

Penetrasi rollan.ak@gmail.com

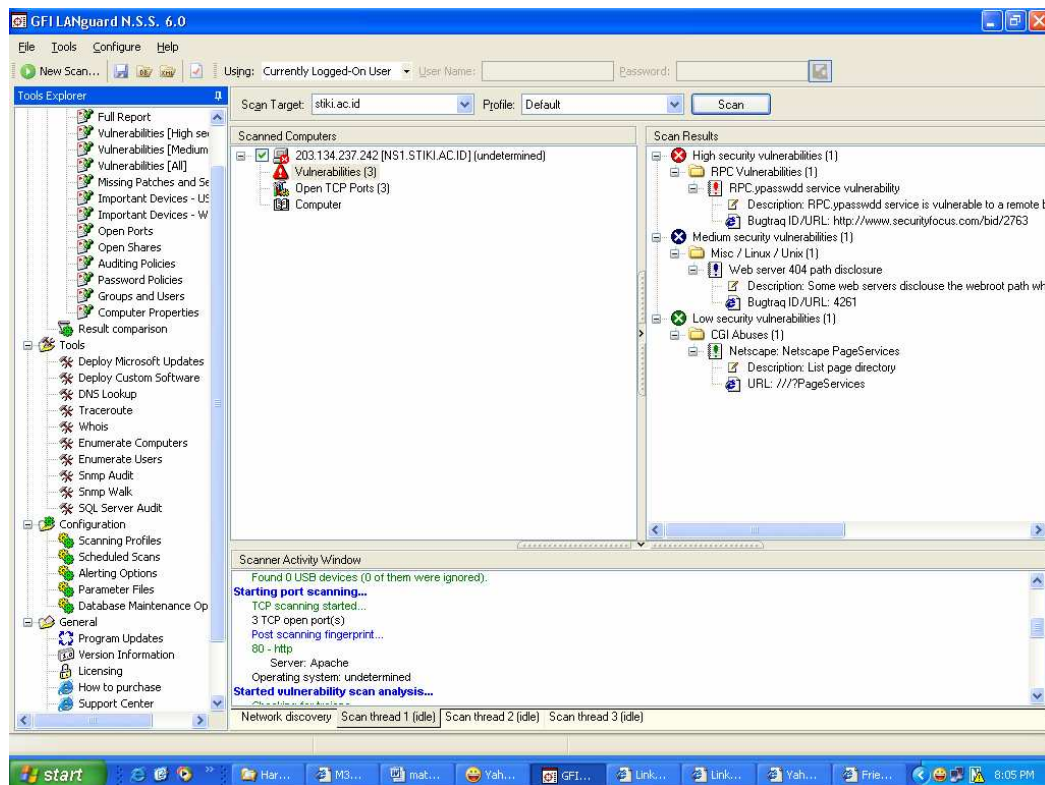
Dalam mempelajari hacking tingkat dasar adalah yang terpenting pertama adalah harus dapat menyamakan jejak dan kedua mengetahui metode penetrasi yaitu mengetahui celah lubang yang dibuka oleh host target. Entah itu dalam internet atau dalam jaringan lokal.

Disini yang dibahas melakukan penetrasi saja dilain kesempatan mungkin kita bahas metode yang lainnya. Dalam melakukan penetrasi adalah dasar basic hacking dimana dapat mengetahui celah dan vulnerabilities di host tersebut. Untuk memahami lebih lanjut tentang hal tersebut anda bisa memperdalam daftar port dan TCP/IP.

Dalam melakukan penetrasi dengan menggunakan GFI-Languard dimana bisa diupdate database vulnerabilities dan banyak fasilitas yang lainnya.GFI-Landguard bisa di download

<http://www.gfi.com/downloads/downloads.aspx?pid=lanss&lid=en>.

Mari kita coba melakukan penetrasi suatu host/server contoh target stiki.ac.id kita bisa mengetahui port/lubang apa saja yang bisa kita masuki dan vulnerability apa saja dihost tersebut.

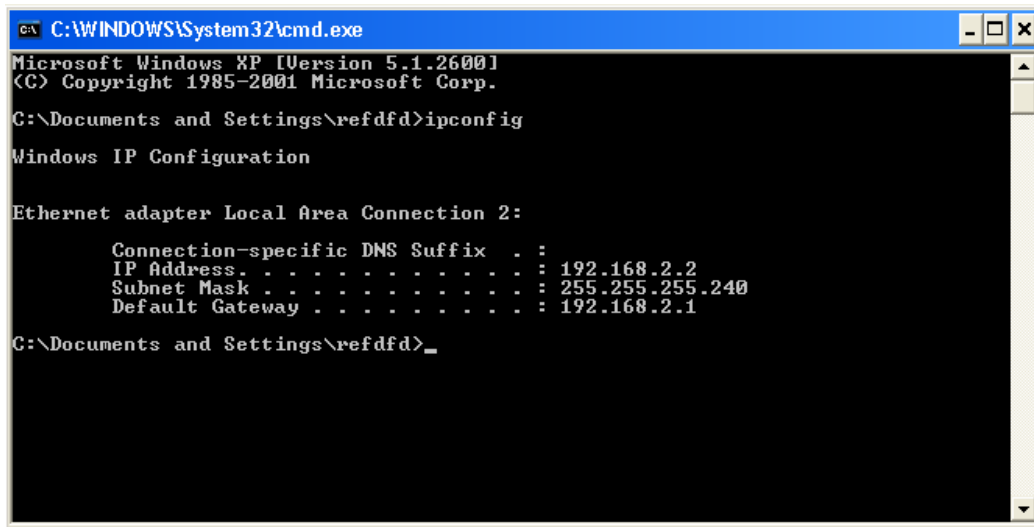


Gambar 1.Hasil Scanning Ke stiki.ac.id

Disitu terlihat IP public yang dipake adalah 203.134.237.242, vulnerabilities ada 3 dan port yang terbuka ada 3 yaitu 53 (dns) - 80 (web) - 443 (ssl) dimana ketiga port yang terbuka tersebut dapat kita tembus dengan metode exploit dan buffer overflow. Untuk Vulnerability ada 3 yaitu di RPC untuk High security.

