IMPLEMENTASI *BADUSB MITM ATTACKS* MENGGUNAKAN *REMOTE PENETRATION TEST* PADA KALI NETHUNTER

Iqbal Zulfikar Muhammad — Telkom University — iqbalzulfikar64@gmail.com

Moch Fahru Rizal,S.T., M.T — Telkom University — mfrizal@tass.telkomuniversity.ac.id

Mia Rosmiati,S.Si., M.T. — Telkom University — mia@tass.telkomuniversity.ac.id

Abstrak

Penetration testing merupakan suatu tindakan atau perilaku dimana dilakukannya pengujian terhadap suatu sistem. Tujuannya adalah untuk mendapatkan celah keamanan pada suatu sistem, yang tentunya bermanfaat untuk pemilik atau produsen sistem tersebut. Pada proyek akhir kali ini akan mengimplementasi Kali NetHunter yang berplatform pada Android device sebagai device utama penetration testing. Penyerangannya menggunakan metode BadUSB MITM Attack, yang membutuhkan spesifikasi hardware diantaranya smartphone jenis nexus atau smartphone lainnya yang support dengan ROM kali nethunter. Juga membutuhkan laptop yang nantinya menjadi korban atau client dan tentunya kabel USB untuk menyambungkan smartphone dan laptop. Sementara dari sisi kebutuhan software proyek kali ini membutuhkan installer atau ISO kali nethunter, wireshark, beberapa macam browser juga software atau tools yang nantinya akan menunjang dalam melakukan penetration testing. Hasil pengujian penetration test adalah diantaranya adalah berupa dapat diimplementasikannya BadUSB MITM attack, dapat mengcapture traffic jaringan dan mendapatkan credential data atau informasi penting korban seperti username dan password dari suatu website yang diakses.

Kata Kunci : ***Penetration Test, Kali NetHunter, BadUSB MITM Attack***

Abstract

Penetration testing is an action or behavior in which the testing of a system. The purpose is to get a security hole in a system, which is certainly beneficial to the owner or manufacturer of the system. In this final project it will implement Kali NetHunter which is platform on Android device as the main device of penetration testing. The attack uses the BadUSB MITM Attack method, which requires hardware specifications such as smartphone type nexus or other smartphones that support with ROM times nethunter. Also requires a laptop that will become a victim or client and of course a USB cable to connect smartphones and laptops. While in terms of software project needs this time requires the installer or ISO times nethunter, wireshark, some kind of browser software or tools that will later support in doing penetration testing. Penetration test results are among others can be the implementation of BadUSB MITM attack, can mengcapture network traffic and get credential data or important information victims such as username and password of a website accessed.

Keyword : Penetration Test, Kali NetHunter, BadUSB MITM Attack

Pendahuluan

Penetration test merupakan sebuah tindakan atau perilaku yang dilakukan untuk pengujian keamanan terhadap sebuah sistem. Usaha ini dimaksudkan untuk mendapatkan suatu celah keamanan pada sistem tersebut. Hasil pengujian yang didapat akan digunakan sebagai acuan untuk memperbaiki sistem tersebut.

Pada proyek akhir ini akan mengimplementasikan software sekelas Kali Linux pada smartphone berplatform andriod. Software tersebut adalah Kali NetHunter, sebuah software yang memiliki fungsionalitas seperti layaknya OS Kali Linux. Kali NetHunter memiliki banyak tools hacking didalamnya, diantaranya yang akan diangkat pada proyek akhir ini adalah tentang BadUSB MITM Attack. Orang awam pasti belum banyak mengetahui tentang tools ini, tools ini bisa menyerang siapapun tanpa diketahui. Sistem penyerangan BadUSB yaitu ketika ada orang yang ingin mencolokkan USB ke device kita yang alasannya mungkin ingin mentransfer data atau bahkan hanya ingin charging Handphone, kita pasti mengira itu hanyalah sebuah USB pada umumnya. Tetapi bisa saja orang tersebut mengincar informasi penting yang bisa didapat dengan metode serangan MITM Attack.

