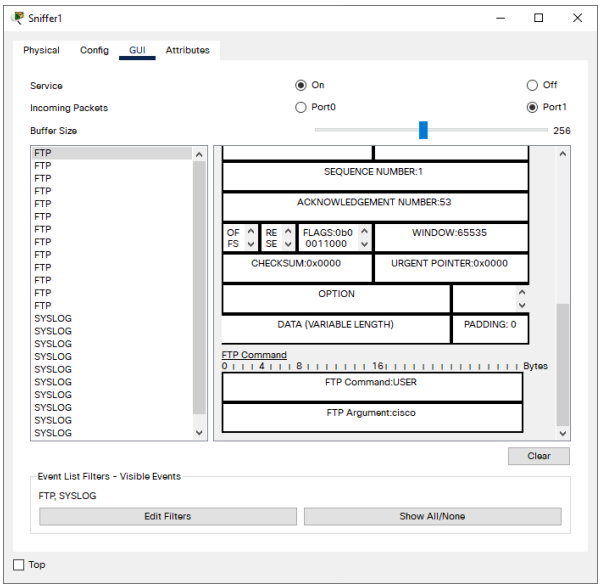
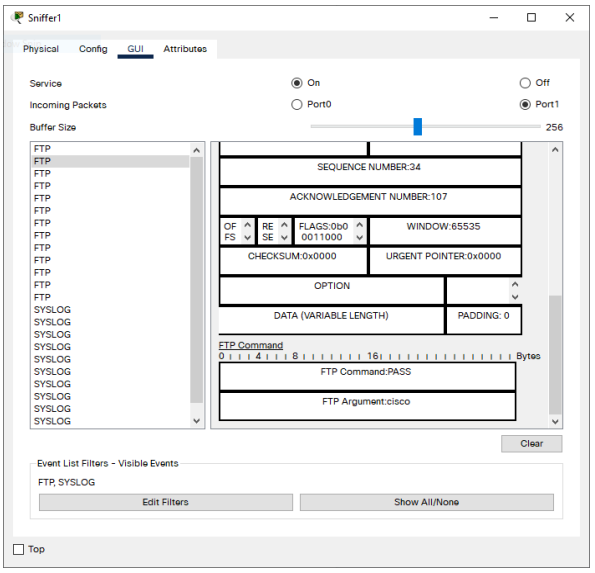
Muhammad Anbia Senggagau
Cyber Security Operational

Packet Tracer - Logging Network Activity

1. What is the security vulnerability presented by FTP?



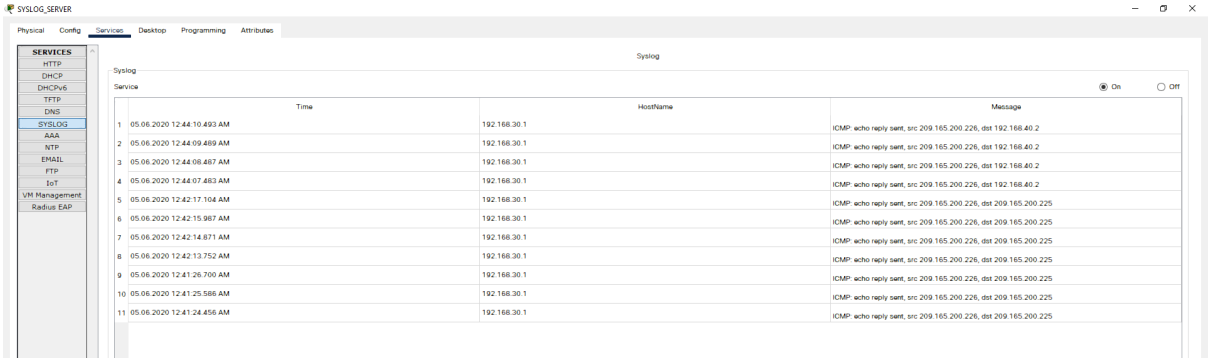


Dari gambar di atas, dapat dilihat bahwa pada sniffer mampu menangkap packet yang melalui sniffer itu sendiri sebelum sampai kepada tujuan, melalui sniffer kita dapat melihat id user dan password yang dimasukkan pengguna tanpa ada yang disembunyikan sedikit pun, sehingga ketika terjadi serangan man in the middle, para hacker mampu memperoleh info login ke server ftp

2. What should be done to mitigate this vulnerability?

Yang dapat dilakukan untuk menangani permasalahan ini adalah dengan menggunakan enkripsi untuk menyembunyikan informasi yang ada di dalam paket, sehingga meskipun hacker mampu menangkap paket tersebut, mereka tetap tidak tahu apa arti dari informasi yang didapatkan

3. There should be four messages from PC-A and four messages from PC-B. Can you tell which echo replies are for from PC-A and PC-B from destination addres? Explain



Dari gambar di atas, kita dapat melihat terdapat 12 echo reply untuk masing masing PC yang melakukan ping ke router 2. Penentuan yang mana echo reply untuk PC-A dan untuk PC-B tidak dapat dilakukan (jika kita tidak mengetahui info waktu dari suatu PC melakukan ping), karena PC-A dan PC-B berada pada jaringan yang berbeda, sehingga, destination IP Address yang ditujukan adalah IP Address untuk ke router 1, karena pada saat pengecekan, jaringan di router 2 mengkonfirmasi bahwa alamat IP yang dituju tidak ada pada jaringan tersebut, sehingga paket akan dikirimkan ke default gateway yaitu router 2. Dari router 2 akan dikirimkan ke router 1 melalui fitur routing di internet, setelah sampai di router 1, router 1 kemudian menentukan kepada siapa echo reply yang dituju di jaringan tersebut. Akan tetapi, pada saat PC-C melakukan ping ke router 2, IP Address Destination akan mengarahkan langsung ke alamat IP PC-C, karena PC-C berada pada jaringan yang sama dengan router 2.