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

Moduli di formazione InCyT

Sicurezza delle informazioni per i dipendenti **Unità n.: (3) Settimana 5** **Nome dell'unità (modulo): (Sicurezza nei viaggi di lavoro)**	
Attività di apprendimento	❑ **Webinar** ❑ **Esercizi** ❑ **Workshop** ❑ **Presentazione** ❑ **Altro**
Apprendimento responsabile	• Mirosław Mazurek • Paweł Dymora
Obiettivi dell'attività di apprendimento	1. Reti wireless 2. VPN 3. Crittografia delle e-mail
Competenze da acquisire	• **TS3** • **SS2**
Durata dell'attività di apprendimento	2 settimane
Apprendimento requisiti	***Cosa serve?***
	• Accesso a Internet • Browser Internet • MS Office365

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

Brevi informazioni sul modulo

Descrizione
L'obiettivo generale di questo modulo è quello di fornire alcune questioni teoriche e pratiche relative alla conoscenza e alle competenze pratiche in materia di sicurezza durante i viaggi di lavoro. Avrete la possibilità di proteggere la vostra rete wireless e di utilizzare reti wireless protette con l'idea della VPN. Il modulo tratterà anche come inviare e-mail in modo sicuro utilizzando il protocollo gratuito PGP per messaggi criptati che nessuno può decifrare senza il vostro permesso.

Contenuto del materiale didattico

1. Introduzione alle reti wireless. Basi teoriche: principio di funzionamento, protocolli di crittografia.

I precedenti protocolli WEP e WPA venivano utilizzati per proteggere le reti wireless, ma non erano resistenti agli attacchi degli hacker. L'introduzione del protocollo WPA2 ha permesso di garantire un livello di sicurezza sufficiente, ma non fornisce comunque una sicurezza completa. Esistono molte topologie di rete, protocolli di accesso wireless e tecniche di acquisizione dell'accesso alla rete, e per l'acquisizione delle chiavi di rete vengono utilizzate sia architetture di calcolo CPU (Central Processing Unit) che GPU (Graphics Processing Unit) [1,2].

Il WEP (Wired Equivalent Privacy) è uno dei più vecchi standard di crittografia wireless IEEE 802.11. Fornisce una protezione delle informazioni basata sull'uso dell'algoritmo RC4. Ha molte vulnerabilità di sicurezza note e per questo è stato più volte violato. È uno dei più vecchi standard per la protezione delle reti WLAN (pubblicato nel 1997). Non richiede un'elevata potenza di calcolo dei dispositivi installati. Utilizza due metodi di autenticazione degli utenti: Autenticazione aperta e Autenticazione a chiave condivisa. Inoltre, consente la verifica degli utenti in base agli indirizzi MAC fisici utilizzando l'ACL (Access Control List). Esiste una variante WEP a 64 bit (basata su una chiave a 40 bit e un vettore di inizializzazione a 24 bit) e una variante WEP a 128 bit (basata su una chiave a 104 bit). Alcuni produttori hanno introdotto anche uno standard WEP a 256 bit [1,2].

WPA (Wi-Fi Protected Access) è un altro standard per la crittografia delle reti wireless IEEE 802.11. È stato introdotto per migliorare il livello di sicurezza delle reti WLAN. È stato introdotto per migliorare il livello di sicurezza delle reti WLAN, sostituendo le vulnerabilità note dello standard WEP. Si basa sull'uso di protocolli: TKIP (Temporal Key Integrity Protocol) ed EAP (Extensible

Authentication Protocol), lo standard 802.1x e il meccanismo MIC (Message Integrity Check). Lo standard si basa sull'algoritmo RC4. È stato implementato come soluzione intermedia tra lo standard WEP e l'attuale standard di crittografia wireless più sicuro 802.11i. Funziona in due modalità, che comprendono: Enterprise (utilizzando un server RADIUS che gestisce l'assegnazione delle chiavi agli utenti) e Personal (utilizzando una chiave PSK condivisa) [1,2].

WPA2 (Wi-Fi Protected Access 2) è attualmente lo standard di crittografia più potente per le reti wireless (note anche come 802.11i). Offre una protezione delle informazioni basata sull'uso dell'AES (Advanced Encryption Standard). È stato introdotto per migliorare il livello di sicurezza delle reti WLAN, sostituendo le vulnerabilità note dello standard WEP e dello standard provvisorio WPA. Implementa il protocollo 802.1x per migliorare il controllo dell'accesso degli utenti alla rete. Funziona in due modalità, che comprendono: Enterprise (con l'utilizzo di un server RADIUS che gestisce l'assegnazione delle chiavi agli utenti) e Personal (con l'utilizzo di una chiave PSK condivisa), oggi spesso utilizzata nelle soluzioni domestiche [1,2].

L'algoritmo WEP è lo standard di crittografia meno sicuro per le reti wireless IEEE 802.11. È stato violato più volte con vari metodi a causa delle numerose vulnerabilità attualmente note negli aspetti della sicurezza. È stato violato più volte con vari metodi a causa delle numerose vulnerabilità attualmente note negli aspetti di sicurezza dell'algoritmo. I principali svantaggi dello standard includono[3]:

- Mancanza di un sistema di gestione delle chiavi definito (spesso una chiave di rete viene utilizzata da tutti i nodi di una rete wireless);
- Insufficiente dimensione in bit della chiave di rete (la prima versione dello standard WEP introduce chiavi a 40 bit);
- Dimensione di bit insufficiente del vettore di inizializzazione IV (lo standard WEP introduce un vettore di inizializzazione di 24 bit, che si rivela insufficiente e, a causa della probabilità relativamente alta di collisioni con un numero ridotto di pacchetti ricevuti, esiste la possibilità di un attacco crittografico per ottenere il valore della chiave WEP);
- Checksum ICV debole basato sulla funzione lineare CRC-32 (esiste la possibilità di modificare in modo impercettibile le informazioni inviate in rete);
- Algoritmo di crittografia delle informazioni RC4 debole (ci sono troppe dipendenze tra la chiave di rete e il risultato della crittografia delle informazioni);
- Sistema di autenticazione degli utenti insufficiente (esiste la possibilità di falsificare i messaggi di autenticazione).
- Sulla base delle debolezze presentate dell'algoritmo WEP, sono stati creati molti strumenti per condurre attacchi che testano il livello di sicurezza delle reti WLAN. Gli attacchi più popolari contro il WEP includono:
- Attacco FMS - un attacco statistico (sviluppato da Fluhrer, Mantin e Shamir) all'algoritmo RC4 utilizzato nello standard di crittografia WEP;
- Attacco KoreK - un attacco statistico (sviluppato da una persona soprannominata KoreK) che utilizza diverse dipendenze in più (rispetto all'attacco FMS) del processo di crittografia dell'algoritmo RC4;
- Attacco Chopchop - un attacco interattivo, condotto nella direzione di ottenere l'accesso alla rete decrittando gradualmente uno dei pacchetti ricevuti;

- Attacco PTW - è un attacco statistico (sviluppato da Pyshkin, Tews e Weinmann) all'algoritmo RC4 che, grazie alle dipendenze successive del processo di cifratura dei dati, aumenta significativamente la probabilità di ottenere il valore della chiave con un numero relativamente piccolo di pacchetti ricevuti.

Un altro tipo di attacco frequentemente utilizzato è l'attacco con dizionario. È uno dei metodi di forza bruta per acquisire, ad esempio, i valori delle chiavi crittografiche nelle reti di computer wireless. Per ottenere i valori delle chiavi WPA/WPA2, il metodo si basa sulla crittografia unidirezionale e sul confronto delle voci del dizionario con le informazioni contenute nella sequenza di handshake a 4 vie. Gli attacchi al dizionario vengono eseguiti con l'intento di ridurre il tempo di ottenimento dei valori delle chiavi rispetto al metodo della forza bruta. Il processo di recupero del valore della chiave continua fino a quando non si ottiene un risultato positivo (cioè quando la voce del dizionario risulta essere un valore chiave valido) o fino a quando tutte le voci del dizionario non vengono confrontate con il risultato negativo. Un risultato negativo può indicare un elevato livello di complessità del valore della chiave e la necessità di ricorrere al metodo della forza bruta[3].

Il successo di questo attacco consiste nella selezione di un dizionario appropriato. Il dizionario è un file di testo utilizzato nel caso di attacchi a dizionario per ottenere, ad esempio, valori di chiavi crittografiche. Contiene un elenco di elementi opportunamente preparati che possono costituire il valore della chiave ricercata. L'uso di dizionari nel caso di attacchi di forza consente di ridurre significativamente l'insieme dei valori esaminati, il che può accelerare il processo di acquisizione del valore della chiave crittografica. Il contenuto dei dizionari viene costruito, ad esempio, sulla base degli elementi presentati[3]:

- un elenco di parole presenti nei dizionari nazionali e stranieri;
- combinazioni di parole con lettere maiuscole e minuscole, parole scritte al contrario (cioè palindromi);
- combinazioni di voci del dizionario con vocali o consonanti tagliate;
- combinazioni di ripetizioni multiple di nomi, cognomi e voci di dizionario selezionati;
- combinazioni di parole con valori numerici, caratteri speciali, ecc;
- un elenco delle password e dei login più frequentemente utilizzati dagli utenti;
- un elenco di aziende popolari, organizzazioni, termini tecnici, nomi propri, ecc;
- fughe di informazioni (ad es. login, nickname, password) da vari portali Internet;
- combinazioni di caratteri adiacenti della tastiera per i modelli selezionati (Fig. 1).

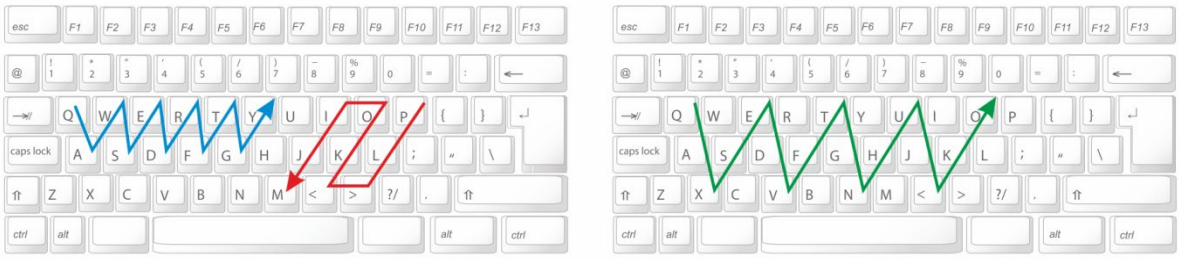

Fig. 1 . Schema che mostra esempi di modelli di creazione di chiavi di rete

La rete gioca un ruolo fondamentale nello studio della resilienza della rete. È una sequenza di caratteri utilizzata dagli utenti della rete nel processo di autenticazione. Il processo di autenticazione è un passo importante per proteggere l'accesso ai servizi condivisi e alle risorse di rete da utenti non autorizzati. Le chiavi di rete sono spesso create e gestite dagli amministratori di rete e possono costituire l'anello più debole della sicurezza di una rete informatica. I valori delle chiavi che risultano relativamente lunghi o impossibili da decifrare con metodi di forza bruta in tempi realistici dovrebbero essere generati, ad esempio, in base alle regole presentate[3]:

- Ogni rete wireless gestita dall'amministratore deve essere protetta con una chiave di rete diversa;
- Ogni utente della rete deve utilizzare una chiave di rete individuale;
- Le chiavi di rete devono essere costruite su un numero sufficiente di caratteri;
- La generazione delle chiavi deve basarsi sullo spazio massimo disponibile per i caratteri;
- Le chiavi non devono essere generate utilizzando informazioni aziendali e personali;
- La generazione delle chiavi non deve basarsi su un elenco di voci presenti in dizionari pubblicamente disponibili;
- Le chiavi di rete devono essere costruite sulla base di sequenze casuali di caratteri;
- Le chiavi di rete devono essere aggiornate periodicamente;
- I valori chiave attualmente utilizzati non devono essere associati a valori chiave non più utilizzati.

