**LAPORAN PRAKTIKUM**

**BETTERCAP**

****

**DISUSUN OLEH :**

Nama : Diki Candra

Nim : 2022903430010

Kelas : TRKJ 2B

Jurusan : Teknologi Informasi dan Komputer

Program Studi : Teknologi Rekayasa Komputer Jaringan

Dosen Pengajar : Atthariq, SST.,M.T.

**JURUSAN TEKNOLOGI INFORMASI DAN KOMUNIKASI**

**PRODI TEKNOLOGI REKAYASA KOMPUTER DAN JARINGAN**

**POLITEKNIK NEGERI LHOKSEUMAWE**

**TAHUN 2023**

**LEMBARAN PENGESAHAN**

Laporan Yang Berjudul : Bettercap

Disusun Oleh : Diki Candra

NIM : 2022903430010

Tanggal Praktikum : 7 Desember 2023

Tanggal Penyerahan : 14 Desember 2023

Jurusan : Teknologi Informasi & Komputer

Program Studi : Teknologi Rekayasa Komputer Jaringan

Mata Kuliah : Cybersecurity fundamental

Tabel Penilaian : :

Mengetahui,

Dosen Pembimbing, Penyusun,

Atthariq, SST.,M.T. Diki Candra

NIP. 197807202001121001 NIM. 2022903430010

1. **Teori**

Bettercap adalah sebuah alat (tool) sumber terbuka yang digunakan untuk melakukan uji penetrasi atau pengujian keamanan pada jaringan komputer. Alat ini dikembangkan dalam bahasa pemrograman Go dan berfungsi sebagai platform untuk melakukan serangan terhadap jaringan, serta menganalisis keamanan sistem.

Beberapa fitur utama dari Bettercap melibatkan kemampuan untuk melakukan serangan Man-in-the-Middle (MITM), sniffing (memata-matai) paket data, dan melakukan serangan terhadap protokol-protokol jaringan tertentu. Bettercap juga dapat digunakan untuk mengumpulkan informasi mengenai perangkat yang terhubung ke jaringan, termasuk perangkat keras dan perangkat lunak yang sedang berjalan.

Walaupun Bettercap dapat digunakan untuk tujuan-tujuan positif seperti mengidentifikasi kelemahan keamanan dalam suatu jaringan dan membantu organisasi meningkatkan keamanan mereka, perlu dicatat bahwa alat ini juga dapat disalahgunakan untuk aktivitas ilegal atau merugikan. Oleh karena itu, Bettercap atau alat serupa sebaiknya hanya digunakan oleh para profesional keamanan komputer atau dalam konteks yang sah dan etis.

**II. Alat/Bahan**

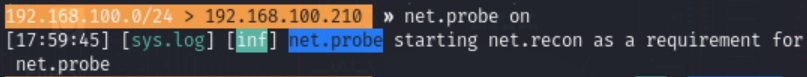
Alat dan bahan yang diperlukan dalam praktikum ini adalah perangkat hardware dan sofware yaitu:

1. Komputer/Labtop
2. Virtual box
3. Kali linux

**III. Prosedur Praktikum**

1. Siapkan komputer/labtop .
2. Siapkann Sistem operasi kali linux.
3. Bukalah aplikasi bettercap di kali linux.
4. Lalu ketik “**net.probe on”.**

net.probe on pada Bettercap mengaktifkan fitur pemindaian jaringan WiFi yang secara terus-menerus mendeteksi dan memantau perangkat yang terhubung ke jaringan. Fitur ini berguna untuk identifikasi perangkat, analisis keamanan, dan pemantauan real-time. Penting untuk digunakan dengan izin dan etika keamanan jaringan.