Pada proyek akhir ini akan mengimplementasi BadUSB MITM Attack tersebut sebagai bahan penelitian dan pembelajaran yang diharapkan nantinya dapat menghasilkan sebuah konsep keamanan agar dapat mengatasi MITM attack. Bukan untuk mengajarkan suatu kejahatan atau hal kriminal lainnya. Diharapkan juga nantinya bisa menjadi pengetahuan bagi khalayak umum supaya lebih waspada terhadap apapun yang berhubungan dengan keamanan device.

Tinjauan Pustaka

Kali NetHunter

Kali NetHunter adalah salah satu *software* rilisan Kali linux yang dapat beroperasi di smartphone android. Kali NetHunter tersebut merupakan *project pertama open source android platform* yang dikhususkan untuk *penetration testing*. Tetapi untuk sekarang hanya smartphone keluaran google Nexus dan One Plus saja yang dapat terinstall Kali NetHunter. Untuk smartphone lain mungkin sudah beberapa dilakukan percobaan tetapi masih bersifat non resmi. Dan juga sedang dalam tahap pengembangan.

Gambar 1 Kali Net Hunter

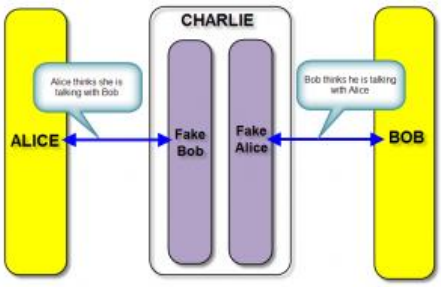
Kali NetHunter merupakan sebuah terobosan yang sangat dikatakan terbaru dan mungkin akan terus berkembang. Kali NetHunter bisa terbilang merupakan Kali Linux versi mini. Bayangkan kita mempunyai sebuah software yang mungkin kemampuannya setara dengan OS Kali Linux pada genggaman kita. Banyak hal yang mungkin kita bisa lakukan dengan Kali NetHunter ini.

Beberapa *tools* yang ada pada Kali NetHunter :

1. HID Keyboard Attack
2. BadUSB Man In the Middle Attack
3. Wireless Injection
4. Software Defined Radio support

Man In the Middle Attack

Serangan MITM adalah jenis serangan *cyber* dimana seseorang yang berbahaya mendaftarkan dirinya sendiri dalam sebuah percakapan antara dua pihak, mendengarkan percakapan kedua belah pihak dan memperoleh akses terhadap informasi bahwa kedua pihak sedang berusaha untuk mengirim satu sama lain.



Gambar 2 Skema proses MITM Attack

Sekarang mari lihat proses terjadinya MITM dalam contoh kasus Alice berkomunikasi dengan Bob. Charlie sebagai attacker akan berusaha berada di tengah antara Alice dan Bob. Agar Charlie berhasil menjadi orang ditengah, maka Charlie harus :

1. menyamar sebagai Bob dihadapan Alice
2. menyamar sebagai Alice dihadapan Bob

Dalam MITM, Alice mengira sedang berbicara dengan Bob, padahal dia sedang berbicara dengan Charlie. Begitu juga Bob, dia mengira sedang berbicara dengan Alice, padahal sebenarnya dia sedang berbicara dengan Charlie. Jadi agar bisa menjadi orang di tengah Charlie harus bisa menyamar di dua sisi, tidak bisa hanya di satu sisi saja. Maka dari itu serangan MITM ini bisa terbilang serang yang dilakukan secara aktif.