2. Tunnel VPN virtuali. Basi teoriche: tipi, architettura, principio di funzionamento, protocolli di crittografia. Installazione del programma Open VPN (configurazione, indirizzamento, selezione dei parametri, generazione delle chiavi).

Una rete privata virtuale ("Virtual Private Network" - VPN) è un tunnel attraverso il quale il traffico di rete privato scorre tra il mittente e il destinatario su una rete pubblica. Una rete VPN cifra tutte le attività su Internet, nasconde l'indirizzo IP e protegge l'identità dell'utente della rete. Una connessione VPN offre un accesso sicuro ad applicazioni, siti web e piattaforme di intrattenimento da qualsiasi parte del mondo. È possibile comprimere o cifrare opzionalmente i dati trasmessi per fornire una migliore qualità o un livello di sicurezza più elevato, proteggendo così la privacy all'interno della rete [4].

La creazione di un tunnel sicuro avviene tramite la prima autenticazione del client con il server VPN. Il server applica quindi un protocollo di crittografia a tutti i dati inviati e ricevuti. Per garantire la sicurezza di ogni pacchetto di dati, la VPN lo inserisce in un pacchetto esterno, che viene poi crittografato mediante incapsulamento. Questo garantisce la sicurezza dei dati durante la trasmissione ed è un componente fondamentale del tunnel VPN. Dopo che i dati raggiungono il server, i pacchetti esterni vengono rimossi nel processo di decodifica [4].

Le VPN possono essere suddivise in due categorie principali [5]:

- Una VPN ad accesso remoto che consente agli utenti di connettersi a una rete remota, di solito tramite un software speciale.

- VPN site-to-site utilizzate dalle aziende, in particolare dalle grandi società. Consentono agli utenti di località selezionate di accedere in modo sicuro alle reti di altri utenti.

Un esempio di software di sviluppo VPN dedicato è *RadminVPN*. Nella maggior parte dei casi non è necessario disporre di un indirizzo IP statico nella rete locale per configurare un tunnel VPN. Dopo aver scaricato il software appropriato, verrà creata una rete appropriata (26.0.0.0) con un indirizzo statico del computer [6].

Radmin VPN consente di connettersi a due computer su due reti diverse. Di seguito è riportato un esempio di configurazione. Per facilitare la comprensione del funzionamento del canale VPN, le Figure 2 e 3 mostrano la configurazione iniziale dei computer tra i quali deve essere creato un canale sicuro.

