**Ministerul Educaţiei și Cercetării al Republicii Moldova**

**Universitatea Tehnică a Moldovei**

**Facultatea Calculatoare, Informatică și Microelectronică**

**RAPORT**

Lucrarea de laborator nr.4

*la Tehnologii de Securitatea Informațională*

A efectuat:

st. gr. TI-214 Buza Cătălin

A verificat: Bulai Rodica

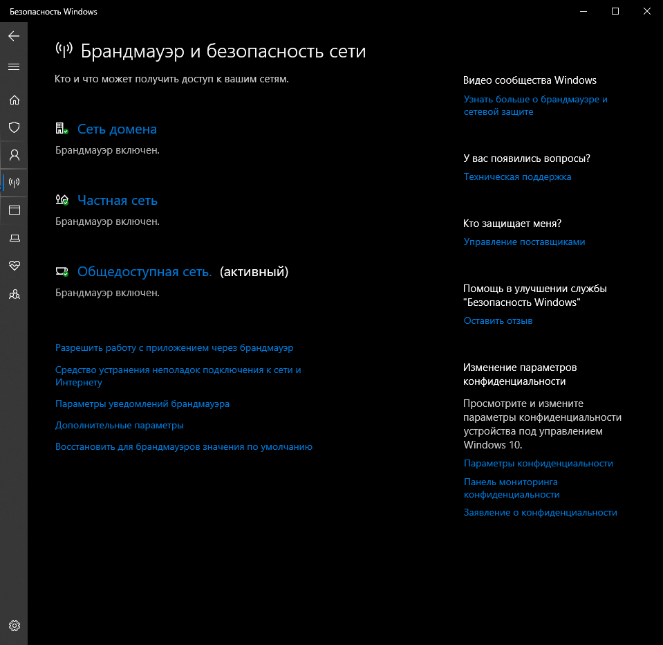
Chişinău - 2023

**1. Firewall**

* Configurarea windows firewall, configurarea firewall în linux

Firewall & de rețea în Securitate Windows vă permite să vizualizați starea Firewallului Microsoft Defender firewall și să vedeți la ce rețele este conectat dispozitivul dvs. Puteți să activați Microsoft Defender firewall și să accesați opțiunile complexe Microsoft Defender firewall pentru următoarele tipuri de rețea:

* Rețele de domeniu (loc de muncă)
* Rețele private (care se pot descoperi)
* Rețele publice (care nu se pot descoperi)



Atunci când selectați unul dintre cele trei tipuri de rețea, veți obține pagina de setări pentru aceasta. Aici, Securitate Windows vă va spune care rețele, dacă există, de acel tip la care sunteți conectat în prezent. De obicei, computerul dvs. va fi conectat doar la o singură rețea la un moment dat.

De asemenea, veți găsi un glisor simplu pentru activarea sau dezactivarea firewallului pentru acel tip de rețea.

**Important**: Dezactivarea firewallului poate crește riscul pentru dispozitivul sau datele dvs. Vă recomandăm să îl închideți, cu excepția cazului în care este absolut necesar să îl dezactivați.

Sub secțiunea Conexiuni de intrare veți găsi o singură casetă de selectare pentru Blochează toate conexiunile de intrare, inclusiv pentru cele din lista de aplicații permise. Bifarea acestei casete spune Firewallului Microsoft Defender să ignore lista de aplicații permise și să blocheze totul. Activarea acestei aplicații vă mărește securitatea, dar unele aplicații pot să nu mai funcționează.