Sniffing

Sniffing merupakan metode penyerangan yang bertujuan melihat seluruh paket data yang lewat pada sebuah media komunikasi yang terhubung dengan yang lain lalu paket - paket tersebut disusun ulang sehingga data dikirimkan yang dikirimkan oleh seseorang dapat dilihat oleh orang yang melakukan sniffer. Sebuah sniffer dapat berupa kombinasi perangkat lunak dan perangkat keras. Perangkat lunak yang

digunakan dapat berupa sebuah perangkat lunak yang digunakan untuk analisis jaringan secara umum dengan pilihan-pilihan *debugging* yang sangat lengkap, atau dapat berupa sniffer yang sebenarnya. Sebuah sniffer harus diletakkan di dalam blok jaringan yang sama dengan jaringan yang menjadi sasaran. Dengan beberapa pengecualian, sniffer tersebut dapat diletakkan di mana saja di dalam jaringan sasaran.[6] Ada 2 jenis sifat sniffing yaitu sniffing aktif dan sniffing pasif. Sniffing aktif yaitu kegiatan yang dapat melakukan perubahan paket data dalam jaringan. Sedangkan Sniffing pasif yaitu kegiatan tanpa merubah data atau paket apapun dijaringan.

SSLSTRIP

Sslstrip adalah salah satu dari sekian banyak tools penetration. Tools ini merupakan demonstrasi atau implementasi tentang serangan pengupasan HTTPS yang Moxie Marlinspike sajikan di Black Hat DC 2009. Tools ini akan secara transparan membajak lalu lintas HTTP di jaringan, mengawasi tautan HTTPS dan pengalihan, lalu memetakan tautan tersebut ke tautan HTTP serupa atau homograf- Link HTTPS serupa. Sslstrip juga mendukung mode untuk memasok favorit icon yang terlihat seperti ikon kunci, selektif logging, dan penolakan sesi. [8]

Bagaimana ini bekerja? Arpspoof meyakinkan host bahwa alamat MAC kita adalah alamat MAC router, dan target mulai mengirimkan semua lalu lintas jaringannya. Kernel meneruskan semuanya kecuali lalu lintas yang ditujukan ke port 80, yang dialihkan ke $ listenPort (10000, misalnya)

VNC

Real VNC adalah software yang digunakan untuk meremote desktop pada computer menggunakan koneksi lokal jaringan Internet, dimana real VNC ini dapat digunakan disemua Operasi System yaitu Windows, Linux maupun Macintosh maupun android. Software ini terdiri dari 2 yaitu realVNC Server (untuk membuat server VNC) dan VNC Viewer (untuk meremote VNC server).

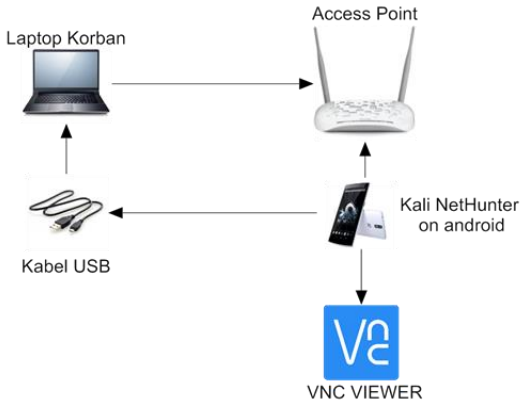
Gambar 3 VNC server untuk remote penetration

Analisis dan perancangan

Gambaran Sistem Saat Ini

Pada saat ini kebanyakan orang yang melakukan pentest atau hacking masih menggunakan laptop sebagai device utama. Biasanya didukung dengan operating system berbasis kali linux. Untuk melakukan pentesting dari jarak jauh cukup aman dengan menggunakan laptop/computer. Hal tersebut pasti akan lebih merepotkan pada saat melakukan penetration test jarak dekat atau pada satu ruang lingkup yang kecil. Maka pada proyek akhir ini akan menggunakan device yang lebih kecil atau sederhana yaitu alat komunikasi sehari-hari berupa smartphone android. Dan menggunakan Kali NetHunter sebagai tools penetrationnya.

