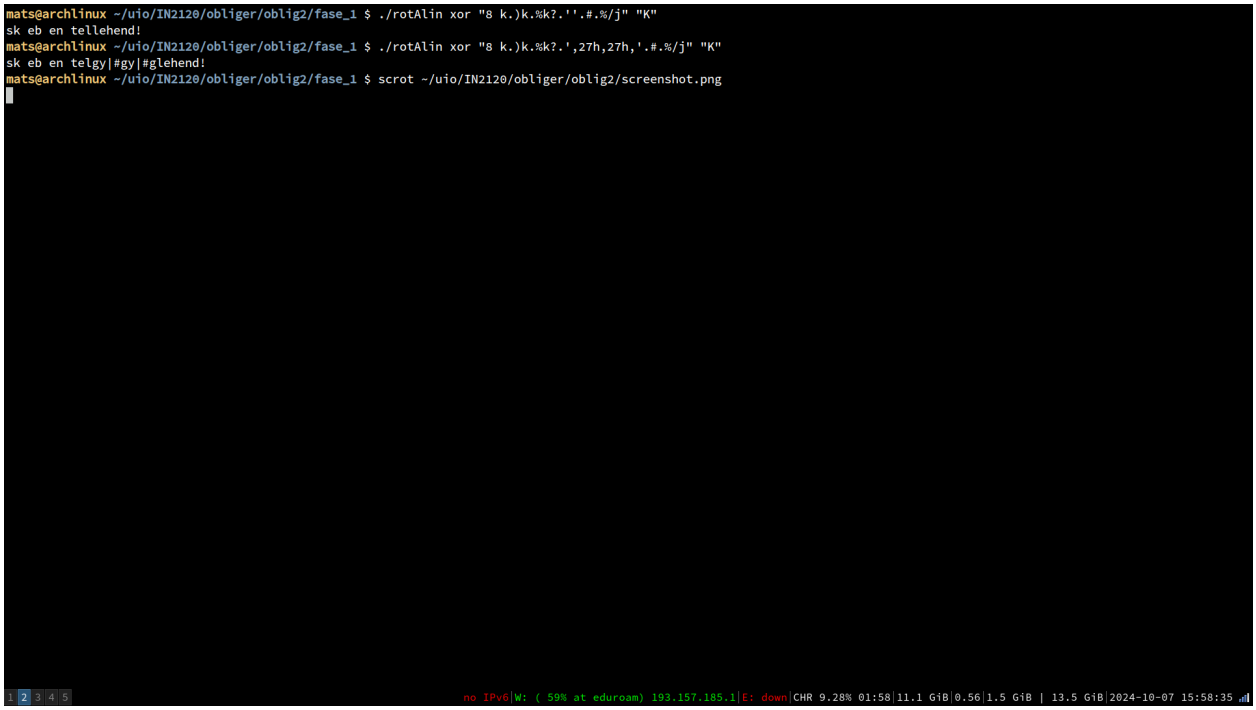
Oblig. 2 Mats Andersen (matande)

Fase 1)

1) Jeg ville ha opprettet studentforeningen “Milsec", som spesialiserer seg paa militaer informasjonssikkerhet. Saa ville jeg ha rekruttert noen medlemmer fra instituttet, og arrangert en helt ordinaert omvisning av fasilitetene paa huseby militaerleir. Moetet avsluttes paa kontoret til gardesjefen, hvor vi tar bilder, og laerer mer om leirens organisatoriske struktur og sikkerhetstiltak. Under denne seansen ville jeg ha rappet minnepinnen.

2) Programmet bryter seg gjennom brannmuren paa port 19, infiltrerer stormaskinen og gjemmer seg i CPU-en. Deretter “deployer” den “payloaden”. Programmet har paa et vis tre ulike funksjoner. Naar du bruker “exec”-flagget, “kjoeres” skadevirus. Naar du bruker “xor"-flagget, kan du kjoere XOR-kryptering. Uten noe flagg printes det bare “Hei verden!”.

3) Det dekrypterte innholdet i “tullehund” gir meg “sk eb en tellehend!”, saa antageligvis “Ask er en tullehund!”. Antageligvis er Ask en tullehund. Jeg fant dette ved aa dekryptere vha. XOR paa det krypterte innholdet i tullehund. Noekkelen var “K”. At jeg fant tullehund i .data forteller meg at det er en global variabel. Jeg mistenker at jeg ikke faar den fullstendige setningen, fordi noe informasjon ble tapt pga. Ida, eller kanskje pga. operativsystemet mitt. Det kan ogsaa vaere intendert, for aa forvirre. F.eks maatte jeg konvertere 27h til ascii.