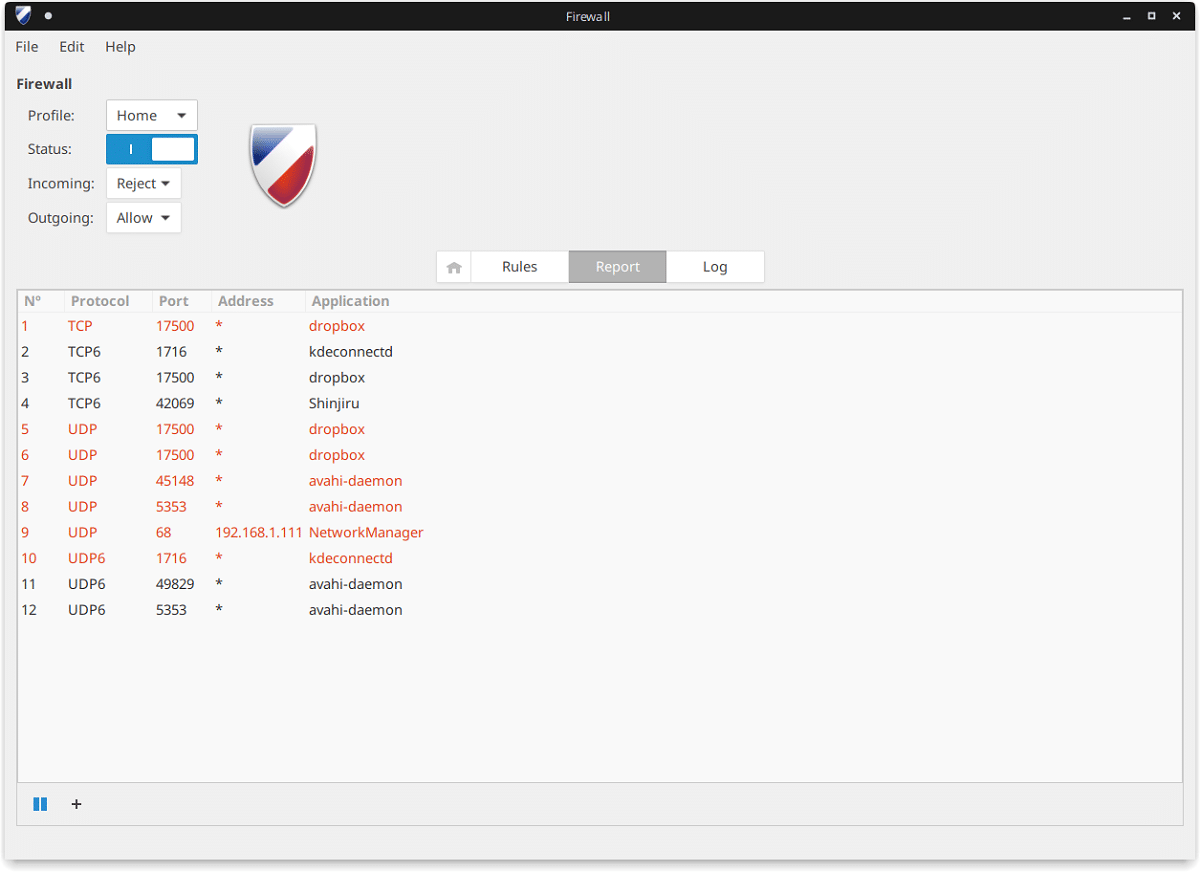
**Configurarea firewall în linux**

Deschidem terminalu si instalam aplicatia **GUFW** folosind comanda **sudo apt install gufw -y.**

Cu **GUFW** instalat în sistem, este timpul să activăm **firewall-ul**, pentru aceasta trebuie să deschidem aplicația pe care le putem găsi în meniul aplicațiilor noastre.

Cu **GUFW** deschis, prima instanță Vom vedea că este „dezactivat”.

Pentru a schimba acest lucru, în opțiuni vom vedea că există unul numit „status” și are un buton pe care urmează să îl apăsăm pentru a comuta de la „OFF” la „ON”.



Am făcut asta, putem activa oricare dintre cele trei profiluri de securitate prestabilite. Aceste profiluri de securitate vin cu reguli de filtrare preconfigurate care se ocupă de toate regulile de securitate plictisitoare.

**ACASA**

Profilul de securitate implicit pe care GUFW îl folosește când starea sa este schimbată din „dezactivat” în „activat”. Acest profil are reguli de securitate standard și permite utilizatorilor să aibă mai multe porturi deschise pentru utilizare, acesta este de obicei profilul potrivit pentru cei care nu au nevoie de multă securitate.

Pentru a trece la acest profil, trebuie doar să schimbați opțiunea „Profil” și să selectați „ACASĂ”.

