Co-funded by the
Erasmus+ Programme
of the European Union

Module de instruire InCyT

Securitatea informațiilor pentru angajați **Unitatea 3 Săptămâna 5** **Numele unității: Securitate la călătoriile de afaceri**	
Activități de învățare	❑ **Webinar** ❑ **Exerciții** ❑ **Workshop** ❑ **Prezentare** ❑ **Alte**
Responsabil de învățare	• Mirosław Mazurek • Paweł Dymora
Obiectivele activității de învățare	1. Rețele wireless 2. VPN 3. Criptare e-mail
Abilități de dobândit	• **TS3** • **SS2**
Durata activității de învățare	2 săptămâni
Cerințe de învățare	***Ce e necesar?***
	• Acces la internet • Motor de cautare • MS Office365

Co-funded by the
Erasmus+ Programme
of the European Union

Informații scurte despre modul

Descriere
Structura generală a acestui modul este de a oferi câteva aspecte teoretice și practice legate de securitatea cunoștințelor și abilităților practice la călătoriile de afaceri. Veți avea posibilitatea de a vă proteja rețeaua wireless și de a utiliza rețele wireless protejate cu ideea de VPN. Modulul va acoperi, de asemenea, cum să trimiteți e-mailuri în siguranță folosind protocolul PGP gratuit pentru mesaje criptate pe care nimeni nu le poate descifra fără permisiunea dvs..

Conținutul materialului de învățare

1. Introducere în rețelele fără fir. Baze teoretice: principiu de funcționare, protocoale de criptare.

Protocoalele WEP și WPA anterioare au fost folosite pentru a securiza rețelele fără fir, dar nu erau rezistente la atacurile hackerilor. Introducerea protocolului WPA2 a permis asigurarea unui nivel suficient de securitate, dar oricum nu oferă securitate deplină. Există multe topologii de rețea, protocoale de acces fără fir și tehnici de achiziție de acces la rețea disponibile, iar arhitecturile de calcul CPU (Unitate centrală de procesare) și GPU (Unitate de procesare grafică) sunt utilizate în achiziția cheii de rețea [1,2].

WEP (Wired Equivalent Privacy) este unul dintre cele mai vechi standarde de criptare wireless IEEE 802.11. Oferă protecție a informațiilor pe baza utilizării algoritmului RC4. Are multe vulnerabilități de securitate cunoscute și, prin urmare, a fost spart de mai multe ori. Este unul dintre cele mai vechi standarde pentru securizarea rețelelor WLAN (stabilit în 1997). Nu necesită putere mare de calcul a dispozitivelor instalate. Utilizează două metode de autentificare a utilizatorului: Autentificare deschisă și Autentificare cu cheie partajată. În plus, permite verificarea utilizatorului pe baza adreselor MAC fizice folosind ACL (Access Control List). Există o variantă WEP pe 64 de biți (bazată pe o cheie de 40 de biți și un vector de inițializare pe 24 de biți) și o variantă WEP pe 128 de biți (bazată pe o cheie de 104 biți). Unii producători au introdus și un standard WEP pe 256 de biți [1,2].

WPA (Wi-Fi Protected Access) este un alt standard pentru criptarea rețelelor wireless IEEE

802.11. A fost introdus pentru a îmbunătăți nivelul de securitate al rețelelor WLAN, înlocuind vulnerabilitățile cunoscute în standardul WEP. Se bazează pe utilizarea protocoalelor: TKIP (Temporal Key Integrity Protocol) și EAP (Extensible Authentication Protocol), standard 802.1x și mecanismul MIC (Message Integrity Check). Standardul se bazează pe algoritmul RC4. A fost implementat ca o soluție intermediară între standardul WEP și cel mai sigur standard de criptare fără fir actual 802.11i. Oferă lucru în două moduri, care includ: Enterprise (folosind un server RADIUS care gestionează alocarea cheilor către utilizatori) și Personal (folosind o cheie PSK partajată) [1,2].

WPA2 (Wi-Fi Protected Access 2) este în prezent cel mai puternic standard de criptare pentru rețelele fără fir (cunoscut și ca 802.11i). Oferă protecție a informațiilor pe baza utilizării AES (Advanced Encryption Standard). A fost introdus pentru a îmbunătăți nivelul de securitate al rețelelor WLAN, înlocuind vulnerabilitățile cunoscute în standardul WEP și standardul interimar WPA. Implementează protocolul 802.1x îmbunătățind controlul accesului utilizatorilor la rețea. Oferă lucru în două moduri, care includ: Enterprise (folosind un server RADIUS care gestionează alocarea cheilor către utilizatori) și Personal (folosind o cheie PSK partajată) - adesea folosit în soluțiile pentru acasă astăzi [1,2].

Algoritmul WEP este cel mai puțin sigur standard de criptare pentru rețelele wireless IEEE 802.11. A fost spart de multe ori prin diferite metode din cauza numeroaselor vulnerabilități cunoscute în prezent în aspectele de securitate ale algoritmului. Principalele dezavantaje ale standardului includ[3]:

- Lipsa unui sistem definit de gestionare a cheilor (adesea o cheie de rețea este utilizată de toate nodurile unei rețele fără fir);
- Dimensiunea de biți insuficientă a cheii de rețea (prima versiune a standardului WEP introduce chei de 40 de biți);
- Dimensiunea de biți insuficientă a vectorului de inițializare IV (standardul WEP introduce un vector de inițializare pe 24 de biți, care se dovedește a fi insuficient și, din cauza probabilității relativ mari de coliziuni cu un număr mic de pachete recepționate, există posibilitatea ca un atac criptografic pentru a obține valoarea cheii WEP);
- Sumă de control ICV slabă bazată pe funcția liniară CRC-32 (există o posibilitate de modificare inobservabilă a informațiilor transmise în rețea);
- Algoritm slab de criptare a informațiilor RC4 (există prea multe dependențe între cheia de rețea și rezultatul criptării informațiilor);
- Sistem insuficient de autentificare a utilizatorului (există posibilitatea de falsificare a mesajelor de autentificare).
- Pe baza punctelor slabe prezentate ale algoritmului WEP, au fost create multe instrumente pentru a conduce atacuri care testează nivelul de securitate al rețelelor WLAN. Cele mai populare atacuri împotriva WEP includ:
- Atacul FMS - un atac statistic (dezvoltat de Fluhrer, Mantin și Shamir) asupra algoritmului RC4 utilizat în standardul de criptare WEP;