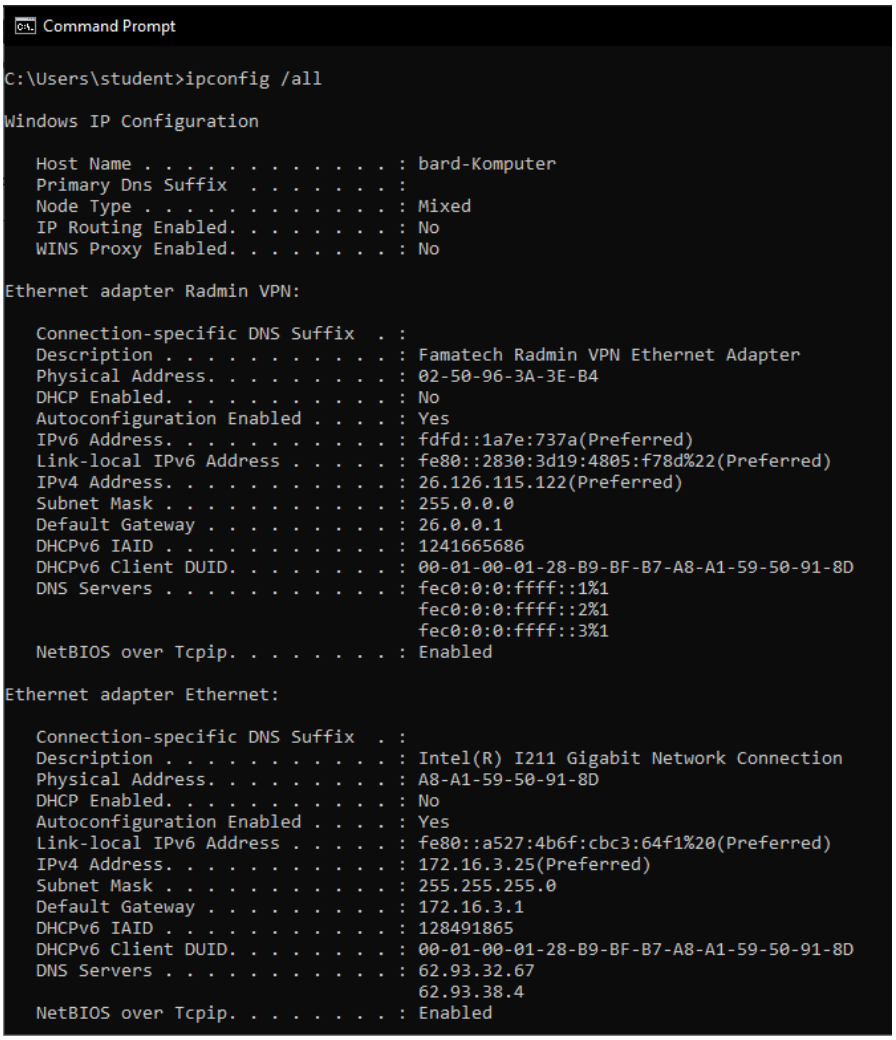

Figura 2. Configurazione iniziale dei computer

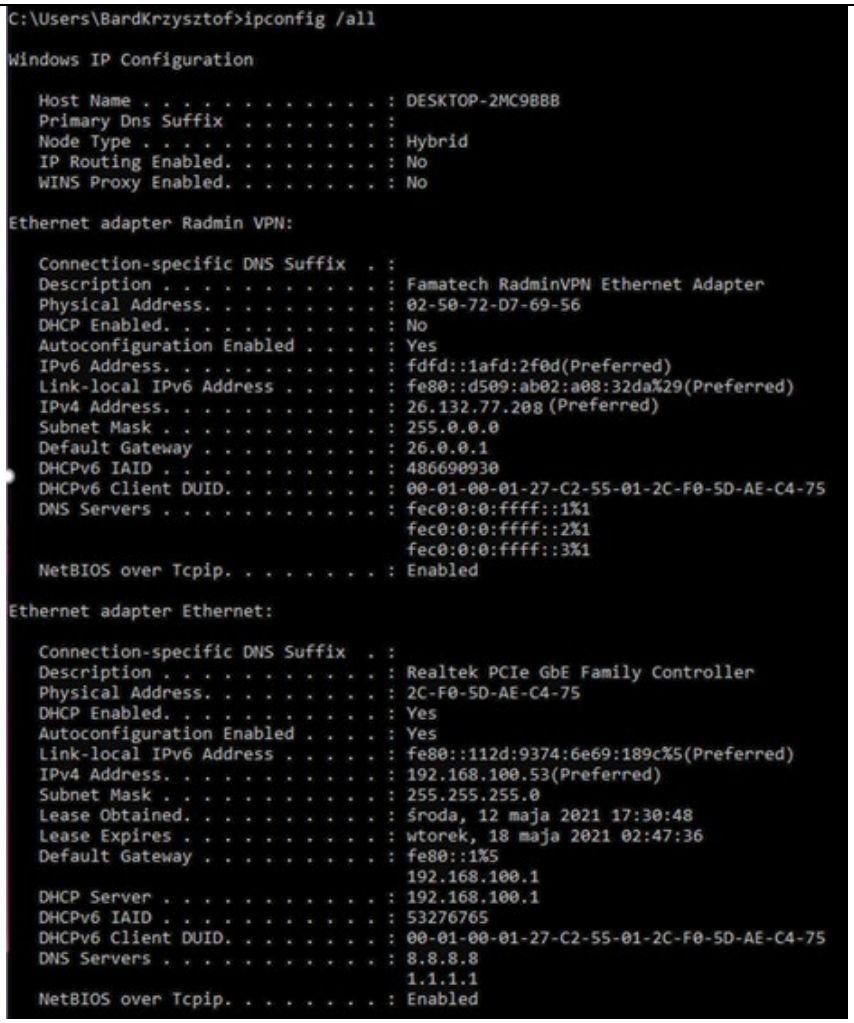

Figura 3. Configurazione iniziale dei computer

Come si può notare, gli indirizzi dei gateway sono completamente diversi, quindi i computer non hanno una connessione fisica o logica tra loro. Per creare un canale, installare RadminVPN su entrambi i computer. Su uno di essi è necessario iniziare a creare la propria rete.

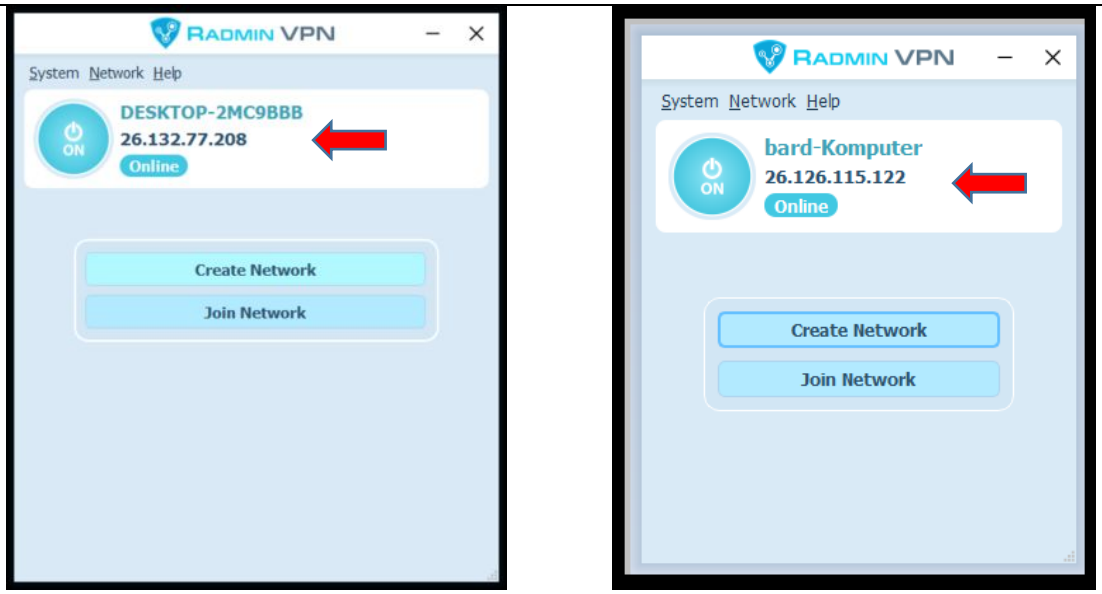

Figura 4. Vista della schermata principale dell'applicazione
(a sinistra la configurazione del computer 1, a destra quella del computer 2).

Per creare una rete, selezionare **Create Network (Crea rete)** nella finestra dell'applicazione (nella versione italiana), fornire un nome e una password per la rete e confermare con il pulsante **Create**. Sul secondo computer, la rete così creata deve essere aggiunta facendo clic sul pulsante **Join Network** (collega alla rete), inserendo il nome (qui è "Siec Niepozorna") e la password della rete appena creata.