1. Lalu ketik “**net.show”.**

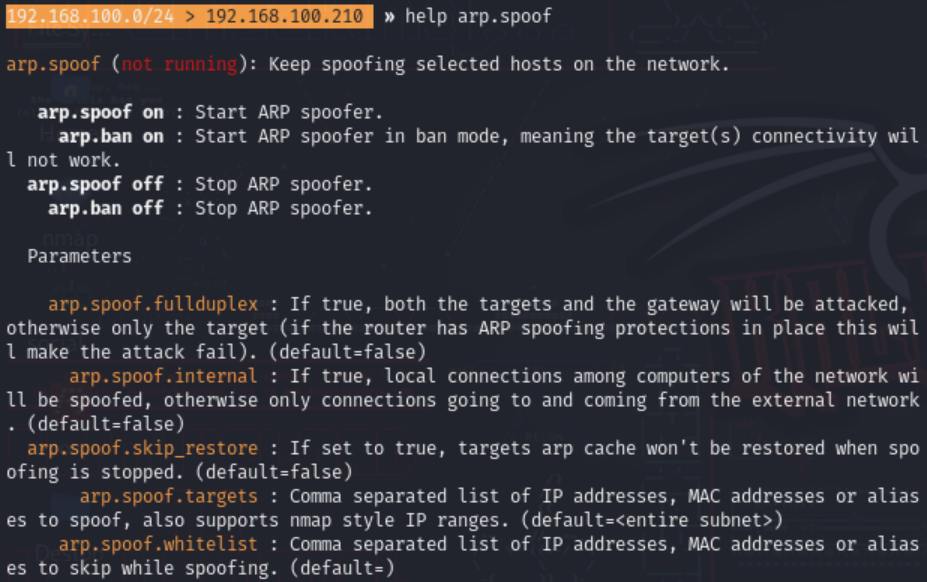
* Dalam Bettercap pada Kali Linux, perintah **net.show** digunakan untuk menampilkan informasi tentang perangkat yang terhubung ke jaringan. Ini memberikan tampilan ringkas yang mencakup alamat IP, alamat MAC, dan informasi lainnya tentang perangkat yang terdeteksi. Perintah ini berguna untuk memonitor dan menganalisis perangkat dalam jaringan selama sesi Bettercap.



1. Kemudian ketik **“ help arp.spoof”**

* Perintah help arp.spoof pada Bettercap di Kali Linux memberikan panduan atau bantuan singkat terkait modul "arp.spoof". Modul ini umumnya digunakan untuk melakukan serangan Man-in-the-Middle (MITM) menggunakan teknik ARP spoofing, di mana Bettercap mengirimkan paket-paket ARP palsu ke jaringan untuk mengelabui perangkat-perangkat di dalamnya.

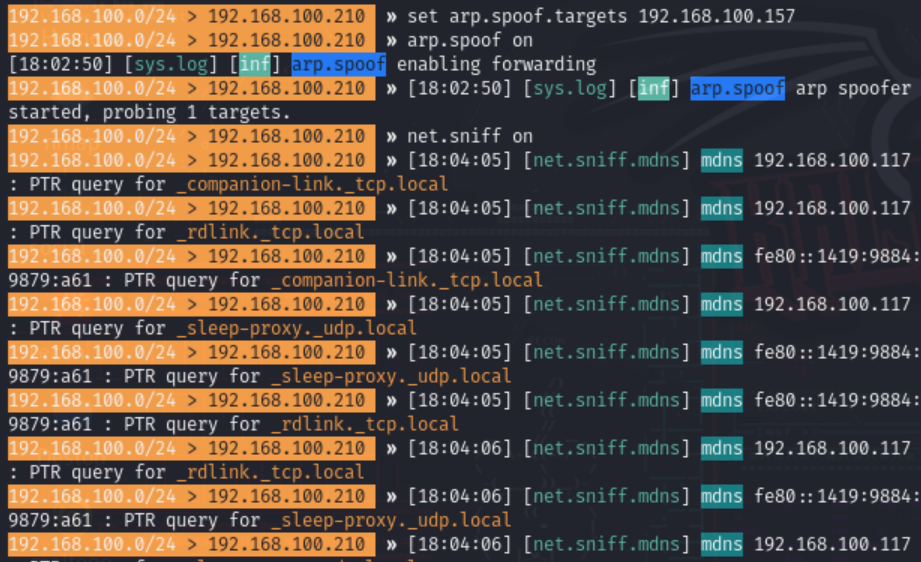
Informasi yang mungkin diberikan oleh perintah ini termasuk opsi-opsi konfigurasi, sintaksis perintah, dan penjelasan singkat tentang cara menggunakan modul "arp.spoof". Penggunaan modul ini harus dilakukan dengan hati-hati dan hanya dalam konteks uji penetrasi atau kegiatan keamanan yang sah.



1. Lalu ketik **“set arp.spoof.targets 192.168.100.157”**

* Perintah set arp.spoof.targets 192.168.100.157 pada Bettercap digunakan untuk menetapkan target ARP spoofing, yaitu perangkat dengan alamat IP 192.168.100.157. Dengan mengatur target ini, Bettercap akan fokus pada melakukan serangan Man-in-the-Middle (MITM) pada perangkat tersebut, mengelabui jaringan dengan mengirimkan paket ARP palsu.

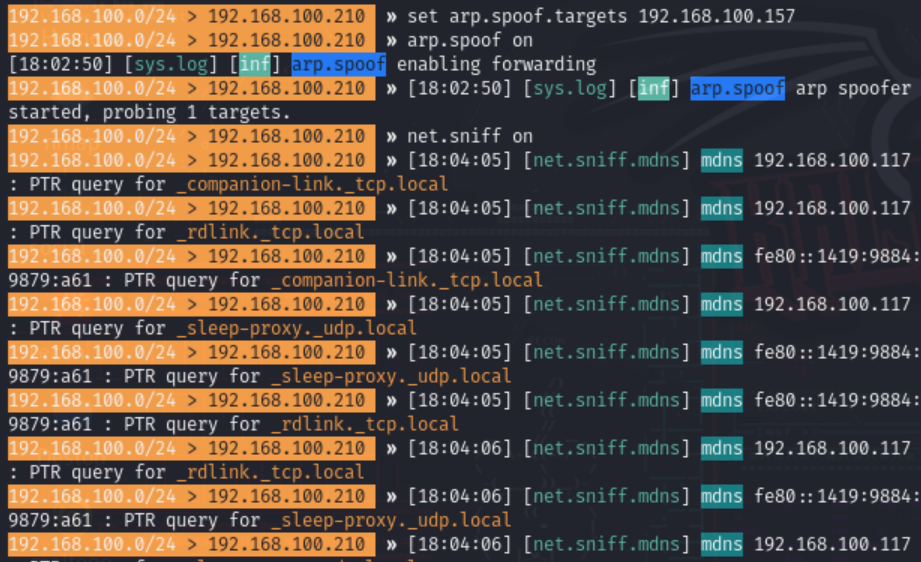
Perlu diingat bahwa penggunaan perintah semacam ini harus dilakukan dengan hati-hati dan hanya dalam konteks uji penetrasi yang sah atau kegiatan keamanan yang diizinkan. ARP spoofing dapat digunakan untuk tujuan jahat, oleh karena itu, pastikan untuk memahami dan mematuhi etika serta regulasi yang berlaku**.**



1. Lalu ketik **“arp.spoof on”.**

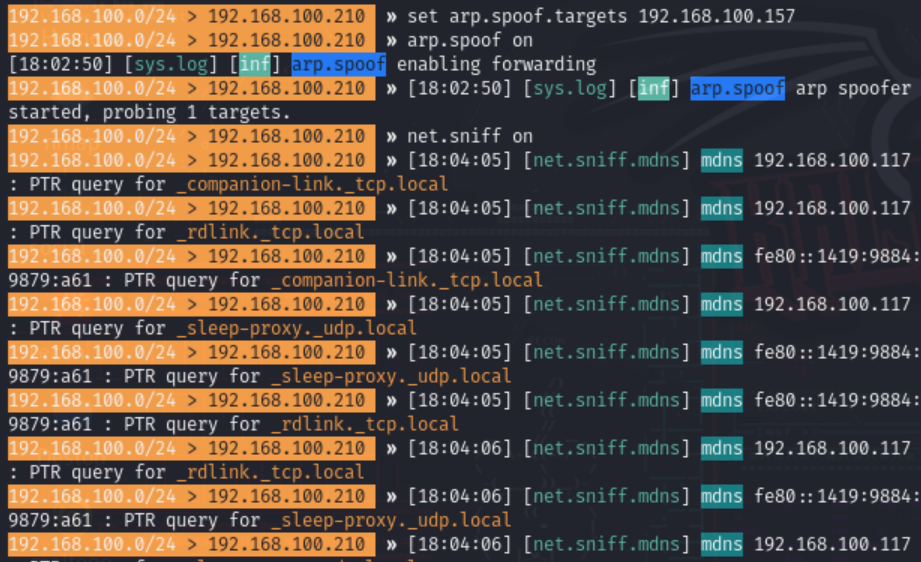
* Perintah arp.spoof on pada Bettercap diaktifkan setelah menetapkan target ARP spoofing. Perintah ini secara efektif memulai serangan Man-in-the-Middle (MITM) menggunakan teknik ARP spoofing. Bettercap akan mengirimkan paket-paket ARP palsu ke jaringan untuk mengelabui perangkat-perangkat di dalamnya, membuatnya percaya bahwa Bettercap adalah gateway atau perangkat lain yang sah.

Penting untuk dicatat bahwa penggunaan ARP spoofing atau teknik MITM lainnya harus dilakukan dengan izin dan etika yang ketat, seperti dalam uji penetrasi atau pengujian keamanan yang diizinkan. Penyalahgunaan teknik ini dapat merugikan dan melanggar hukum serta etika keamanan jaringan.