- Atacul KoreK - un atac statistic (dezvoltat de o persoană supranumită KoreK) care utilizează mai multe (comparativ cu atacul FMS) dependențe ale procesului de criptare a algoritmului RC4;
- Atacul Chopchop - un atac interactiv, efectuat în direcția obținerii accesului la rețea prin decriptarea treptată a unuia dintre pachetele primite;
- Atacul PTW - este un atac statistic (dezvoltat de Pyshkin, Tews și Weinmann) asupra algoritmului RC4, care, datorită dependențelor succesive ale procesului de criptare a datelor, crește semnificativ probabilitatea de a obține valoarea cheii cu un număr relativ mic de pachetele primite.

Un alt tip de atac folosit frecvent este atacul Dicționarului. Este una dintre metodele brute de a dobândi de ex. valorile cheilor criptografice în rețelele de calculatoare fără fir. Pentru a obține valorile cheii WPA/WPA2, metoda se bazează pe criptarea unidirecțională și pe compararea intrărilor din dicționar cu informațiile din secvența de strângere de mână în 4 direcții capturată. Atacurile de dicționar sunt efectuate cu intenția de a reduce timpul de obținere a valorilor cheie în comparație cu metoda brute-force. Procesul de recuperare a valorii cheii continuă până când se obține un rezultat pozitiv (adică atunci când intrarea în dicționar se dovedește a fi o valoare cheie validă) sau până când toate intrările din dicționar sunt comparate cu rezultatul negativ. Un rezultat negativ poate indica un nivel ridicat de complexitate al valorii cheii și necesitatea utilizării metodei brute-force[3].

Succesul acestui atac este alegerea unui dicționar adecvat. Dicționarul este un fișier text utilizat în cazul atacurilor de dicționar pentru a obține, de exemplu, valorile cheilor criptografice. Conține o listă de articole pregătite corespunzător care pot constitui valoarea cheie căutată. Utilizarea dicționarelor în cazul atacurilor forțate permite reducerea semnificativă a setului de valori examinate, ceea ce poate duce la accelerarea procesului de achiziție a valorii cheii criptografice. Conținutul dicționarelor este construit, de exemplu, pe baza articolelor prezentate[3]:

- o listă de cuvinte care apar în dicționare naționale și străine;
- combinații de cuvinte cu litere mari și mici, cuvinte scrise invers (adică palindrom);
- combinații de intrări din dicționar cu vocale sau consoane decupate;
- combinatii de repetari multiple ale numelor selectate, numelor de familie, intrărilor din dicționar;
- combinaţii de cuvinte cu valori numerice, caractere speciale etc.;
- o listă de parole și autentificări utilizate cel mai frecvent de utilizatori;
- o listă de companii populare, organizații, termeni tehnici, nume proprii etc.;
- scurgeri de informații (adică autentificări, porecle, parole) de la diverse portaluri de internet;
- combinații de caractere adiacente de la tastatură pentru modelele selectate (Fig. 1).

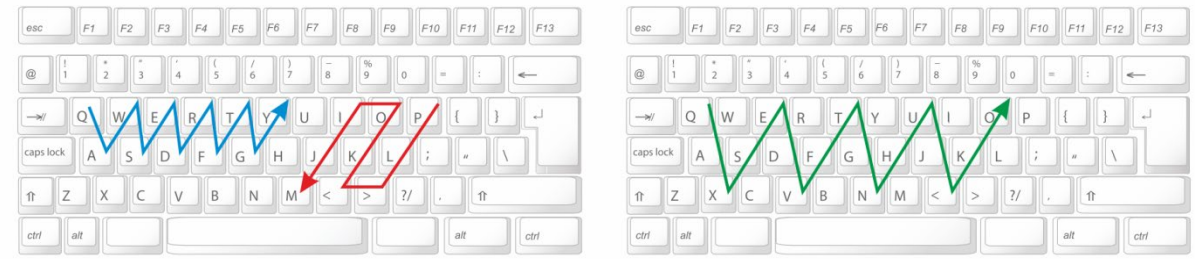

Fig. 1. Schemă care prezintă exemple de modele de creare a cheilor de rețea

Cheia de rețea joacă un rol cheie în studiul rezilienței rețelei. Este o secvență de caractere folosită de utilizatorii rețelei în procesul de autentificare. Procesul de autentificare este un pas important în protejarea accesului la serviciile partajate și la resursele rețelei de utilizatorii neautorizați. Cheile de rețea sunt adesea create și gestionate de administratorii de rețea și pot constitui cea mai slabă verigă în securitatea unei rețele de calculatoare. Valorile cheie care se dovedesc a fi relativ consumatoare de timp sau imposibil de spart folosind metode de forță brută în timp realist ar trebui generate, de exemplu, pe baza regulilor prezentate[3]:

- Fiecare rețea fără fir gestionată de administrator ar trebui să fie securizată folosind o cheie de rețea diferită;
- Fiecare utilizator de rețea ar trebui să utilizeze o cheie de rețea individuală;
- Cheile de rețea ar trebui să fie construite pe un număr suficient de caractere;
- Generarea cheilor trebuie să se bazeze pe spațiul maxim disponibil pentru caractere;
- Cheile nu trebuie generate folosind informații corporative și personale;
- Generarea cheilor nu ar trebui să se bazeze pe o listă de articole din dicționarele disponibile publicului;
- Cheile de rețea ar trebui să fie construite pe baza unor secvențe aleatorii de caractere;
- Cheile de rețea ar trebui actualizate periodic;
- Valorile cheie utilizate în prezent nu trebuie asociate cu valorile cheie care nu mai sunt utilizate.

2. Tuneluri VPN virtuale. Baze teoretice: tipuri, arhitectură, principiu de funcționare, protocoale de criptare. Instalarea programului Open VPN (configurare, adresare, selectare parametri, generare cheie).