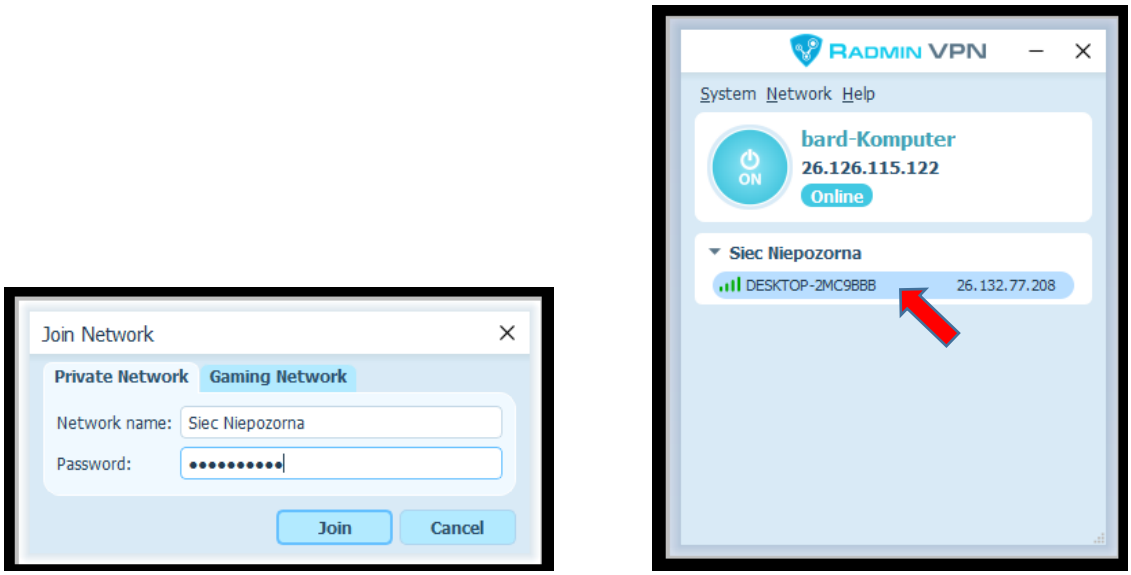

Fig. 5. a) Vista della finestra di connessione alla rete; b) Stato della connessione.

Dopo l'unione della rete, entrambi i computer dovrebbero trovarsi connessi in rete (come mostrato nella Figura 5b). In questo caso, è possibile vedere il nome e l'indirizzo del computer dall'altra parte del tunnel. Lo stesso avverrà sul secondo computer. Il tentativo di connessione in questa fase fallirà,

poiché Radmin Server è necessario per il funzionamento del sistema. Nell'applicazione appariranno informazioni sull'installazione, che dovrà essere eseguita su entrambi i computer e riavviata. Dopo aver completato l'intero processo di installazione, i computer saranno in grado di comunicare, ma non sarà possibile per uno prendere il controllo dell'altro. Per poter controllare l'uno sull'altro è necessario configurare il desktop remoto del sistema in Windows (Pannello di controllo->Sistema e a destra scegliere Impostazioni di sistema avanzate).

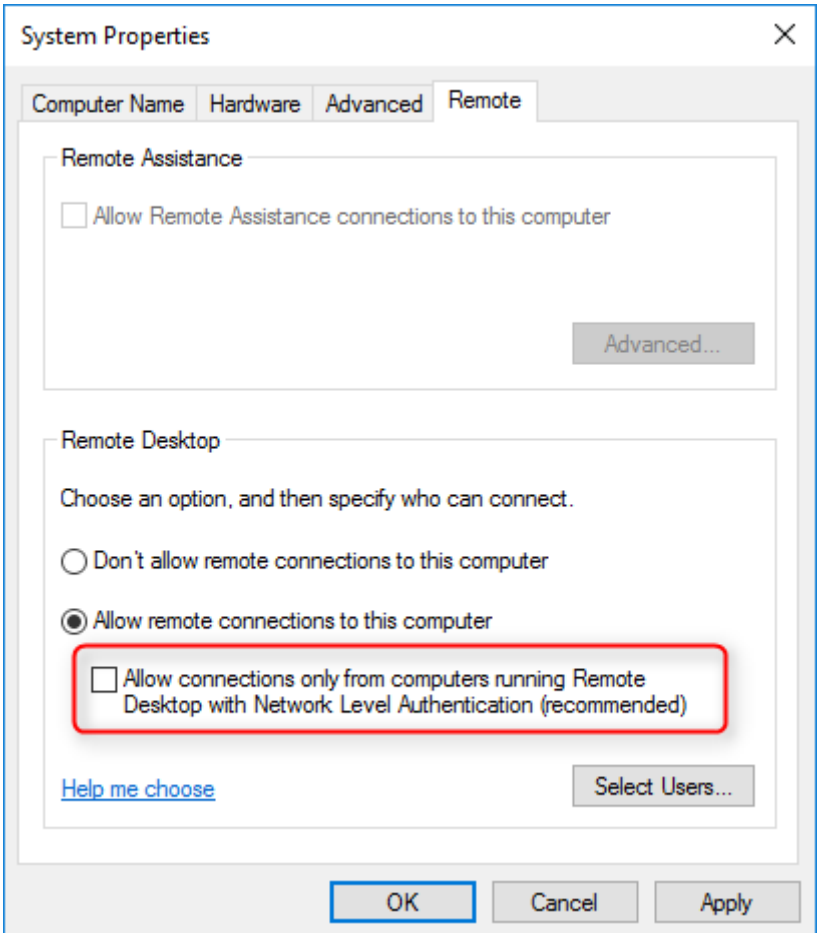

Figura 6. Impostazioni della sezione Desktop remoto
(selezionare il riquadro nella parte selezionata in rosso)

Appare la finestra “Proprietà del sistema”. Selezionare quindi la scheda *Remoto* e la sezione *Desktop remoto* selezionando *Consenti connessioni remote a questo computer* (Fig. 6). Dopo aver approvato le modifiche su entrambi i computer, creare un utente con determinati diritti di accesso. A tale scopo, eseguire RadminServer e, nei campi a destra, scegliere *Autorizzazion*i e poi l'opzione *Autorizzazioni*. Nella finestra dei permessi, selezionare *Accesso completo* e creare un utente (è necessario assegnargli un nome e una password). Questo completa il processo di configurazione del canale VPN. Il tunnel creato è bidirezionale e può essere facilmente utilizzato per controllare i computer da entrambi i lati.