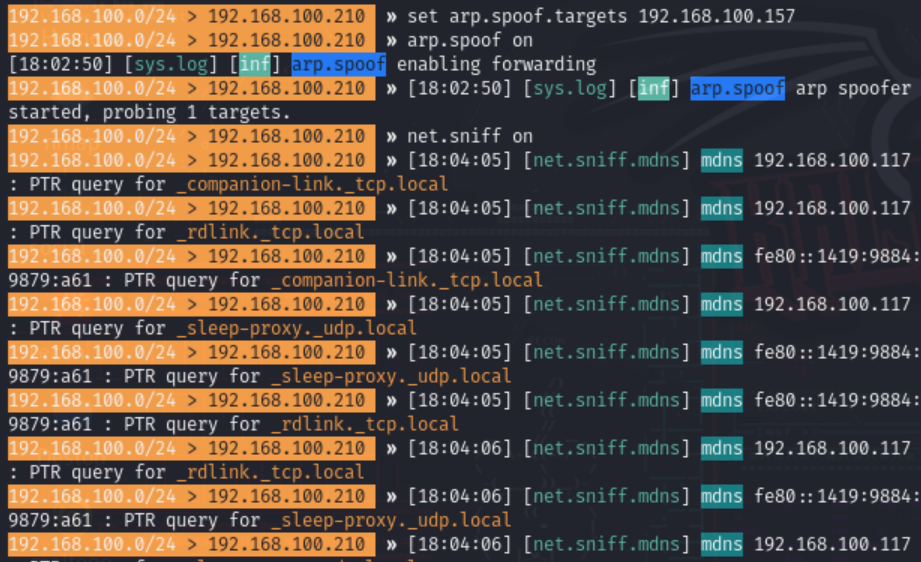
1. Lalu ketik **“ [18:20:50] [sys.log] [inf] arp.spoof arp spoofer”.**

* Pesan "[18:20:50] [sys.log] [inf] arp.spoof arp spoofer" pada Bettercap menunjukkan informasi log sistem. Secara spesifik, pesan ini memberitahukan bahwa modul ARP spoofing (arp.spoof) telah diaktifkan dan sedang berjalan sebagai "arp spoofer". Ini merupakan konfirmasi bahwa Bettercap berhasil memulai serangan ARP spoofing pada jaringan yang ditentukan. Pesan log ini memberikan pemantauan dan pembaruan terkait aktivitas ARP spoofing selama sesi Bettercap.



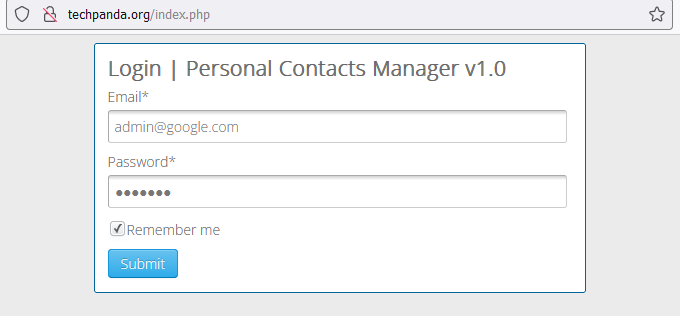
1. Ketik **“net.sniff on”.**

* Perintah **net.sniff on** pada Bettercap digunakan untuk mengaktifkan modul sniffing dalam jaringan. Setelah diaktifkan, Bettercap akan mulai memantau dan mencatat paket data yang melewati jaringan tersebut. Ini berguna untuk menganalisis lalu lintas jaringan, menangkap informasi sensitif, atau memahami komunikasi antar perangkat dalam suatu jaringan. Penting untuk dicatat bahwa penggunaan modul ini harus mematuhi regulasi dan etika, serta hanya digunakan dalam konteks keamanan yang sah dan diizinkan.