O rețea privată virtuală este un tunel prin care traficul rețelei private circulă între expeditor și destinatar printr-o rețea publică. VPN înseamnă „Virtual Private Network”. O rețea VPN criptează toate activitățile de pe internet, ascunde adresa IP, protejând identitatea utilizatorului rețelei. O conexiune VPN oferă acces securizat la aplicații, site-uri web și platforme de divertisment de oriunde în lume. Este posibilă opțional comprimarea sau criptarea datelor transmise pentru a oferi o calitate mai bună sau un nivel mai ridicat de securitate, protejând astfel confidențialitatea în

rețea [4].

Un tunel securizat este creat prin autentificarea mai întâi a clientului cu serverul VPN. Serverul aplică apoi un protocol de criptare tuturor datelor care sunt trimise și primite. Pentru a asigura securitatea fiecărui pachet de date, VPN-ul îl plasează într-un pachet extern, care este apoi criptat prin încapsulare. Acesta asigură securitatea datelor în timpul transmisiei și este o componentă fundamentală a tunelului VPN. După ce datele ajung pe server, pachetele externe sunt eliminate în procesul de decriptare [4].

VPN-urile pot fi împărțite în două categorii principale [5]:

- Un VPN de acces la distanță care permite utilizatorilor să se conecteze la o rețea de la distanță, de obicei prin intermediul unui software special.
- VPN-uri site-to-site utilizate de companii, în special de marile corporații. Acestea permit utilizatorilor din locații selectate să acceseze în siguranță rețelele altor utilizatori.

Un exemplu de software de dezvoltare VPN dedicat este RadminVPN. În majoritatea cazurilor, nu este necesar să aveți o adresă IP statică în rețeaua locală pentru a configura un tunel VPN. După descărcarea software-ului corespunzător, acesta va crea o rețea adecvată cu o adresă statică a computerului dvs. [6].

Radmin VPN vă permite să vă conectați la două computere din două rețele diferite. Un exemplu de configurare este prezentat mai jos. Pentru o înțelegere mai ușoară a funcționării canalului VPN, Fig. 2 și 3 prezintă configurația inițială a computerelor între care urmează să fie creat un canal securizat..