**PUBLIC**

Profilul de securitate „public” este cel mai strict profil de securitate disponibil pentru sistemul de firewall GUFW. Vine cu caracteristici riguroase de filtrare și este, în general, o opțiune pentru cei care folosesc Ubuntu pe un laptop și, de obicei, se conectează la rețelele publice.

Pentru a trece la acest profil, faceți clic pe „Profil” și selectați „Public”.

**OFFICE**

Profilul de securitate „Office” pentru GUFW este aproape la fel ca «Acasă». Acest lucru este bun pentru stabilirea unor reguli speciale la locul de muncă.

Pentru a trece la acest profil, trebuie să selecteze „Office”.

* Tipuri de Firewall. Importanța

Există mai multe tipuri de firewall-uri disponibile, fiecare cu propriile caracteristici și funcționalități specifice. Iată câteva tipuri comune de firewall-uri:

* Firewall hardware - Acesta este un tip de firewall care utilizează echipamente hardware specializate pentru a filtra traficul de rețea și a proteja sistemul. Acestea sunt adesea folosite pentru protecția rețelelor de afaceri și pot oferi o protecție mai bună decât firewall-urile software.
* Firewall software - Acestea sunt firewall-uri care rulează ca software pe un sistem de operare, precum Windows Firewall. Acestea sunt adesea folosite pentru protejarea sistemelor personale și pot fi configurate pentru a bloca traficul nedorit sau pentru a permite accesul la anumite aplicații.
* Firewall bazat pe pachete - Acest tip de firewall analizează pachetele de date care intră și ies din rețea și blochează sau permite accesul în funcție de setările configurate.
* Firewall bazat pe aplicație - Acestea sunt firewall-uri care analizează traficul de rețea pentru aplicații specifice și blochează sau permite accesul în funcție de politici specifice pentru fiecare aplicație.
* Firewall de ultimă generație - Acestea sunt firewall-uri care combină caracteristici de bază ale unui firewall cu alte caracteristici de securitate, precum detecția intruziunilor, filtrarea de conținut sau protecția împotriva malware-ului.

Importanța firewall-urilor constă în protejarea sistemelor și rețelelor de atacuri cibernetice și filtrarea traficului de rețea nedorit. Acestea ajută la prevenirea accesului neautorizat la datele personale și la protejarea sistemelor de viruși și alte amenințări cibernetice. Firewall-urile sunt esențiale pentru a menține securitatea informațiilor și a proteja împotriva pierderii datelor și a daunelor financiare.

**2. VPN (Virtual Private Network)**

* Tipuri de VPN. Aplicații

Există mai multe tipuri de VPN-uri, dar cele mai comune sunt:

* VPN remote access (acces la distanță): Acesta permite utilizatorilor să se conecteze la rețeaua de la distanță prin intermediul unui server VPN. Acest tip de VPN este utilizat frecvent pentru a oferi angajaților acces la rețea atunci când lucrează în afara biroului.
* VPN site-to-site (de la site la site): Acest tip de VPN permite două sau mai multe rețele să se conecteze între ele printr-un tunel securizat, astfel încât să poată comunica între ele ca și cum ar fi o rețea comună. Acest tip de VPN este utilizat frecvent în cadrul companiilor care au sucursale în diferite locații geografice.
* VPN client-to-site (de la client la site): Acest tip de VPN permite utilizatorilor individuali să se conecteze la rețeaua unei companii prin intermediul unui server VPN. Acest tip de VPN este utilizat frecvent de către angajații care lucrează la distanță sau de către clienții care doresc să acceseze serviciile unei companii.

Exemple de aplicații de VPN includ:

* **OpenVPN** - este o soluție VPN open-source, care oferă o criptare puternică și se poate configura pentru a se integra cu diferite protocoale VPN, precum SSL/TLS, IPsec și PPTP.
* **SoftEther VPN** - este o soluție VPN open-source care oferă suport pentru multiple protocoale VPN, printre care SSL-VPN, L2TP/IPsec, OpenVPN și Microsoft Secure Socket Tunneling Protocol.
* **WireGuard** - este o soluție VPN modernă, open-source și ușor de configurat, care oferă o performanță excelentă și securitate puternică.
* **ZeroTier** - este o soluție VPN peer-to-peer, care permite conectarea dispozitivelor la o rețea virtuală globală. ZeroTier oferă o securitate puternică și o performanță excelentă, fiind folosită în diverse aplicații, de la jocuri video la infrastructuri cloud.
* **NordVPN** - este o soluție VPN comercială, care oferă o criptare puternică, servere în mai mult de 60 de țări și suport pentru mai multe protocoale VPN. NordVPN este folosită pentru protecția datelor personale, accesarea conținutului geo-restricționat și navigarea anonimă pe internet.
* Setarea unui VPN

Intram in setari „Rețea și internet, in subsecțiunea VPN, apasăm pe butonul numit “Adăugați o conexiune VPN”.