3. Crittografia delle e-mail. Basi teoriche: tipi di crittografia (simmetrica e asimmetrica), sicurezza, protocolli, chiavi. Installazione e configurazione di OpenPGP. Installazione e configurazione di un client di posta elettronica.

Uno dei canali di comunicazione più utilizzati è la posta elettronica (e-mail), che sta diventando sempre più un obiettivo per gli attacchi di hacking. La protezione di questo elemento è una parte importante di un pacchetto di soluzioni di sicurezza informatica. La protezione della posta elettronica e la crittografia degli allegati sono due aspetti molto importanti per la sicurezza online. La crittografia delle e-mail non solo riduce al minimo il rischio di fuga di dati riservati, ma impedisce anche l'intercettazione non autorizzata. Le e-mail e i relativi allegati non sono protetti per impostazione predefinita dai protocolli SSL e TLS e tutti i messaggi vengono inviati in chiaro [8].

Gli algoritmi di crittografia, come la crittografia, si dividono in due categorie:

- algoritmi di crittografia simmetrica;
- algoritmi di crittografia asimmetrica;

La differenza principale tra i due metodi di crittografia è il numero di chiavi utilizzate. La crittografia simmetrica utilizza una sola chiave, mentre la crittografia asimmetrica utilizza due chiavi diverse ma correlate. Una delle due chiavi è la chiave privata e l'altra è la chiave pubblica. Gli algoritmi di crittografia simmetrica utilizzano la stessa chiave per eseguire le funzioni di crittografia e decrittografia. L'algoritmo di crittografia asimmetrica utilizza una chiave per crittografare i dati e un'altra per decifrarli. Ciò significa che se vogliamo inviare un messaggio cifrato a qualcuno, lo cifriamo con la chiave pubblica del destinatario e quest'ultimo usa la sua chiave privata per decifrarlo.

Un altro criterio per dividere la crittografia è quello della lunghezza della chiave. La lunghezza della chiave è direttamente correlata al livello di sicurezza fornito da ciascun algoritmo crittografico. Più lunga è la chiave, più sicuri sono i dati. Negli algoritmi simmetrici, le chiavi sono selezionate in modo casuale e la loro lunghezza è in genere di 128 o 256 bit, a seconda del livello di sicurezza richiesto. Nel caso della crittografia asimmetrica, affinché la crittografia e la decrittografia abbiano luogo, deve esistere una relazione matematica tra la chiave pubblica e quella privata (sotto forma di una formula matematica unica).

Grazie alla sua maggiore velocità, la crittografia simmetrica è ampiamente utilizzata per proteggere le informazioni in molti sistemi informatici moderni, come l'Advanced Encryption Standard (AES), utilizzato dal governo degli Stati Uniti per crittografare informazioni riservate e segrete. L'AES ha sostituito il precedente standard di crittografia dei dati (DES).

La crittografia asimmetrica è utilizzata nei sistemi in cui più utenti possono richiedere l'accesso sia alla crittografia che alla decrittografia di un messaggio o di un insieme di dati. Un esempio è la crittografia delle e-mail, dove la chiave pubblica può essere utilizzata per crittografare il messaggio e la chiave privata per decifrarlo.

Una soluzione è lo standard OpenPGP. Definisce le estensioni crittografiche delle e-mail - crittografia e firme digitali. Lo standard si basa sul programma PGP esistente. Attualmente esistono molte implementazioni diverse. Lo standard è definito nella RFC 4880. Spesso gli utenti utilizzano il client di posta elettronica Thunderbird per l'invio di e-mail. Questo client consente di inviare e ricevere e-mail crittografate e firmate digitalmente utilizzando lo standard OpenPGP. Questa funzione è comunemente nota come crittografia end-to-end (e2ee) e rende la comunicazione più sicura e meno soggetta a spionaggio da parte di terzi. Thunderbird 78 ha il supporto integrato per due standard di crittografia, OpenPGP e S/MIME.

Le versioni precedenti di Thunderbird (v68 e precedenti) avevano il supporto S/MIME integrato ed era possibile aggiungere il supporto OpenPGP utilizzando il componente aggiuntivo Enigmail e il software GnuPG. Il componente aggiuntivo Enigmail non è più disponibile per Thunderbird 78, se non per aiutare i vecchi utenti a migrare a OpenPGP in Thunderbird 78 o per ottenere indicazioni su come ripristinare le regole della "Modalità Junior" da Enigmail. È possibile aggiornare le impostazioni di Thunderbird da una versione precedente (ad esempio 68.x) alla versione 78.x. Prima di utilizzare Thunderbird 78 per la prima volta, tuttavia, si consiglia di eseguire un backup del profilo Thunderbird, poiché dopo l'aggiornamento il profilo non può più essere utilizzato con Thunderbird 68.