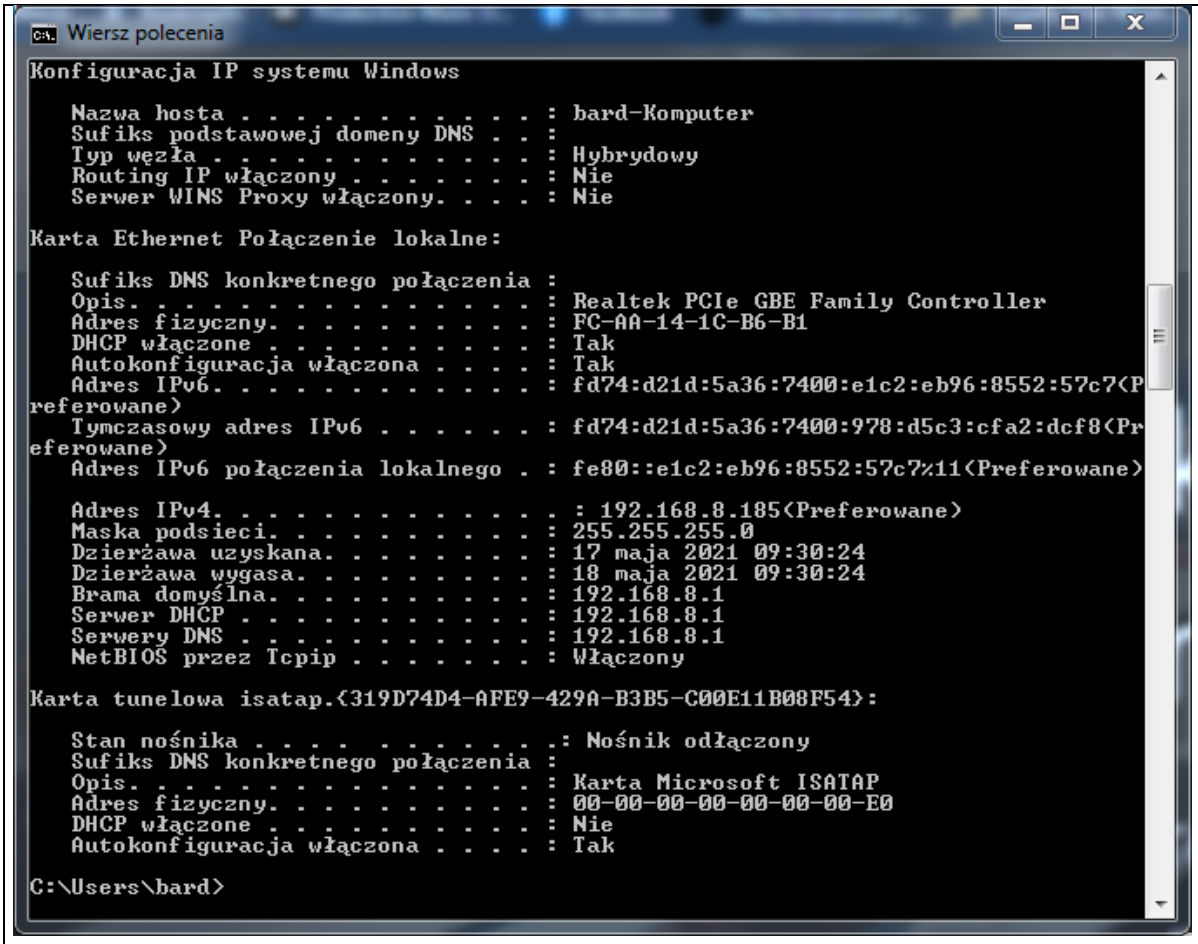

Fig. 2. Configurarea inițială a calculatoarelor

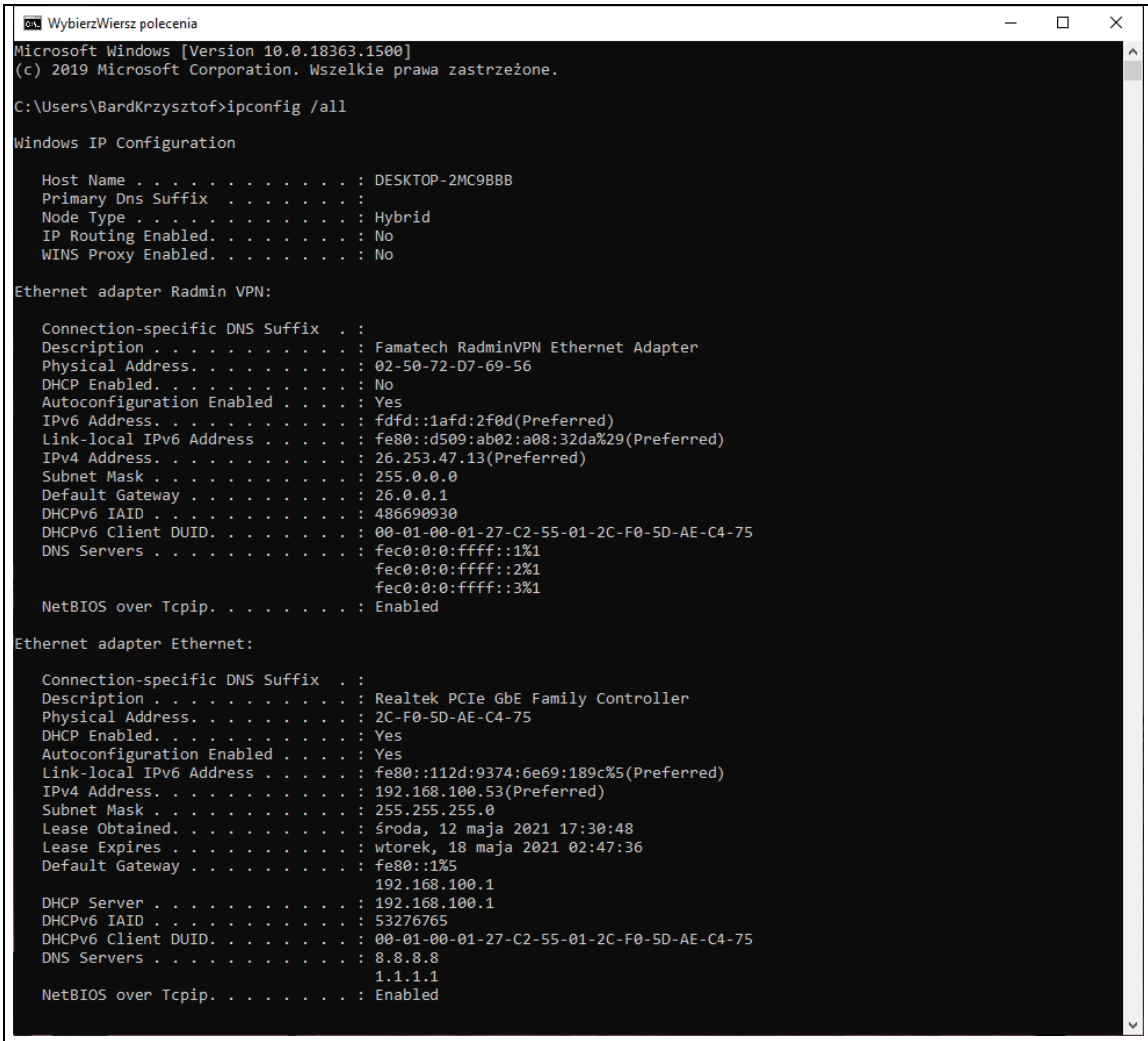

Fig. 3. Configurarea inițială a calculatoarelor

După cum puteți vedea, adresele de gateway sunt complet diferite, astfel încât computerele nu au o conexiune fizică sau logică între ele. Pentru a crea un canal, instalați RadminVPN pe ambele computere. Pe unul dintre ele trebuie să începeți prin a vă crea propria rețea.

Fig. 4. Vedere a ecranului principal al aplicației (imagine din stânga - configurația computerului 1, imaginea din dreapta - computerul 2).

Pentru a crea o rețea, selectați Creare rețea în fereastra aplicației, furnizați un nume și o parolă pentru rețea și confirmați cu butonul Creare. Pe al doilea computer, rețeaua creată în acest fel trebuie adăugată făcând clic pe butonul Alăturați-vă rețelei, introducând numele și parola rețelei tocmai create.

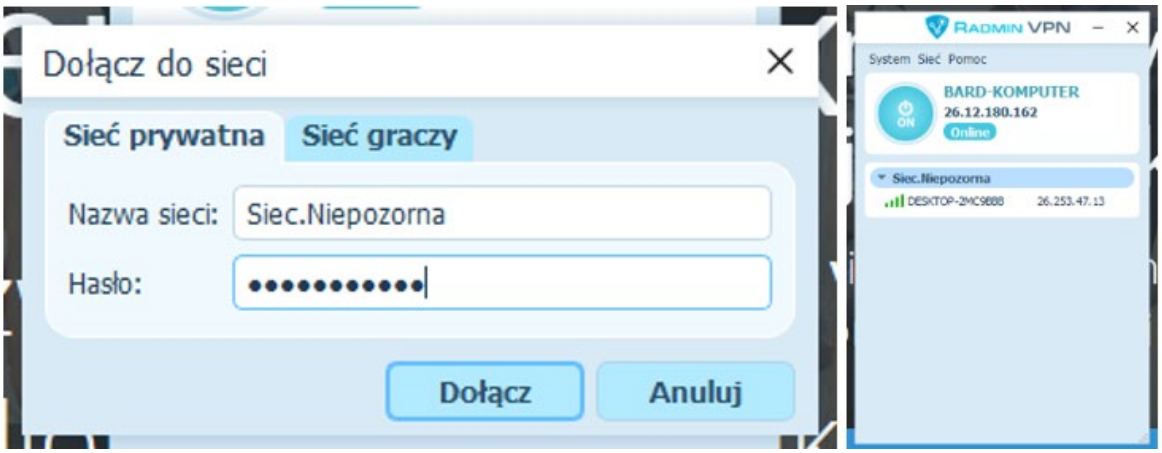

Fig. 5. a) Vedere a ferestrei de conectare la rețea; b) starea conexiunii.