Topologi Sistem



Gambar 4 Topologi sistem usulan

Gambar diatas merupakan gambaran sistem yang dibangun pada proyek ini membutuhkan device berupa Smartphone, khususnya pada proyek ini menggunakan jenis Smartphone keluaran google yaitu nexus 5. Pada smartphone ini nantinya akan dilakukan penginstalan Kali NetHunter diatas platform android yang menjadi default smartphone tersebut. Sehingga nantinya dapat mengimplementasi tools BadUSB MITM Attack yang ada pada Kali NetHunter. Pengimplementasian tools tersebut diharapkan akan dapat memonitoring dan mendapatkan data dari korban penetration testing yang dilakukan.

Implementasi dan Pengujian

Implementasi Kali NetHunter

Adapun implementasi pengerjaan dari sistem yang akan di bangun adalah sebagai berikut:

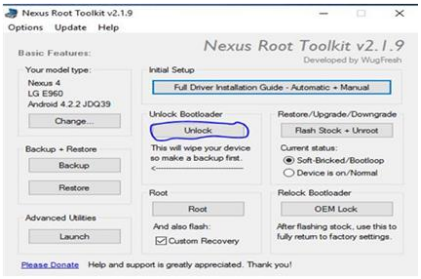
1. Melakukan Unlock dan Rooting Device
2. Instalasi BusyBox
3. Instal Kali NetHunter
4. Instalasi VNC server

1. Melakukan Unlock dan Rooting Device

Langkah-langkah cara unlock dan rooting device adalah sebagai berikut

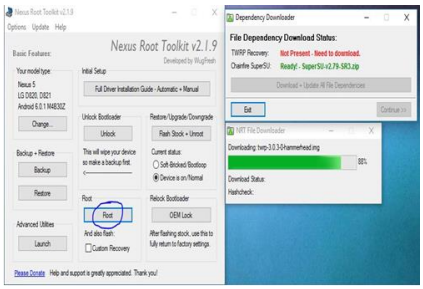
1. Membuka setting Handphone pada About Phone > Build number > Tekan 7 kali di times to become developer > Developer Options > USB Debugging > Click to enable USB Debugging.
2. Masuk ke FastBoot dengan cara menekan tombol Lock + Volume Up

3. Membuka Aplikasi Nexus Root Toolkit dan mengkilk Unlock. Maka hp dengan otomatisnya akan ter-unlock.



Gambar 5 Melakukan unlock device

4. Klik root untuk melakukan rooting device



Gambar 6 Melakukan rooting device

2. Instalasi *BusyBox*

Melakukan instalasi BusyBox dengan menggunakan playstore atau googlestore yang ada pada device android.

3. Instalasi Kali NetHunter

1. Mendownload Iso Kali NetHunter pada web kali linuxbpada website https://www.offensive-security.com/kali-linux-nethunter-download/ . Pastikan mendownload dengan benar dan tidak terjadi corrupt data untuk menghindari kegagalan instalasi atau fungsi kali nethunternya.

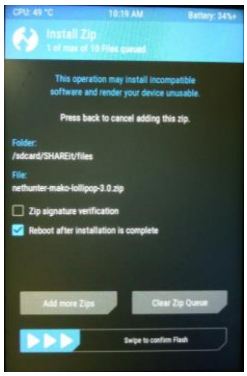
2. Masuk ke recovery twrp

   Masuk ke recovery TWRP yang sebelumnya sudah terinstall. Caranya dengan menekan tombol volume up dan tombol power secara bersamaan.