Enigmail utilizza GnuPG per memorizzare e gestire tutte le chiavi e le impostazioni di fiducia. È possibile migrare ed Enigmail leggerà le vecchie chiavi da GnuPG e le importerà. Thunderbird 78 utilizza impostazioni diverse da Enigmail. Con Enigmail era possibile abilitare OpenPGP per un account di posta elettronica, ma lasciare che scegliesse automaticamente la chiave da utilizzare. Thunderbird 78 combina queste impostazioni. Per abilitare OpenPGP per un account di posta elettronica, è necessario specificare esplicitamente la chiave da utilizzare.

Per la crittografia verrà utilizzato il software GPG4win. Si tratta di un insieme di strumenti avanzati per la crittografia dei dati. Consente di proteggere dall'accesso non autorizzato non solo le e-mail, ma anche i file e le cartelle. Il funzionamento di Gpg4win si basa sulla crittografia asimmetrica, cioè su due chiavi, una privata e una pubblica. La prima viene utilizzata per cifrare i dati, la seconda deve arrivare ai destinatari del messaggio che possono accedervi. Conservare la chiave privata in un luogo sicuro.

Il pacchetto comprende elementi quali lo strumento di crittografia GnuPG, il gestore di certificati Kleopatra (Fig. 7), il gestore alternativo di certificati GPA, il client di posta elettronica Claws Mail, nonché due plugin che consentono l'integrazione con Microsoft Outlook (nelle versioni 2003, 2007, 2010 e 2013) e Windows Explorer.

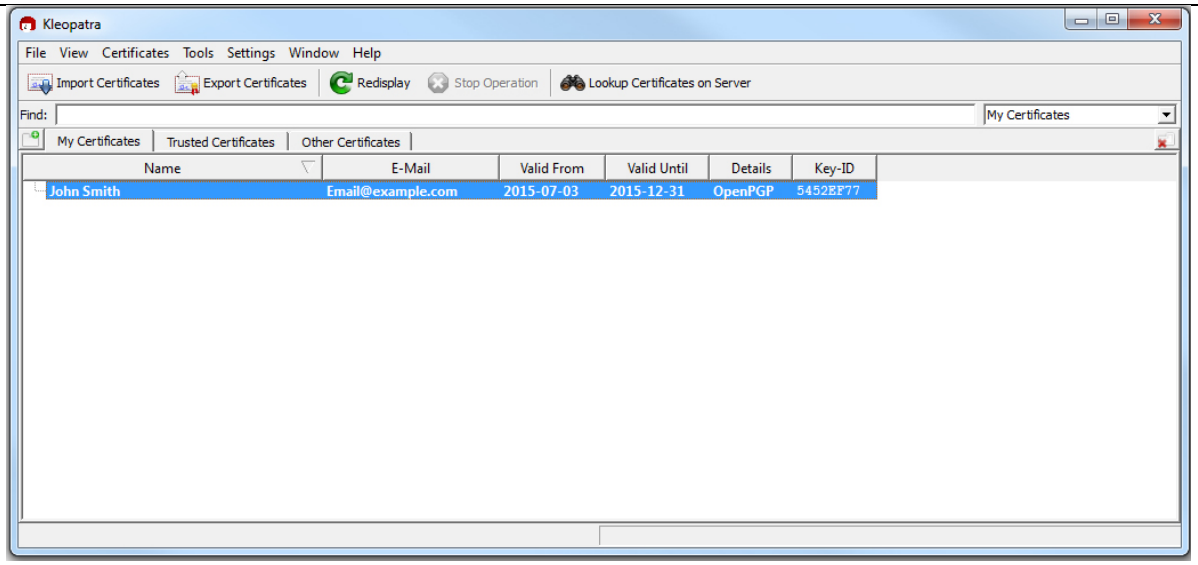

Figura 7. Gestore di certificati - Kleopatra.

Gpg4win supporta gli standard OpenPGP e S/MIME (X.509), creando certificati per impostazione predefinita utilizzando chiavi a 2048 bit. RSA è l'algoritmo standard di crittografia e firma. Inoltre, il pacchetto consente anche la generazione e la verifica di checksum SHA1, SHA256 e MD5.

Configurazione dell'ambiente di crittografia dei messaggi.

Dopo aver assegnato gli account di posta elettronica al programma GPG4WIN, è necessario generare una coppia di chiavi. Una coppia di chiavi è composta da una chiave privata e da una chiave pubblica. La chiave privata è assegnata a un account specifico. Chi vuole inviare un messaggio crittografato a questo account deve avere la chiave pubblica del destinatario.

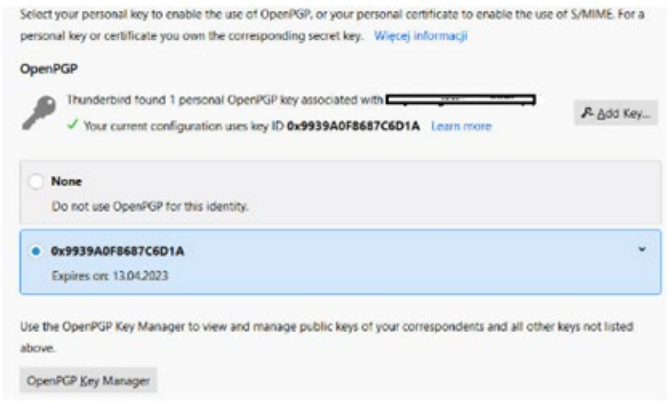

Figura 8. Impostazioni della sezione Desktop remoto

Una volta configurati gli account in Cleopatra, è possibile utilizzare direttamente Thunderbird per inviare e ricevere messaggi criptati senza utilizzare un programma esterno. Ricordarsi di inviare

la propria chiave pubblica quando si invia il primo messaggio a un nuovo destinatario (Fig. 8). Un esempio di messaggio criptato è mostrato nella Fig. 9.