După conectarea cu succes la rețea, ambele computere ar trebui să fie într-o vizualizare a conexiunii la rețea (așa cum se arată în Figura 5b). În acest caz, puteți vedea numele și adresa

computerului de cealaltă parte a tunelului. Va fi la fel și pe al doilea computer. Încercarea de conectare în această etapă va eșua deoarece Radmin Server este necesar pentru funcționarea sistemului. Informațiile despre instalare vor apărea în aplicație și trebuie făcută pe ambele computere și repornită. După finalizarea întregului proces de instalare, computerele vor putea comunica, dar nu va fi posibil ca unul să preia controlul asupra celuilalt. Pentru a vă putea controla reciproc, trebuie să configurați desktopul de la distanță al sistemului în Windows (Panou de control->Sistem și în partea dreaptă alegeți Setări avansate de sistem).

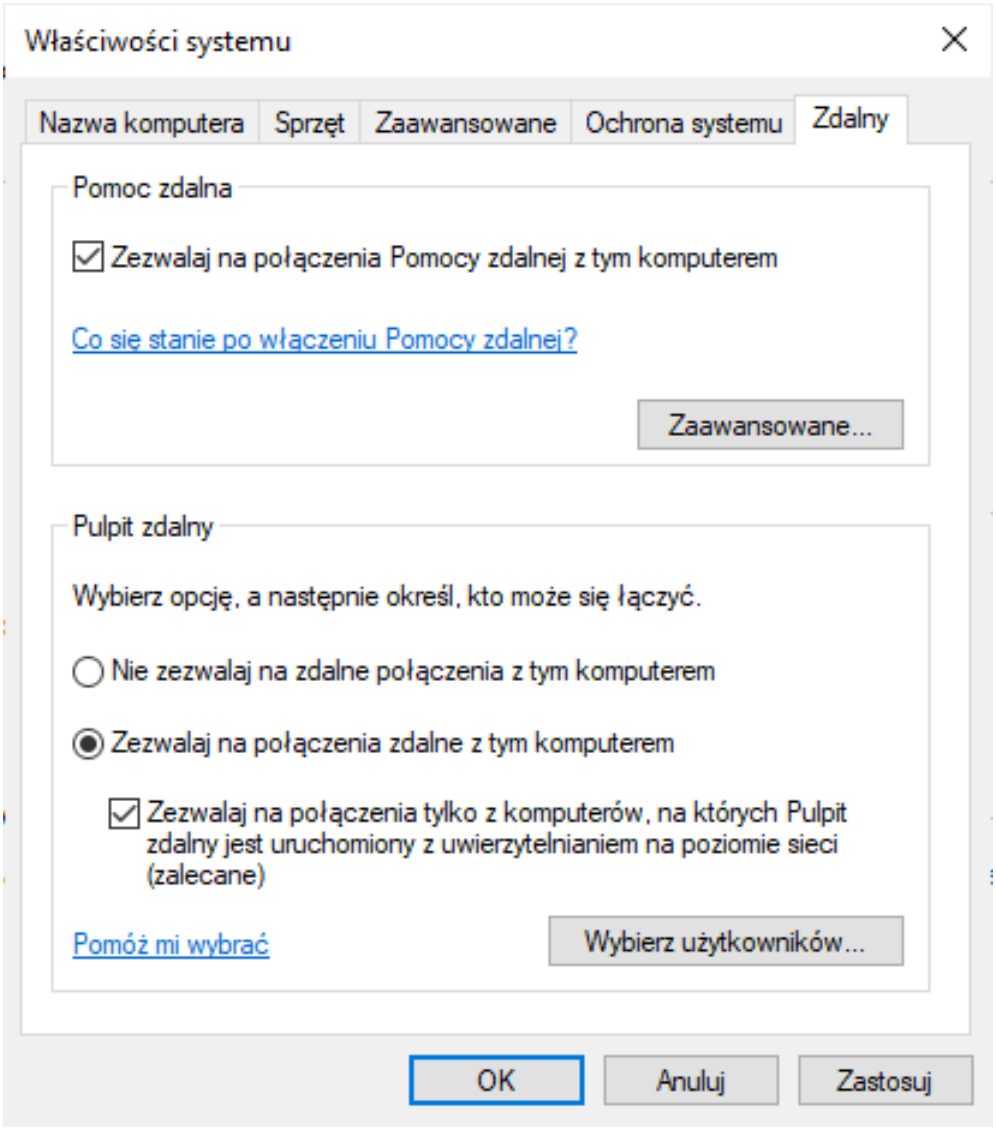

Fig. 6. Setările secțiunii Remote Desktop

Apare fereastra System Properties. Apoi selectați fila La distanță și secțiunea Desktop la distanță selectând Permite conexiuni la distanță la acest computer (Fig. 6). După aprobarea modificărilor pe ambele computere, creați un utilizator cu drepturi de acces date. Pentru a face acest lucru, rulați

RadminServer și din câmpurile din dreapta alegeți Permisiuni și apoi opțiunea Permisiuni. În fereastra de permisiuni, bifați Acces complet și creați un utilizator (trebuie să îi oferiți un nume și o parolă). Aceasta completează procesul de configurare a canalului VPN. Tunelul creat este bidirecțional și poate fi utilizat cu ușurință pentru a controla computerele din ambele părți.

3. Criptare e-mail. Baza teoretică: tipuri de criptare (simetrică și asimetrică), securitate, protocoale, chei. Instalarea și configurarea OpenPGP. Instalarea și configurarea unui client de e-mail.

