UJI PENETRASI 1

1. Langkah Instalasi Ubuntu Server
   1. Pertama, silahkan install Virtualbox
   2. Setelah install virtualbox, jalankan virtualbox, dan buat virtualisasi baru dan pilih sesuai dengan yang anda inginkan. Untuk kali ini, ubuntu server dibuat dengan alokasi penggunaan ram 1.5 GB, dan allokasi harddisk yang tetap sebesar 10 GB
   3. Setelah pembuatan Virtual box baru berhasil, silahkan pilih bootable ubuntu seperti gambar dibawah
   4. Ikuti petunjuk instalasi seperti biasa, hingga ubuntu berhasil di install
2. Langkah Instalasi Xubuntu (OS untuk mempenetrasi)
   1. Pada virtualbox, buat virtualisasi baru tetapi dengan alokasi ram yang lebih besar yaitu 2 GB, dan alokasi harddisk yang juga lebih besar yaitu 20 GB
   2. Lalu silahkan pilih iso dari xubuntu
   3. Ikuti petunjuk instalasi hingga xubuntu berhasil diinstal
3. Langkah instalasi SSH server
   1. Pada xubuntu yang telah diinstal, silahkan buka terminal dan masukkan sudo apt-get install open-ssh server, dan tunggu hingga instalasi selesai
4. Langkah uji penetrasi menggunakan Medusa (Tools untuk SSH Brute Force Attack)
   1. Untuk langkah pengujian, pertama silahkan install dependensi yang mendukung medusa agar bisa di install.
   2. Setelah itu, silahkan mulai install medusa seperti gambar dibawah
   3. Setelah instalasi medusa selesai, buatlah sebuah txt yang bisa dibaca oleh medusa dengan format :username:password
   4. Setelah itu, masukkan syntax medusa –h [ip\_host] –C [nama\_file\_buatan].txt –M ssh
   5. Lihat hasilnya, ketikahasil bruteforce menunjukan success, maka itulah username dan passwordnya

UJI PENETRASI 2

1. Instalasi Fail2Ban

Pada ubuntu server silahkan install fail2ban sebagai countermeasure, dengan cara

sudo apt-get install fail2ban

1. Setting SSH
   1. Untuk setting SSH, saya memanipulasi di bagian penggantian port, dan melakukan "deny" pada user yang tergabung dengan sudoer

Mengubah port menjadi 8080

Membuat user tertentu untuk tidak bisa di akses dan sisanya bisa di akses

* 1. Lalu dicoba untuk menggunakan medusa

Bisa dilihat, karena port diubah, medusa tidak bisa membuka karena port tidak default

* 1. Lalu dicoba test untuk masuk menggunakan user "desktop"

Bisa dilihat, user tidak bisa login, dan muncul permission denied

* 1. Dan coba masuk menggunakan user "coba"

Bisa dilihat, user bisa login karena tidak masuk deny user

1. Setting Fail2Ban
   1. Untuk setting fail2ban, saya membuat setting "maxretry" menjadi 3, jadi ketika gagal login selama 3 kali, maka client yang mencoba masuk akan terkena ban sesuai dengan "bantime". Untuk "bantime" saya isi angka 600
   2. Lalu dicoba untuk menyerang menggunakan medusa

Terlihat bahwa penyerangan di ban karena sudah lebih dari 3 kali coba, dan akan abort

* 1. Lalu dicoba untuk melakukan SSH setelah melakukan hal tersebut

Bisa dilihat ketika itu juga, tidak bisa di SSH karena masih dalam masa Ban