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

wcDMA0r5u59RHK/uAQv/cvK0XliobGKfmQ25IcGe4kxtcXan9oDhQ0HODeAQyLSfpPFYOitt4LpF
Kc2aae3ayqRN+0bhTESVFaxttCw76E5wszkM9cK8UdxYzrX9PuaujtzYj8kSx3m0skfXrdglYnM8
llIYNETSgTnFSZ4jHKQLVIHVw9ZMztoo/ibLVJY3TTd7aKn7+cYyepNasrPPzoxcSGjJ1pQCkJ6t
SGtm8HDBfekKbK6qTKefYdGrCDBS4sAsuszwaX5QtSn50LAE2FkXCiKzTh6DkdFxQQ7yk/rUTs93
MkRwRtjteDqO7KC1yNPBim+KVLVG20EibD1FrdFIsbaEaPIl3Y06LhmjBMrUOUaMhPJpYDM1Ki8u
gqGHOQmqISQU1y6/poyGDmOfSPOFchWaTB+9fjzpmEb32mK10D1JOM2llut5AtmZH8W1lKpy4cdC
XygSXMkJ4as+p9/MtICdESyFkDXamESbtI04Ay5Xj+YrBnQ+Wk0lHOeLfSFg+cj7fwUuasRvEIe0
wcDMA3pK1foZRRoWAQv/UVilR5h++k8Tq8uk/IeUchC3Si832Li8Ro++dGxy65Gomjlzg+oxbOoj
0u1kZGs5QbCywv5+vlo7CxpGSeMcBbjlT5jV/cKk1An9bdCjADXFLw4sEWCtqTR47OFqArvqi2gm
2iOW4g6Zcnd2lcfGe5kmeyRKt8OmHL6LDaZXSnJCJkhNRwr3GKHh8gJeT00bn+72M9TbBKXxLe3T
bnGw2ypPIQJ55k2x+ZbgkjDnQQDogsHpB1ip7K5yYArf+rI4uPqbYQgSU3NYYAUsmOtI2yesouvV
gFic/0TE9xq0qhciE2bTWPxH5ikxCMwLQa33E8+hngsSDfoyoRdolSEwjhI8KHthzddXzPNSkdgn
Q4pdGU1jFaDivtLc7cNs3SFKoZBiZcQaHRTABVNDMQgRqgoG6F0Ditu03vXCh5aR8/zUVS6moGT8
2sh/VWvryEAHKLSUPZulgwaZlD5hxosUMuwzGibLzaCApbilNdzm4zaDz2KdGBwmvyGkC7oT41vj
0sMwAbnd2f3Hz+AuXFajZ6uO8m6ibKMtJRM3EXggkNhue0rIU4KLchp9U9jLAt6GMQjPFKmgGqEj
U7/QPiVbJ8DjbmhYH90JwYH8hJCx1rq4AtXOxJgz8w0B+MOe6maKxDaDqS9gQj/n9N/Hvj8btZKz
turb54Y8MxZXXXoNxLAVZr1HHcbQoweHIx0EXanoMsxEwT3ugAiQetwBzXnR9DOzxTkzeOMK1ooS
6jnVTQy454q1+w6fNWAfBbpYY73Lt1NifD7mHoqe1G3oWhgzj/uUs67TJ1DjLfqzhxqw0TnfXyNM
+457fZCj+iYwdV8DhfDb4dyfYmDjA8LLP8Uw7gLtkFxD1dsaLf7/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
HhUwUllGtpl3gv/WwOxTyoEz2oeQucK5Eq91vEwaudCnip7STqK2WpboGvAQ54ZIZRFbm/4sOd/W
4kH6xyeYBTsIf3ft7LyvoB6Xq91A1xOFe94CcAqty90FynvF26Da7QRsNQalhfhfB1bnaEQIgf+7
J9fpMYQEcC4tT8RW9vtozQurNpgZnZS9sjWjke6/j3XV7paxOW7OG8nc+1r09LQMMtVjvI5Zd1FV
JyAtr1EsoF/9MzFfofn6eCtU8VvXiS8+cIDjTqrb2EKS68Rpu9Z8LCgz
=MjYk
-----END PGP MESSAGE-----
```


Figura 9. Un esempio di messaggio criptato.

Thunderbird decifra automaticamente i messaggi e gli allegati inviati. Ricordate che è necessario conoscere le chiavi pubbliche dei destinatari prima di inviare la corrispondenza crittografata. La crittografia con il componente aggiuntivo GPG protegge non solo il contenuto, ma anche gli allegati. Senza conoscere la chiave del destinatario, non è possibile inviare un messaggio crittografato. Inoltre, Thunderbird consente di sincronizzare diversi account di posta elettronica.

Domande:

Domande Forum di discussione a cui rispondere con una breve spiegazione.

1. Che cos'è una VPN?
2. Come si può utilizzare la soluzione VPN?
3. Potete inviare a qualcuno la vostra chiave privata per la crittografia PGP delle e-mail?

Domande di autovalutazione.

1. Metodo di accesso sicuro ai vostri dati da remoto
2. Metodi per proteggere le conversazioni via e-mail

Allegati:

1. Presentazione
2. Filmati

Riferimenti:

1. Rana, Muhammad Ehsan & Abdulla, Mohamed & Arun, Kuruvikulam. (2021). Protocolli di sicurezza comuni per reti wireless: Un'analisi comparativa. 10.2991/ahis.k.210913.080.
2. Habibi Lashkari, Arash & Sendón Varela, Juan & Samadi, Behrang. (2009). Un'indagine sui protocolli di sicurezza wireless (WEP, WPA e WPA2/802.11i). 10.1109/ICCSIT.2009.5234856.
3. Kumkar, Vishal & Tiwari, Akhil & Tiwari, Pawan & Gupta, Ashish & Shrawne, Seema. (2012). Vulnerabilità dei protocolli di sicurezza wireless (WEP e WPA2). International Journal of Advanced Research in Computer Engineering & Technology. 1.
4. Costa, Luís & Fdida, Serge & M. B. Duarte, Otto Carlos. (2000). Introduzione alle reti private virtuali: Verso le D-VPN.
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