Unul dintre cele mai utilizate canale de comunicare este poșta electronică (e-mail), care devine din ce în ce mai mult o țintă a atacurilor de tip hacking. Protejarea acestui element este o parte importantă a pachetului de soluții de securitate cibernetică. Protejarea e-mailului și criptarea atașamentelor sunt două probleme de securitate online foarte importante. Criptarea e-mailului nu numai că minimizează riscul scurgerii de date confidențiale, dar previne interceptarea neautorizată. E-mailul și atașamentele sale nu sunt securizate în mod implicit cu protocoalele SSL și TLS, iar toate mesajele sunt trimise ca text simplu [8].

Algoritmii de criptare, cum ar fi criptografia, se împart în două categorii:

- algoritmi simetrici de criptare;
- algoritmi de criptare asimetrică;

Principala diferență dintre cele două metode de criptare este numărul de chei utilizate. Criptarea simetrică utilizează o singură cheie, în timp ce criptarea asimetrică utilizează două chei diferite, dar înrudite. Una dintre chei este cheia privată, iar cealaltă este cheia publică. Algoritmii de criptare simetrică folosesc aceeași cheie pentru a efectua atât funcții de criptare, cât și de decriptare. Algoritmul de criptare asimetrică folosește o cheie pentru a cripta datele și o altă cheie pentru a le decripta. Aceasta înseamnă că, dacă vrem să trimitem cuiva un mesaj criptat, îl criptăm cu cheia publică a destinatarului, iar destinatarul folosește cheia sa privată pentru a-l decripta.

Un alt criteriu de împărțire a criptării este acela al lungimii cheii. Lungimea cheii este direct legată de nivelul de securitate oferit de fiecare dintre algoritmii criptografici. Cu cât cheia este mai lungă, cu atât datele sunt mai sigure. În algoritmii simetrici, cheile sunt selectate aleatoriu și lungimea lor este de obicei de 128 sau 256 de biți, în funcție de nivelul de securitate necesar. În cazul criptării asimetrice, pentru ca criptarea și decriptarea să aibă loc, trebuie să existe o relație matematică între cheile publice și private (sub forma unei formule matematice unice).

Datorită vitezei sale mai mari, criptarea simetrică este utilizată pe scară largă pentru a proteja informațiile în multe sisteme informatice moderne, cum ar fi Advanced Encryption Standard (AES) utilizat de guvernul SUA pentru a cripta informațiile confidențiale și secrete. AES a înlocuit standardul anterior de criptare a datelor (DES).

Criptarea asimetrică este utilizată în sistemele în care mai mulți utilizatori pot necesita acces atât la criptarea, cât și la decriptarea unui mesaj sau a unui set de date. Un exemplu ar fi criptarea

e-mailului în care cheia publică poate fi folosită pentru a cripta mesajul și cheia privată poate fi folosită pentru a-l decripta.

O soluție este standardul OpenPGP. Definește extensiile de e-mail criptografice - criptare și semnături digitale. Standardul sa bazat pe programul PGP existent. În prezent, există multe implementări diferite. Standardul este definit în RFC 4880. Adesea, utilizatorii folosesc clientul de e-mail Thunderbird în procesul de trimitere a e-mailurilor. Acest client vă permite să trimiteți și să primiți e-mailuri criptate și semnate digital folosind standardul OpenPGP. Această caracteristică este cunoscută în mod obișnuit ca criptare end-to-end (e2ee) și face comunicarea mai sigură și mai puțin probabil să fie spionată de terți. Thunderbird 78 are suport încorporat pentru două standarde de criptare, OpenPGP și S/MIME.

Versiunile anterioare de Thunderbird (v68 și anterioare) aveau suport S/MIME încorporat și puteai adăuga suport OpenPGP utilizând suplimentul Enigmail și software-ul GnuPG. Suplimentul Enigmail nu mai este disponibil pentru Thunderbird 78, decât pentru a-i ajuta pe foștii săi utilizatori să migreze la OpenPGP în Thunderbird 78 sau pentru a obține îndrumări despre cum să-și restabilească regulile „Junior Mode” din Enigmail. Puteți actualiza setările Thunderbird de la o versiune mai veche (de exemplu, 68.x) la versiunea 78.x. Cu toate acestea, înainte de a utiliza Thunderbird 78 pentru prima dată, este recomandat să faceți o copie de rezervă a profilului dvs. Thunderbird, deoarece după actualizare, profilul nu mai poate fi utilizat cu Thunderbird 68.

Enigmail a folosit GnuPG pentru a stoca și gestiona toate cheile și setările de încredere. Puteți migra și Enigmail va citi cheile vechi din GnuPG și le va importa. Thunderbird 78 folosește setări diferite decât Enigmail. Cu Enigmail, a fost posibil să activați OpenPGP pentru un cont de e-mail, dar lăsați-l să aleagă automat ce cheie să folosească. Thunderbird 78 combină aceste setări. Pentru a activa OpenPGP pentru un cont de e-mail, trebuie să specificați în mod explicit ce cheie să utilizați.

Software-ul GPG4win va fi folosit pentru criptare. Este un set de instrumente avansate de criptare a datelor. Permite protecție împotriva accesului neautorizat nu numai la e-mail, ci și la fișiere și foldere. Lucrul cu Gpg4win se bazează pe criptarea asimetrică, adică pe baza a două chei - privată și publică. Primul este folosit pentru a cripta datele, al doilea ar trebui să ajungă la destinatarii mesajului care îl pot accesa. Păstrați cheia privată într-un loc sigur.

Pachetul include elemente precum instrumentul de criptare GnuPG, managerul de certificate Kleopatra (Fig. 7), managerul de certificate GPA alternativ, clientul de e-mail Claws Mail, precum și două plugin-uri care permit integrarea cu Microsoft Outlook (în versiunile 2003, 2007, 2010 și 2013) și Windows Explorer.