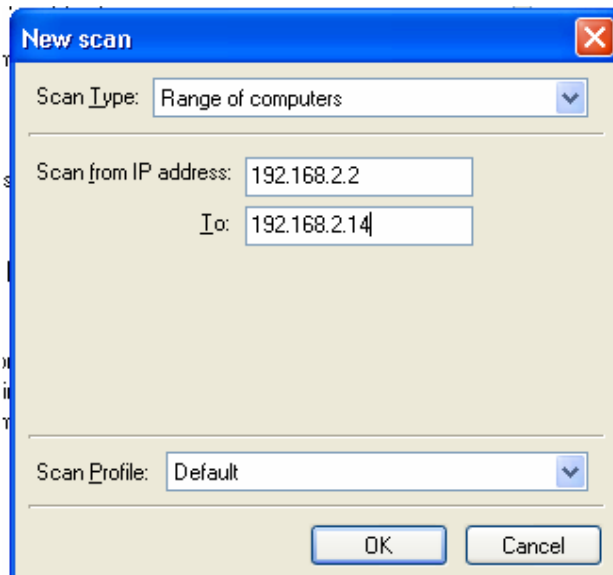
Untuk jaringan lokal mari kita coba lakukan penetrasi jangan lupa kita harus mengetahui IP address n subnet kita jadi kita bisa mengetahui range dalam satu sub

network.untuk mengetahui IP kita masuk start-→ run-→ketik cmd-→ketik ipconfig
lihat gambar 2. dibawah Ini



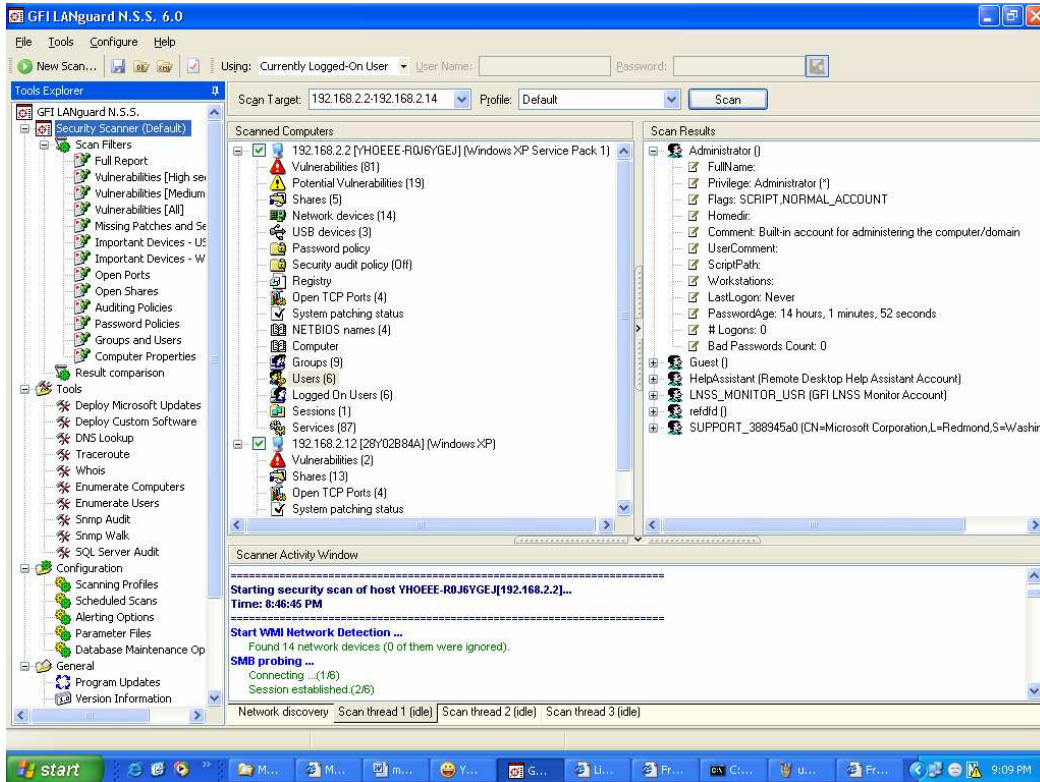
Gambar 2. Ipconfig

Kita mengetahui IP kita 192.168.2.2 mempunyai subnet 255.255.255.240 berarti dimana dalam satu sub network ada sebanyak 14 host.Kita bisa mengetahui IP berapa saja yang hidup dan apa saja yang kita bisa masuk kedalam host target. Terkadang GFI-Languard bisa memberikan hak akses langsung kedalam target dengan kita mengklik vulneribilitas host tersebut. Di GFI-Lan Guard kita ctrl-n scan type kita pilih range of computers.lihat gambar 3 untuk keterangan



Gambar 3. konfigurasi scanning

Disitu terlihat ada 2 host yang hidup sekarang bagaimana kita berkreasi dengan host yang hidup tersebut. Lihat gambar 4.



Gambar 4. Scanning untuk Jaringan local

Dengan informasi diatas kita bisa mengetahui vulneribilites, patching, port yang terbuka, nama host dan bisa memakai mac addressnya untuk membuat cloning dengan host tersebut. Ok selamat mencoba dan berkreasi.

-- Terima Kasih --