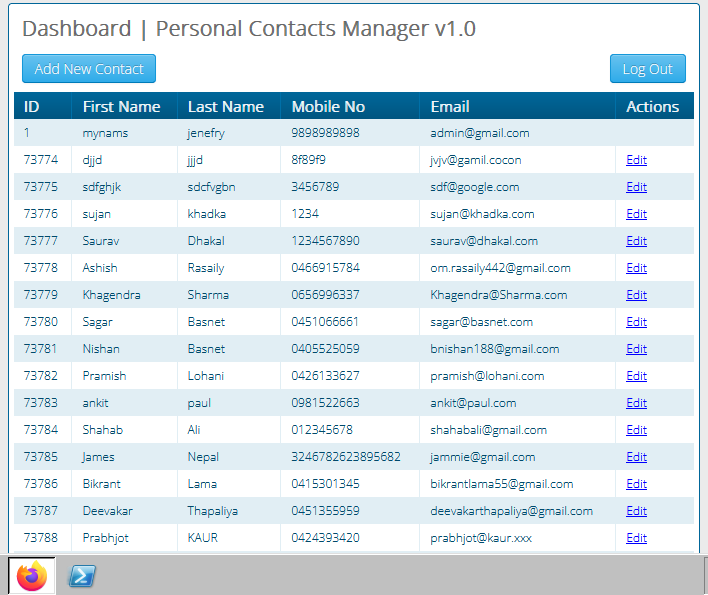


1. Lalu masuk ke **“techpanda.org/index.php”**

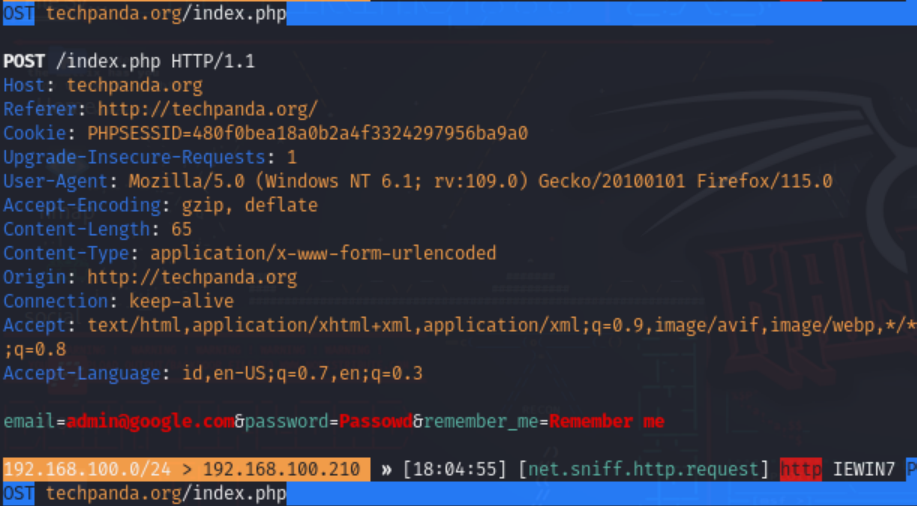
* email dan password yang sesuai dan tertera pada bettercap tadi lalu submit.



1. Lalu di dalam web ini tertera data yang sesuai dengan bettercap tadi dan memang tertera seperti di bawah.



1. Lalu hasil dari semua di atas akan keluar seperti di bawah ini.



**V. Analisa dan Kesimpulan**

Bettercap adalah alat uji penetrasi (penetration testing) dan keamanan jaringan yang berjalan pada sistem operasi Kali Linux. Berikut adalah kesimpulan singkat tentang Bettercap:

1. **Fungsi Utama:**
   * Bettercap dirancang untuk melakukan uji penetrasi dan analisis keamanan pada jaringan.
   * Menyediakan berbagai modul untuk melaksanakan serangan Man-in-the-Middle (MITM), pemindaian jaringan, dan sniffing paket.
2. **Fitur Utama:**
   * Modul ARP spoofing untuk serangan MITM.
   * Modul pemindaian jaringan untuk mengidentifikasi dan memantau perangkat dalam jaringan.
   * Modul sniffing untuk memantau dan menganalisis lalu lintas paket.
3. **Penggunaan Etis:**
   * Bettercap sebaiknya digunakan dengan izin dan hanya dalam konteks keamanan yang sah dan etis, seperti uji penetrasi atau aktivitas keamanan yang diizinkan.
4. **Sinkronisasi dengan Kali Linux:**
   * Dikembangkan khusus untuk digunakan pada sistem operasi Kali Linux, platform populer untuk keamanan jaringan dan uji penetrasi.
5. **Monitoring Real-time:**
   * Memberikan kemampuan untuk memantau dan mendeteksi perubahan dalam jaringan secara real-time.
6. **Pentingnya Pemahaman:**
   * Pemahaman mendalam tentang penggunaan Bettercap sangat penting untuk menghindari penyalahgunaan dan memastikan bahwa alat ini digunakan dengan benar.

Penting untuk diingat bahwa Bettercap, seperti alat keamanan lainnya, seharusnya hanya digunakan oleh profesional keamanan yang memahami implikasi etis dan hukum dari kegiatan yang mereka lakukan. Selain itu, penggunaan Bettercap pada jaringan tanpa izin dapat melanggar hukum dan etika.