3. Mencari file image Kali Nethunter

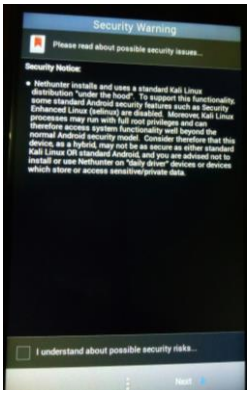
Gambar 7 Instalasi iso nethunter

4. Menginstall file kali nethunter



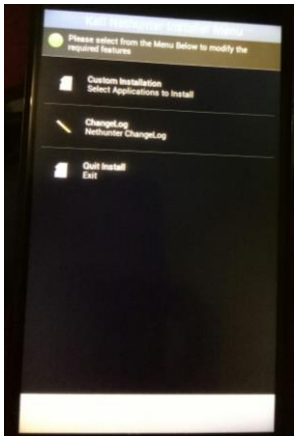
Gambar 8 Menginstal kali nethunter

5. Mengikuti alur penginstalan pada TWRP.



Gambar 9 Alur penginstalan klik ceklist lalu OK

6. Pada pilihan seperti gambar dibawah klik Costum Instalation



Gambar 10 Pilih custom instalation lalu ok

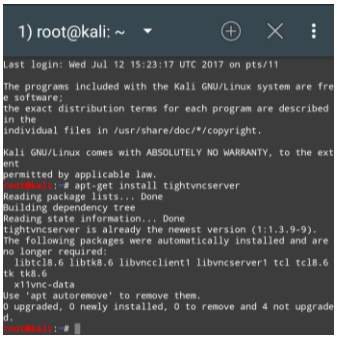
7. Kotak dialog akan muncul untuk memastikan software/aplikasi apa saja yang ingin diinstall. Selanjutnya klik Yes

Gambar 11 Klik yes untuk instalasi sampai selesai

4. Instalasi VNC server

Membuka terminal kali nethunter. Melakukan instalasi tightvncserver

"apt-get install tightvncserver"



Gambar 12 Melakukan instalasi VNC server

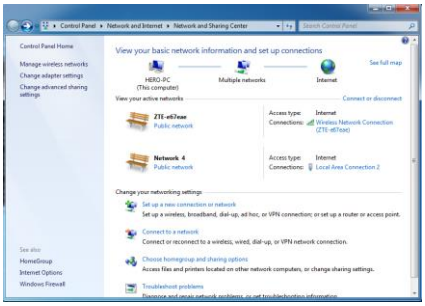
Pengujian

a. Pengujian BADUSB MITM ATTACK

1. Melakukan pengaktifan badusb attack

Gambar 13 Mengaktifkan BadUSB MITM

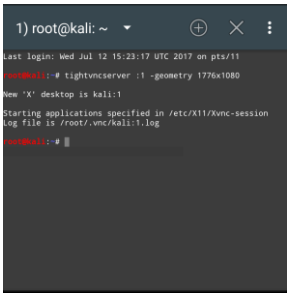
2. Hasil pengujian setelah badusb diaktifkan pada laptop korban terdapat adapter baru



Gambar 14 Hasil setelah BadUSB diaktifkan

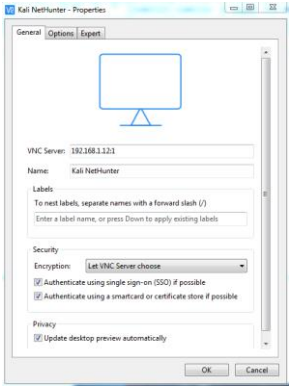
b. Pengujian remote penetration

1. Melakukan pengaktifan vnc server



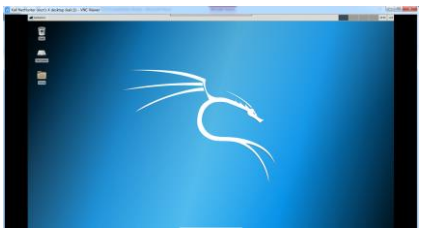
Gambar 15 Melakukan pengaktifan vnc server

2. Konfigurasi dari sisi remote



Gambar 16 Konfigurasi VNC pada sisi remote

3. Hasil VNC remote server



Gambar 17 Hasil remote vnc server

c. Pengujian SSLSTRIP

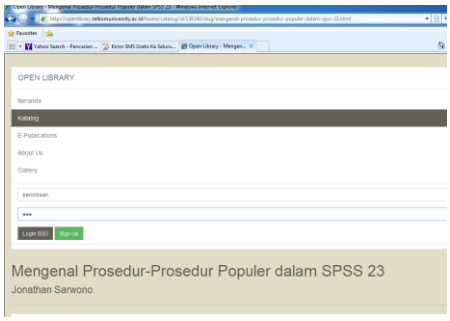
1. Langkah pertama mengaktifkan ip forwarding dengan mengetikkan perintah pada terminal vnc

