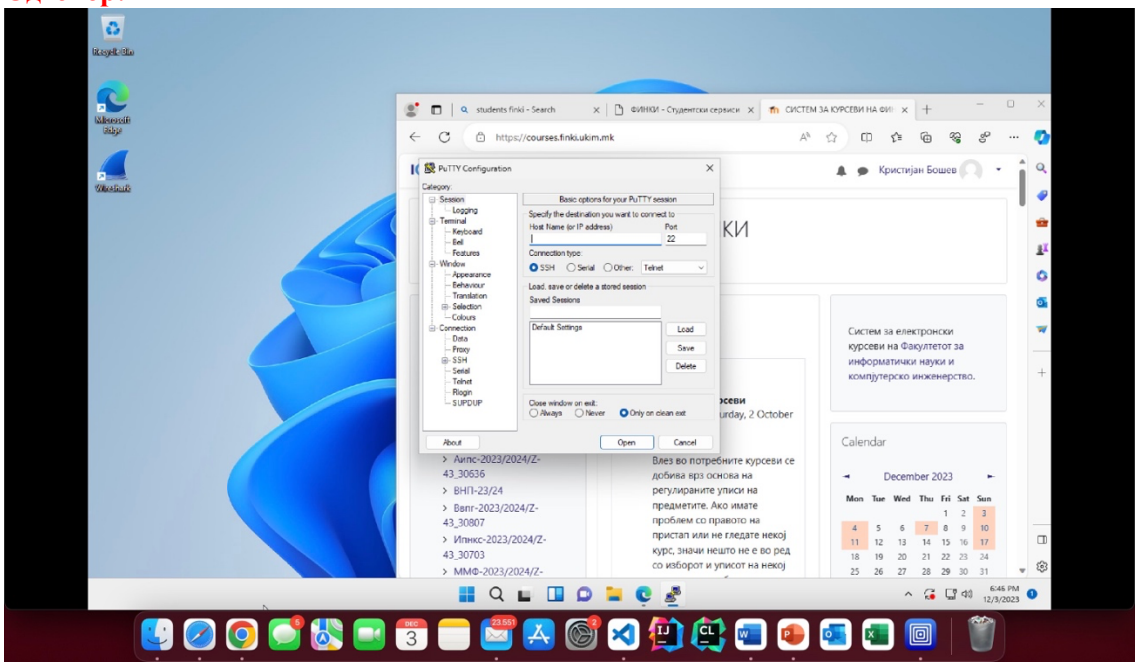
Лабораториска вежба 4 – Анализа и заштита на SSH сообраќај	*Име и презиме* *Кристијан Бошев*	*Индекс* *203159*

Забелешка: Одговорите на прашањата давајте ги со црвена боја.

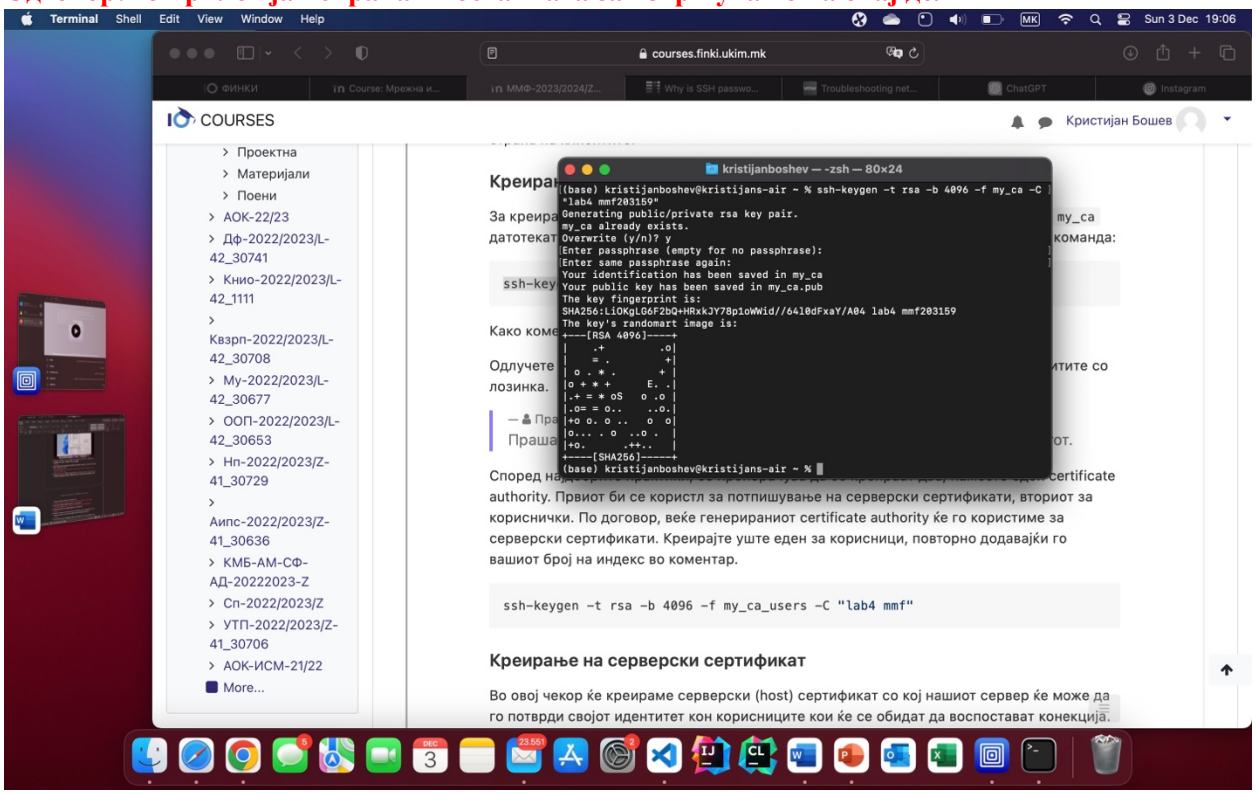
1. Дали најавата со корисничко име и лозинка беше успешно? Погледајте во `/var/log/auth.log` датотеката и направете слика од соодветните линии каде што е забележана вашата најава.
   Одговор: Најавата беше успешна, но сепак не беше креиран auth.log датотека
2. Кои се ризиците од најава исклучиво со корисничко име и лозинка на SSH сервери?
   Одговор: Доколку корисникот е најавен само со лозинка, можи да биди exploit преку brute force, исто така може да се заборави лозинката доколку е сложена и може да и се направи shoulder surfed
3. Внесете го вашиот изгенериран јавен клуч во елаборатот.
   Одговор: ssh-rsa 2048 SHA256:u1RrxpjV/ZXqqXSD6GMpgePWd3b5wc46OMBuWsVzU6Q
4. Прикачете слика каде што ќе се гледа новиот профил во Putty / Бидејќи ја искористивме основната патека за зачувување на приватниот клуч, openssh автоматски го користи овој новогенериран клуч. Истражете на интернет како може рачно да ја наведете патеката до приватниот клуч кој би сакале да се користи за најава.
   Одговор:



5. Обидете да се најавите на машината. Дали бевте прашани за лозинка за отклучување на приватниот SSH клуч? Поставете слика од тој prompt.
   Одговор:
6. Дали лозинката за отклучување на вашиот приватен клуч се испраќа до оддалечениот сервер? Која е нејзината функција?
   Одговор:Лозинката не се испраќа, таа се користи само за отклучување на клучот локално во компјутерот
7. Пробајте да се најавите **БЕЗ** клуч на SSH серверот (побарајте како да го реализирате ова со помош на openssh командата под UNIX или Putty под Microsoft Windows). Што се случи?

Успешно ли беше најавувањето? Поставете слика.
Одговор: Пристапот не е овозможен затоа што бара да се внесе клучот за најава

8. Која од трите опции ја одбравте за изработка на оваа задача?
Одговор:Ја избрав првата опција, да изработувам преку UNIX based machine
9. Внесете го јавниот дел од certificate authority-то во елаборатот.
Одговор:Во прилог ја испраќам постапката за извршување на овај дел



10. Обидете да се најавите кон серверот. Дали бевте прашани да го потврдите идентитетот на серверот, како што е случај при првата најава кога се користи лозинка? Зошто?
Одговор:Со користење на овај метод немаше никава потреба од потврда за идентитетот како кај најавата со лозинка затоа што приватниот клуч служи како еден вид на идентитет.
11. Со сопствени зборови споредете ја заштитата која ја нудат клучевите и сертификатите. Кој метод за најава е побезбеден? Зошто?
Одговор:Според мене зависи за каков случај станува збор, но сепак клучевите во поголем дел од случаите се по ефикасни затоа што нападите со brute-force немаат никакво влијание, клучеви не се споделваат како лозинките, и целиот процес и по автоматизиран.
12. Обидете сега да се најавите на SSH серверот. Дали бевте прашани за one time password? Поставете слика од prompt-от.
Одговор:
13. Пробајте да се најавите на SSH серверот. Дали успеавте? Зошто?
Одговор:
14. Отворете го `/var/log/syslog` и погледнете ги последните неколку линии. Што забележувате? Поставете слика.
Одговор:

15. По извршување на port knocking секвенцата, обидете се да се поврзете на SSH серверот. Дали успеавте?
    Одговор:Да, успеав да се најавам на серверот
16. Извршете ја секвенцата за затворање на портата и поставете screenshot од последните неколку линии на `/var/log/syslog`.
    Одговор: outputot e Dec 3 12:34:56 my-server nmap: Nmap scan report for 192.168.1.100
    Dec 3 12:34:56 my-server nmap: Host is up (0.0012s latency).
    Dec 3 12:34:56 my-server nmap: 22/tcp closed
    Dec 3 12:34:56 my-server nmap: 80/tcp closed
    Dec 3 12:34:56 my-server nmap: 443/tcp closed
17. Дали успеавте да откриете нешифриран сообраќај кон порта 22? Каква информација е разменета?
    Одговор:Не успеав да најдам никаков нешифриран сообраќај, само некои размени на клучеви
18. Дали од разгледување на фатените пакети можете да заклучите дека е користен приватен клуч за автентикација наместо лозинка?
    Одговор:Да,Може да се примети преку испраќање на пакети од клент до сервер и обратно во кои има некаков јавен клѕч
19. Дали од разгледување на фатените пакети можете да заклучите дека е користен SSH сертификат за автентикација?
    Одговор:
20. Дали од разгледување на фатените пакети можете да заклучите дека е користен дополнителен TOTP при најавата?
    Одговор:
21. Обидете се да ги најдете пакетите кои го отсликуваат вашето обидување да ја извршите port knocking секвенцата. Која е нивната содржина?
    Одговор:
22. Дали мислите дека напаѓач кој има можност да го следи сообраќајот би можел да ја открие port knocking секвенцата? Образложете го вашиот одговор.
    Одговор:Постои ризик доколку напаѓачот го знај сообраќајот, да може да ја открие секвенцата.