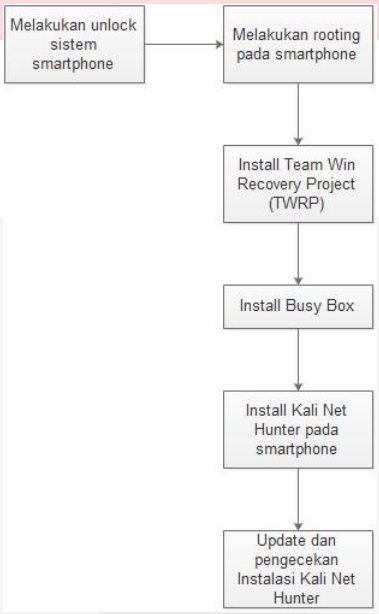


Gambar 3-3 Flowchart usulan

4. Pengujian dan Implementasi

Pada tahap pengujian dijelaskan tentang proses pengujian yang dilakukan ke sistem yang dibangun. Pengujian ini dilakukan dalam beberapa skenario. Skenario pertama dilakukan pada terminal yang terdapat pada *smartphone* langsung, dan pengujian kedua dilakukan remote penetrasi dari mesin lain dengan menggunakan *software* real VNC. Pengujian ini lebih fokus terhadap perekaman *keylogger* yang diinputkan dari *keyboard on board, keyboard on screen, Keyboard external USB cable, Keyboard external Wi-Fi.*

4.1. Implementasi



Gambar 4-1Implementasi

4.2. Langkah Pengerjaan

Langkah pengerjaan akan menjelaskan tentang tahap dari awal hingga akhir pada sistem, langkah pertama adalah melakukan unlock sistem smartphone → melakukan rooting pada smartphone → Install Team Win Recovery Project (TWRP) → Install Busy Box

4.3. Skenario Pengujian 1

1. Melakukan *Social Engineering* kepada *victim.*
2. Menghubungkan setiap *device* dalam satu jaringan
3. Menghubungkan *smartphone* dengan laptop *victim* menggunakan USB kabel.
4. Menjalankan Metasploit pada terminal *smartphone.*
5. Menentukan exploit yang akan diberikan pada korban.
6. Menentukan Payload yang akan memasangkan *backdoor* pada *victim.*
7. Mengeksekusi exploit
8. Mengeksekusi hid attack
9. Melakukan keyscan saat victim mengakses suatu web browser.

4.4. Pengujian 1

Pengujian 1 dilakukan oleh penulis yang bertujuan untuk merekam *keylogger* pada saat *victim* mengetikan *username* dan *password* akun gmail pada suatu *web browser* dengan menggunakan terminal pada *smartphone*.

4.5. Skenario Pengujian 2

1. Melakukan *Social Engineering* kepada *victim.*
2. Menghubungkan setiap *device* dalam satu jaringan
3. Menjalankan VNC server dan VNC viewer dan melakukan remote para terminal *smartphone*
4. Menghubungkan *smartphone* dengan laptop *victim* menggunakan USB kabel.
5. Menjalankan Metasploit pada terminal *smartphone.*
6. Menentukan exploit yang akan diberikan pada korban.
7. Menentukan Payload yang akan memasangkan *backdoor* pada *victim.*
8. Mengeksekusi exploit
9. Mengeksekusi hid attack
10. Melakukan keyscan saat victim mengakses suatu web browser.

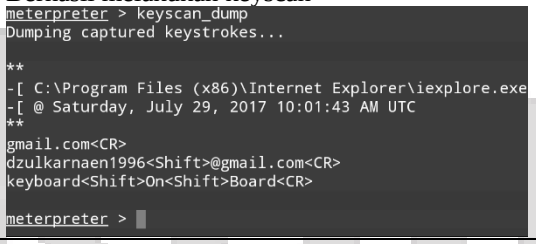
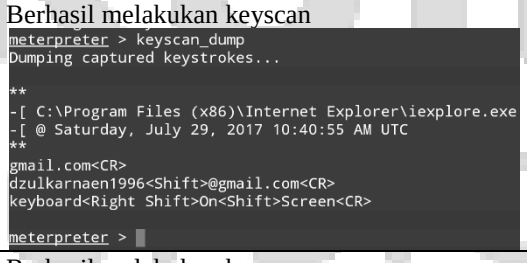
4.6. Pengujian 2

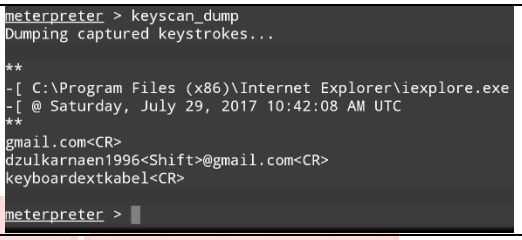
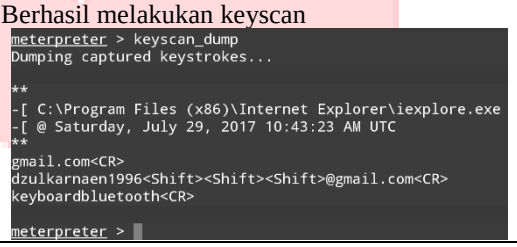
Pengujian 2 dilakukan oleh penulis yang bertujuan untuk merekam *keylogger* pada saat *victim* mengetikan *username* dan *password* akun gmail pada suatu *web browser* dengan *remote* penetrasi pada mesin lain menggunakan *Real* VNC.

4.7. Hasil Pengujian

Berikut adalah tabel hasil pengujian *keyscan* pada keyboard yang berbeda jenis.

Gambar 4-2Tabel Hasil Pengujian

No	Jenis Pengujian	Keterangan	Protokol yang digunakan
1	*Keyboard on board* 	Berhasil melakukan keyscan 	HID *Protocol*
2	*Keyboard on screen* 	Berhasil melakukan keyscan 	HID *Protocol*
3	*Keyboard external USB cable*	Berhasil melakukan keyscan	HID *Protocol*

			
4	*Keyboard Bluetooth* 	Berhasil melakukan keyscan 	HID *Protocol*

5. Kesimpulan dan Saran

5.1. Kesimpulan

Setelah melakukan analisis, perancangan dan pengujian "IMPLEMENTASI USB HID KEYBOARD ATTACKS DENGAN REMOTE PENETRATION PADA KALI NET HUNTER" dapat ditarik kesimpulan sebagai berikut:

1. Dapat merekam dan mengetahui *username* dan *password* akun gmail pada seseorang saat mengakses menggunakan *browser* internet explorer.
2. Dapat melakukan *remote* dengan menggunakan VNC untuk melakukan *test penetration.*
3. Dapat tetap merekam *keylogger* pada saat *victim* menggunakan *keyboard on board*, *keyboard on screen*, *Keyboard external USB cable*, *Keyboard external bluetooth.*

5.2. Saran

Adapun saran dari sistem yang dibangun, yaitu:
Pada sistem yang telah dibuat perlu dilakukan perkembangan agar HID *attack* pada Kali Net Hunter dapat dilakukan walaupun tidak berada dalam satu jaringan.

6. Daftar Pustaka

[1] B. Sahare, A. Naik, dan S. Khandey, "Study Of Ethical Hacking," *Int. J. Comput. Sci. Trends Technol.*, vol. 2, no. 4, hal. 6–10, 2014.

[2] MUTS, "Kali Linux - Penetration Testing Platform," *Kali Linux*, 2013. [Daring]. Tersedia pada: http://www.kali.org/penetration-testing/kali-linux-penetration-testing-platform/.

[3] Offensive Security, "What is Kali Linux," *Kali Linux Documentation*. 2013.

[4] Rapid7, "Penetration Testing Software | Metasploit," *Metasploit*, 2004. [Daring]. Tersedia pada: https://www.metasploit.com/.

[5] C.-L. Tsao, S. Kakumanu, dan R. Sivakumar, "SmartVNC: an effective remote computing solution for smartphones," *Proc. 17th Annu. Int. Conf. Mob. Comput. Netw. - MobiCom '11*, hal. 13, 2011.

[6] L. Notenboom, "No Title," *Keylogger*, no. Will Using an On-Screen Keyboard Stop Keyloggers, 2009.

[7] M. L. Baihaqi, "No Title," *ROTOKOL Jar. Komput.*, hal. 10, 2013.

[8] J. De Clercq dan G. Grillenmeier, *Microsoft Windows Security Fundamentals*. 2007.