   "echo 1 > /proc/sys/net/ipv4/ip_forward"

2. Langkah kedua membuat rules iptables dengan mengetikkan perintah pada terminal vnc

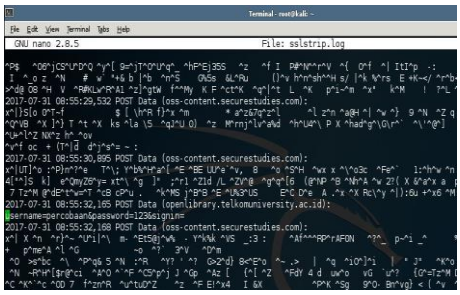
"iptables - t nat - A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080"

3. Langkah ketiga mengaktifkan sslstrip dengan perintah "sslstrip –l port"
4. Melakukan percobaan login pada laptop korban



Gambar 18 Melakukan percobaan login pada wesite protokol http

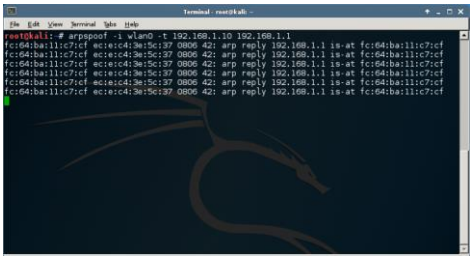
5. Hasilnya terdapat pada sslstrip.log



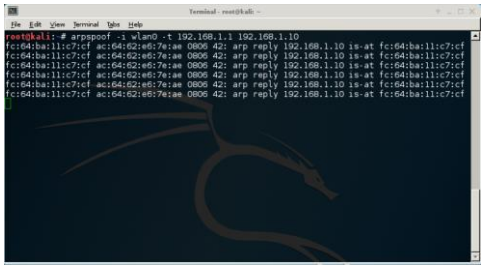
Gambar 19 Hasil sslstrip

d. Pengujian SSLSTRIP+

1. Melakukan NMAP pada jaringan untuk mendapatkan IP address korban
2. Melakukan Arpspoofing untuk menyamarkan mac address

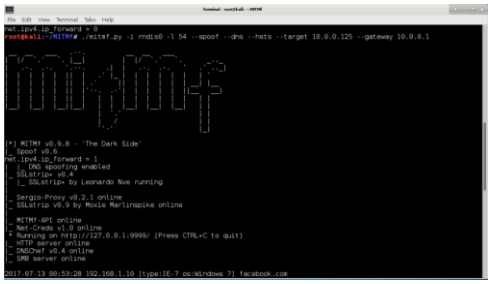


Gambar 20 Melakukan arpspoofing



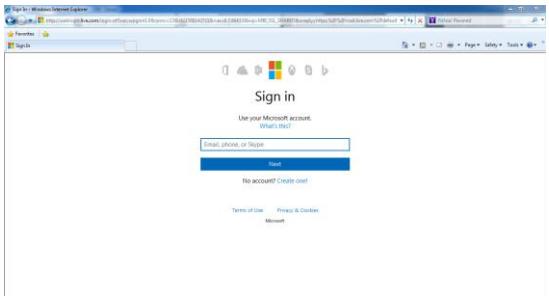
Gambar 21 Melakukan Arpspoofing

3. Melakukan pengaktifan sslstrip+



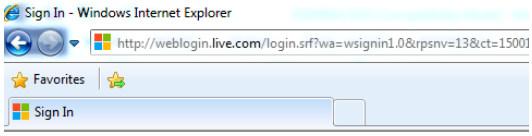
Gambar 22 Mengaktifkan SSLSTRIP+ pada MITMf