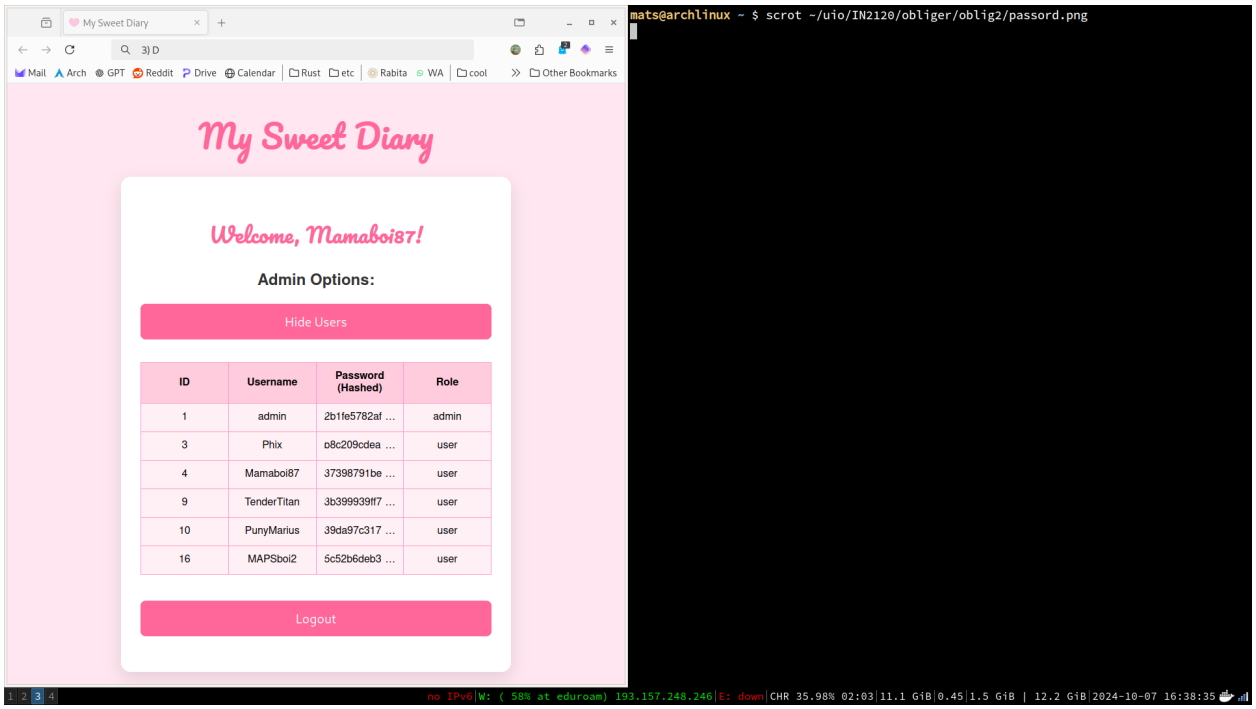


4) Mac, Linux og Windows er ulike operativsystemer med ulike filsystemer og kjernearkitekturer. Disse haandterer alle systemkall paa ulikt vis.

5) For aa oedelegge cyanpilled.no ville jeg leid en bot-arme paa *the dark web* og utsatt siden for et aldri saa lite DDoS-angrep.

Fase 2

1) Jeg skrev `'' OR 1==1 --'` for aa komme meg inn som admin. Dette er SQL injection. Det finnes flere maater aa beskytte seg mot SQL injection paa, men den enkleste er kanskje aa soerge for aa behandle all input som data, og ikke som kommandoer. Man gjoer dette vha. parametriserte spoerringer.



2) Det ikke-hashete passordet er “C00kie!”. Dette fant jeg paa hashes.com.

3) “Rules” lager variasjoner av potensielle passord, ved aa modifisere dem, f.eks. ved aa legge paa suffixer, endre stor og liten bokstav, osv.

4) Jeg valgte spyd-phishing med en emosjonell vri. Motstykket til spyd-phishing er masse-phishing, som ikke sikter seg inn paa noeyaktig en person. Det finnes en tredje type, som gaar under navnet hval-phishing. Dette er naar man gaar etter de store fiskene, som direktoerer og kjendiser.

Hei,

Jeg er et naertstaaende familiemedlem til Vilde-Mathilde. Det har skjedd en alvorlig hendelse.

Vilde-Mathilde har oppfoert seg veldig rart i det siste. Vi fikk hoere at hun gjorde det slutt med deg. Vi syntest det var merkelig og trist, for hun pleide aa snakke saa varmt om deg. Du la kanskje ogsaa merke til det den siste tiden at hun oppfoerte seg rart.

Naa har Vilde-Mathilde forsvunnet, og vi proever aa kontakte mennesker hun omgikk med, foer hun bare sporloest ikke kom hjem en dag. Dette kom som et sjokk paa oss alle, og vi frykter at hun kan ha blitt lurt med paa noe.

Vi hadde satt uendelig stor pris paa om du kunne gi oss noe informasjon om tiden foer det ble slutt mellom dere. Sa hun noe rart? Hang hun med nye mennesker? La du merke til noe spesielt?

Politiet har blitt kontaktet, men det er ingen fremgang i saken. Vi sitter fast i papirmoellen.

I den anledning har vi startet en innsamlingskampanje; familien skraper sammen midler for aa faa raad til en privat firma som kan hjelpe oss aa finne henne. Hvis du kunne ha stoettet oss med hva enn du har, saa hadde vi satt uendelig stor pris paa dette. Det haster med aa faa samlet inn midlene.

Du kan gaa inn paa innsamlingskampanjen her:

http://finn-vilde-mathilde.no

Vi jobber ennaa med aa sette opp siden, saa det kan vaere den ikke funker med en gang. Jeg tror du maa bare ignorere alle beskjedene som kommer opp. Kunne ikke du ha hjulpet oss aa sette opp en ny side senere? Vilde-Mathilde sa jo at du var saa flink paa saanne datagreier :)

Mvh

Mats Andersen

5) Dette angrepsscenarioet er IKKE lovlig. Dersom jeg hadde rappet til meg en minnepinne fra gardesjefen, saa ville det ha vaert tyveri. Aa bryte seg gjennom brannmurer og infiltrere systemer, er ikke lovlig. SQL injection er

ikke lovlig. hashes.com er en lovlig nettside, men jeg brukte den til mine “ulovlige” formaal; til aa faa tilgang paa privat data. Phishing-mailen er iallfall totalt ulovlig. Jeg kommer med grove, falske paastander og rykter, og linker til en infisert nettside.