Mata kuliah : SIJ014 - Keamanan Informasi (Praktikum)

Jumlah SKS : (1 SKS)

Waktu : 01-JULI-2022 10:00 - 12:00

1. Diketahui :
   Lihat url berikut : https://feodotracker.abuse.ch/browse/host/210.57.217.132/
   Dalam URL diatas merupakan web monitoring untuk satu jenis malware yang dikenal dengan nama “emotet” yang saat ini menjadi ancaman bagi perusahaan maupun orang pribadi yang menyebabkan terjadinya kehilangan data dan uang.
   Pertanyaan :
   a. Berdasarkan url diatas kapan pertama kali malware “emotet” menginfeksi korban? Dan melalui port berapa? (poin : 10)
   b. Sebutkan identitas perusahaan yang menjadi korban malware “emotet” ini! (poin : 10)
   c. Tipe file apakah yang terinfeksi oleh malware “emotet”? (poin : 10)
   d. Bagaimanakah cara memitigasi malware “emotet” ini ? (poin : 10)
   e. Bagaimana malware “emotet” menyebar? (poin : 10)
   f. Bagaimanakah cara mengetahui bahwa user/perusahaan anda terinveksi malware “emotet”? (poin : 10)
2. Diketahui :
   Lihat url berikut : http://www.foo.com/
   Pertanyaan :

a. Carilah informasi tentang domain diatas (foo.com), berdasarkan perusahaan pemilik, masa aktif domain, IP address, As Number (sertakan screenshoot) (poin : 10)
b. Carilah informasi tentang port yang terbuka, service yang berjalan pada port tersebut, berdasarkan domain diatas (foo.com) (sertakan screenshoot) (poin : 10)
c. Carilah informasi ssl pada domain diatas (foo.com), (sertakan screenshoot) (poin : 10)
d. Carilah informasi tentang dns dari domain diatas (foo.com), (sertakan screenshoot) (10)