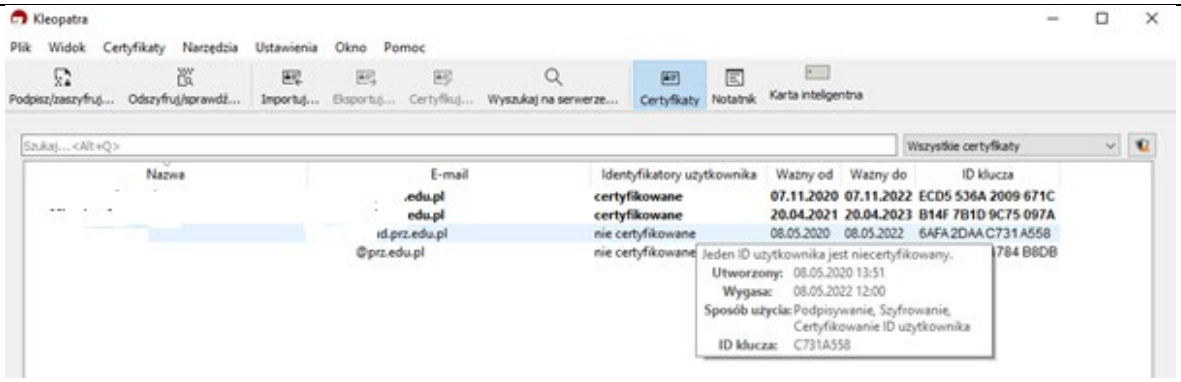

Fig. 7. Manager certificat - Kleopatra.

Gpg4win acceptă standardele OpenPGP și S/MIME (X.509), creând certificate implicit folosind chei de 2048 de biți. RSA este algoritmul standard de criptare și semnare. În plus, pachetul permite, de asemenea, generarea și verificarea sumelor de control SHA1, SHA256 și MD5.

Configurarea mediului de criptare a mesajelor.

După atribuirea conturilor de e-mail programului GPG4WIN, ar trebui generată o pereche de chei. O pereche de chei este formată dintr-o cheie privată și o cheie publică. Cheia privată este atribuită unui anumit cont. O persoană care dorește să trimită un mesaj criptat către acest cont trebuie să aibă cheia publică a destinatarului.

