Chiar daca nu am incarcat nimic pe github aceste zile, nu am stat absolute nici o zi fara sa lucrez la proiect!

Am finalizat preluarea in masina virtual a tuturor informatiilor cerute, in timp real.

In timp ce masina virtuala functioneaza si se dau comenzi, am implementat o serie de scripturi care inregistreaza toata activitatea in fundal, insemnand comenzile date, fisierele modificate, tastele apasate si activitatea in retea. Pentru activitatea in retea se pot vizualiza anumite detalii exclusiv(cererile DNS,ip-urile, cache-ul ARP,traficul general)

Toate aceste informatii sunt trimise prin protocol TCP la o aplicatie cu rol de interfata pe care am creat-o in qt pentru a centraliza si accesa mai usor datele.

Login-ul in aplicatie se face printr-un username si o parola, iar conturi noi pot fi create doar de catre utilizatorii care sunt deja logati, astfel incat doar un administrator de retea poate adauga alt administrator.

Conturile sunt retinute intr-o baza de date retinuta in Microsoft SQL Server Management Studio, care este interogata de aplicatia qt la fiecare logare si in care se adauga conturile noi create.

Este disponibila in aplicatia qt vizualizarea istoricului logarilor in aplicatie si informatiilor vizualizate, istoric care este retinut tot in baza de date si este protejat prin necesitatea unei parole de “super admin”, astfel incat administratorii obisnuiti sa nu aiba acces la tot ce au facut ceilalti admini, ci doar supervizorii care cunosc parola.

Masina virtuala trimite in timp real informatiile la aplicatia qt, lucru implementat prin alte cateva scripturi care ruleaza continuu in fundal, astfel incat aplicatia si VM-ul pot fi pornite simultan, iar activitatea de pe VM poate fi vizualizata in aplicatia client.

Pentru stergerea periodica a logurilor, pentru a nu le incarca de foarte multa informatie, am scris niste cronjoburi care se executa in fiecare zi la ora 16, daca masina virtual este deschisa la acea ora.

Cateva screenshoturi din aplicatie:











