Anàlisi de paquets de xarxa amb Wireshark

En aquesta pràctica analitzarem el fitxer atac.pcap que trobaràs al Moodle, es correspon a la captura de paquets durant un atac informàtic en xarxa. Els paquets foren capturats des del dispositiu atacat. Per aquesta tasca usarem el programari open-source Wireshark que disposa d'eines que ens permetran filtrar el tràfic de la xarxa segons la informació que cerquem en cada moment.

1. **Quina és l'adreça IP de l'atacant i de l'atacat? I les direccions MAC? A partir de les IPs obtingudes geolocalitza l'atacant i l'atacat.** Pots utilitzar el següent recurs online: https://www.geolocation.com/

2. **Quines sessions TCP hi ha obertes entre les dos IPs? Indica'n els ports usats i el nombre de paquets enviats.**

3. **Quant temps dura l'atac?**

4. **Quin és el sistema operatiu del sistema atacat?** Pots consultar la relació entre la versió i el nom comercial aquí: https://www.gaijin.at/en/infos/windows-version-numbers

5. **Aquest atac ha explotat una vulnerabilitat de l'Active Directory. Cerca paquets de protocol DSSETUP per obtenir-ne informació i aconsegueix el codi CVE de la vulnerabilitat i les seves característiques.** El CVE és una llista d'informació registrada sobre vulnerabilitats de seguretat conegudes.
   Quin protocol s'usà per explotar la vulnerabilitat esmentada?

6. **Quin port escoltava el servidor de l'atacant? Quin protocol s'usa en l'atac per descarregar un fitxer maliciós addicional al sistema atacat? Quin és aquest fitxer? En reconeixes el nom?** Analitza els fluxos TCP.