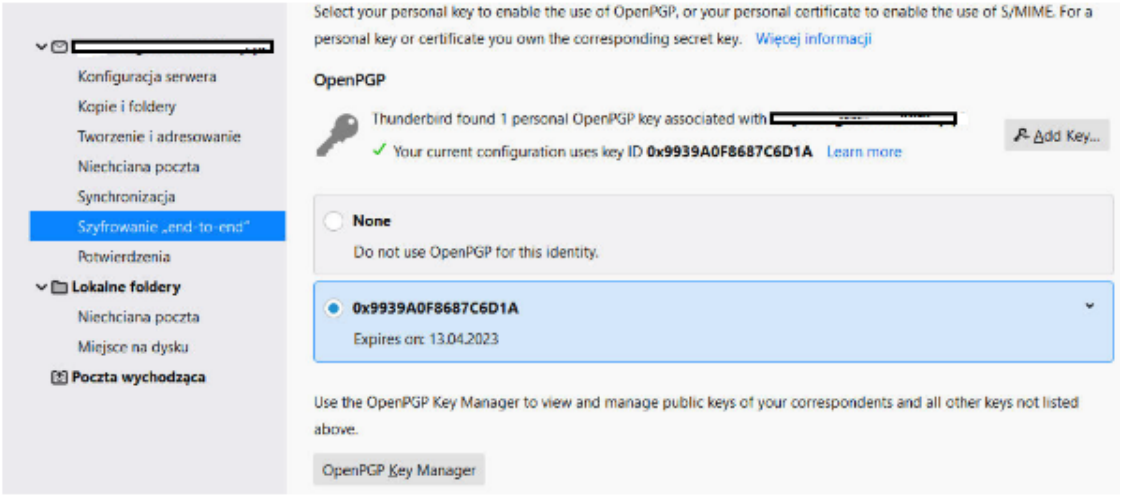

Fig. 8. Setările secțiunii Remote Desktop

Odată ce conturile au fost configurate în Cleopatra, puteți utiliza direct Thunderbird pentru a trimite și primi mesaje criptate fără a utiliza un program extern. Nu uitați să trimiteți cheia publică atunci când trimiteți primul mesaj către un nou destinatar (Fig. 8). Un exemplu de mesaj criptat este prezentat în Fig. 9.

```
-----BEGIN PGP MESSAGE-----

wcDMA0r5u59RHK/uAQv/cvK0XliobGKfmQ25IcGe4kxtcXan9oDhQ0HODeAQyLSfpPFYOitt4LpF
Kc2aae3ayqRN+0bhTESVFaxttCw76E5wszkM9cK8UdxYzrX9PuaujtzYj8kSx3m0skfXrdglYnM8
1lIYNETSgTnFSZ4jHKQLVIHVw9ZMztoo/ibLVJY3TTd7aKn7+cYyepNasrPPzoxcSGjJ1pQCkJ6t
SGtm8HDBfekKbK6qTKefYdGrCDBS4sAsuszwaX5QtSn50LAE2FkXCiKzTh6DkdFxQQ7yk/rUTs93
MkRwRtjteDqO7KC1yNPBim+KVLVG20EibD1FrdFIsbaEaPIl3Y06LhmjBMrUOUaMhPJpYDM1Ki8u
gqGHOQmqISQU1y6/poyGDmOfSPOFchWaTB+9fjzpmEb32mK10D1JOM2llut5AtmZH8W1lKpy4cdC
XygSXMkJ4as+p9/MtICdESyFkDXamESbtI04Ay5Xj+YrBnQ+Wk0lHOeLfSFg+cj7fwUuasRvEIe0
wcDMA3pK1foZRRoWAQv/UVilR5h++k8Tq8uk/IeUchC3Si832Li8Ro++dGxy65Gomjlzg+oxbOoj
0u1kZGs5QbCywv5+vlo7CxpGSeMcBbj1T5jV/cKk1An9bdCjADXFLw4sEWCtqTR47OFqArvqi2gm
2iOW4g6Zcnd2lcfGe5kmeyRKt8OmHL6LDaZXSnJCJkhNRwr3GKHh8gJeT00bn+72M9TbBKXxLe3T
bnGw2ypPIQJ55k2x+ZbgkjDnQQDogsHpB1ip7K5yYArf+rI4uPqbYQgSU3NYYAUsmOtI2yesouvV
gFic/0TE9xq0qhciE2bTWPxH5ikxCMwLQa33E8+hngsSDfoyoRdolSEwjhI8KHthzddXzPNSkdgn
Q4pdGUljFaDivtLc7cNs3SFKoZBiZcQaHRTABVNDMQgRqgoG6F0Ditu03vXCh5aR8/zUVS6moGT8
2sh/VWvryEAHKLSUPZulgwaZlD5hxosUMuwzGibLzaCApbilNdzm4zaDz2KdGBwmvyGkC7oT4lvj
0sMwAbnd2f3Hz+AuXFajZ6uO8m6ibKMtJRM3EXggkNhue0rIU4KLchp9U9jLAt6GMQjPFKmgGqEj
U7/QPiVbJ8DjbmhYH90JwYH8hJCx1rq4AtXOxJgz8w0B+MOe6maKxDaDqS9gQj/n9N/Hvj8btZKz
turb54Y8MxZXXXoNxLAVZr1HHcbQoweHIx0EXanoMsxEwT3ugAiQetwBzXnR9DOzxTkzeOMK1ooS
6jnVTQy454q1+w6fNWAfBbpYY73Lt1NifD7mHoqe1G3oWhgzj/uUs67TJ1DjLfqzhxqw0TnfXyNM
+457fZCj+iYwdV8DhfDb4dyfYmDjA8LLP8Uw7gLtkFxDldsaLf7/xQ5g98eKhz/4INI0xL+5Znno
x4SnkX++hy4z/nRKBNQcIupW7KuG1SOABTIhQWx3mtxyte0mxBRxiApfC5HfNzQM+vtmhJK8mlHK
Osc3kVw6kTodafSTi/qLghcOh2R7h8hL7qRc56ig7i4nPY5bnsPpfyyPYAuUDJQUz5z4tFrdEX/+
gw/gH3O8hTS17VSfgya0BUwJvMnlbS1+VZ7zomF405ne8hrFsT5j/dnjP7NgGS3CVMDLyEDtQA7k
Vbru0EN4JTsCu3T7rMnRrGtX1kfsTXBLayhcpbaMyHojMKw60p41o2gvTn5fw/+GJHGQdsZ3HJ+g
fr9EWKLQzQX6PSLsJ5OexLRkMtHXV4jBoSRyTzFTwprBkNNKZu2aRYa17BBFuVc5RTf8rSVWq7Eq
rKrXGOP+GgqGGTxoD8zfFtp0YJ+mP28L0DtuPnmG9IzxdbXO/JG6sT6hzPEA6MIlaW6Y++94Jpg2
XEKsGOdW9IHx9613FwjPtj6HKC8GtN5s8dgSAm3tw5KUWfchtKIOZYiynxuRnwIMN0UM0G2QFKYr
pU+50ba8rdui9D2YFzEcbw9a3meaWksO3Zvd8obQfwGFMX9DwV5VPEcmASHEUMULGBUO3KIUtaxU
Sdg9qmehxPMkkH3bB3x+G79WmV0ss0G9r+uVk/XhzxckqUI0w++q2PmWsXAIP2NsyX7W1BHyZ5J0
HhUwU1lGtpl3gv/WwOxTyoEz2oeQucK5Eq91vEwaudCnip7STqK2WpboGvAQ54ZIZRFbm/4sOd/W
4kH6xyeYBTsIf3ft7LyvoB6Xq91A1xOFe94CcAqty90FynvF26Da7QRsNQalhfhfB1bnaEQIgf+7
J9fpMYQEcC4tT8RW9vtozQurNpgZnZS9sjWjke6/j3XV7paxOW7OG8nc+1r09LQMMtVjvI5Zd1FV
JyAtr1EsoF/9MzFfofn6eCtU8VvXiS8+cIDjTqrb2EKS68Rpu9Z8LCgz
=MjYk
-----END PGP MESSAGE-----
```

Fig. 9. Un exemplu de mesaj criptat.

Thunderbird decriptează automat mesajele și atașamentele trimise împreună cu acestea. Rețineți că trebuie să cunoașteți cheile publice ale destinatarilor înainte de a trimite corespondență criptată. Criptarea cu suplimentul GPG protejează nu numai conținutul, ci și atașamentele. Fără a cunoaște cheia destinatarului, nu putem trimite un mesaj criptat. În plus, Thunderbird vă permite să sincronizați mai multe conturi de e-mail.

Întrebări:

Forumul de discuții la care se răspunde cu o scurtă explicație. Răspunsurile vor fi discutate cu mentorul în timpul sesiunilor de mentorat

1. Ce este un VPN?
2. Cum puteți utiliza soluția VPN?
3. Puteți trimite cuiva cheia dvs. privată pentru criptarea e-mailului PGP?

Întrebări de autoevaluare. După ce răspunde, cursantul poate vedea rezultatele și le poate compara cu cele salvate pe platformă

1. Metodă de acces securizat la datele dvs. din acces la distanță
2. Metode de securizare a conversației prin e-mail

Atasamente:

1. Prezentare
2. Filme video

Referințe:

1. Rana, Muhammad Ehsan & Abdulla, Mohamed & Arun, Kuruvikulam. (2021). Common Security Protocols for Wireless Networks: A Comparative Analysis. 10.2991/ahis.k.210913.080.
2. Habibi Lashkari, Arash & Sendón Varela, Juan & Samadi, Behrang. (2009). A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). 10.1109/ICCSIT.2009.5234856.
3. Kumkar, Vishal & Tiwari, Akhil & Tiwari, Pawan & Gupta, Ashish & Shrawne, Seema. (2012). Vulnerabilities of Wireless Security protocols (WEP and WPA2). International Journal of Advanced Research in Computer Engineering & Technology. 1.
4. Costa, Luís & Fdida, Serge & M. B. Duarte, Otto Carlos. (2000). An Introduction to Virtual Private Networks: Towards D-VPNs.
5. https://www.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/
6. https://www.radmin-vpn.com
7. https://www.fortinet.com/resources/cyberglossary/pgp-encryption