4. Melakukan percobaan login pada sisi korban



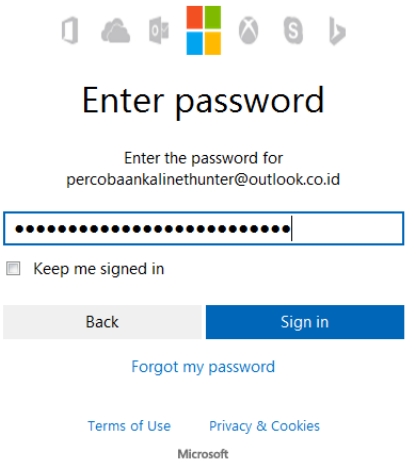
Gambar 23 Melakukan percobaan pada wesite hotmail

5. Hasil redirect https ke http



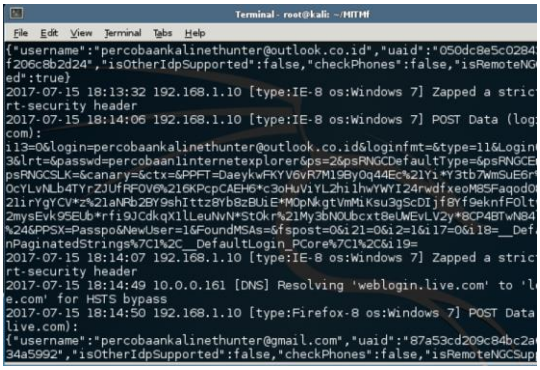
Gambar 24 Redirect https ke http

6. Masukkan username dan password pada website Hotmail yang sudah terdirect ke http



Gambar 25 Melakukan percobaan login pada website Hotmail

7. Hasil yang bisa dilihat secara realtime pada terminal



Gambar 26 Hasil sslstrip+ pada website hotmail yang berprotokol https

Kesimpulan

Pada proyek akhir ini penulis menarik beberapa kesimpulan yang didapat dari pengujian bab 4 :

1. Injeksi BadUSB MITM Attack pada kali nethunter berhasil dilakukan.
2. Hasil pengujian yang didapat adalah berupa password pada suatu web.
3. Jenis web yang bisa di bypass passwordnya adalah web dengan protokol keamanan HTTP, sementara HTTPS tidak bisa.

Saran

Saran penulis pada proyek akhir kali ini yaitu :

1. Pada pengembangan selanjutnya bisa berfokus pada implementasi sebuah sistem yang dapat mendeteksi sekaligus bisa mencegah penetration test BadUSB Man In The Middle Attack.

2. Mengimplementasi BadUSB dengan menggunakan Arduino Micro/Malduino

3. Serta mengembangkan juga pola penyerangan Man In The Middle Atttack.

Daftar Pustaka

[1] K. Linux, "Kali Linux NetHunter for Nexus and OnePlus," [Online]. Available: https://www.kali.org/kali-linux-nethunter/.

[2] K. NetHunter, "Android Mobile Penetration Testing Platform," 6 January 2016. [Online]. Available: https://www.offensive-security.com/kali-nethunter/nethunter-3-0-released/.

[3] Srlabs, "USB peripherals can turn against their users," [Online]. Available: https://srlabs.de/bites/usb-peripherals-turn/.

[4] D. Kearns, "NetHunter BadUSB Attack," 6 January 2016. [Online]. Available: https://github.com/offensive-security/kali-nethunter/wiki/NetHunter-BadUSB.

[5] W. H. Encyclopedia, Man-in-the-middle attack, World Heritage Encyclopedia.

[6] T. W. Onno W. Purbo, Buku Pintar Internet: Keamanan Jaringan Internet, Elex Media Komputindo, 2000.

[7] C. Sanders, PRACTICAL PACKET ANALYSIS 2ND EDITION Using Wireshark to Solve Real-World Network Problems, San Fransisco, 2011.

[8] M. Marlinspike, "Software > SSLSTRIP," 2012. [Online]. Available: https://moxie.org/software/sslstrip/.