Aplicația Setări deschide un expert numit “Adăugați o conexiune VPN”, în care trebuie să introduci detaliile conexiunii VPN.

Mai întâi să alegi un furnizor de VPN. În primul câmp al expertului “Adăugați o conexiune VPN”, selectează opțiunea “Windows (încorporat)” (oricum, este singura opțiune disponibilă).

În câmpul următor, numit “Nume conexiune”, scrie un nume pentru conexiunea VPN pe care o creezi. Poți alege să o denumești cum vrei tu. Noi am decis să o numim Digital Citizen VPN.

Tastează adresa serverului VPN în câmpul numit “Nume sau adresă server”. Ai grijă ca datele pe care le-ai introdus să se potrivească exact cu datele oferite furnizorul de VPN.

În câmpul “Tip VPN”, selectează tipul conexiunii VPN pe care o creezi. Noi am să folosim protocolul SSTP (Secure Socket Tunneling Protocol) , deoarece aceasta este una dintre cele mai des utilizate metode de implementare a rețelelor virtuale private în Windows. Dacă nu știi ce tip de conexiune VPN trebuie să alegi, poți să lași această opțiune setată pe Automat, iar Windows 10 ar trebui să îl detecteze singur.

Toți furnizorii de VPN îți solicită să utilizezi o metodă predefinită de autentificare, pentru a te putea conecta la rețelele lor virtuale private. În următorul câmp, cel numit “Tipul informațiilor de conectare”, trebuie să selectezi o metodă care se potrivește cu cea oferită de furnizorul tău de VPN. Serviciul folosit de noi pentru acest ghid furnizează un nume de utilizator și o parolă pentru utilizatorii săi, așa că am selectat această opțiune din listă.

Completarea câmpurilor Numele utilizatorului și Parolă este opțională, adică poți lăsa aceste câmpuri goale, dar ți se va cere să introduci numele de utilizator și parola de fiecare dată când te vei conecta la serviciul VPN. Dacă alegi ca aceste informații să fie salvate sau să le introduci de fiecare dată când te conectezi, este în totalitate la latitudinea ta. Până la urmă este vorba de cât de securizat vrei să-ți fie sistemul. Dacă ai ales să introduci un nume de utilizator și parola asociată lui, ar trebui să bifezi și caseta “Rețineți informațiile mele de conectare”, astfel încât sistemul să îți salveze datele de conectare.

După ce ai introdus toate informațiile necesare, apasă pe butonul Salvare din colțul din dreapta jos al ferestrei.

Conexiunea VPN este acum creată și salvată și ești adus înapoi la aplicația Setări. Acum poți să începi să folosești conexiunea VPN. Citește secțiunile următoare ale acestui ghid, pentru a vedea cum te conectezi la un VPN, cum îi modifici setările avansate, cum te deconectezi de la VPN și cum ștergi conexiunea VPN atunci când nu vrei să o mai folosești.

* Protocoale VPN (IPSec SSTP), Efectul de tunel

Protocoalele VPN sunt seturi de reguli și proceduri care permit comunicarea securizată între dispozitive prin intermediul rețelei publice sau a internetului. Cele mai populare protocoale VPN sunt:

1. **IPSec (Internet Protocol Security):** Este unul dintre cele mai vechi și mai populare protocoale VPN, care oferă o conexiune securizată între două dispozitive prin criptarea datelor transmise între ele. Acest protocol poate fi utilizat atât pentru conexiuni site-to-site, cât și pentru conexiuni remote-access.
2. **SSTP (Secure Socket Tunneling Protocol):** Este un protocol VPN dezvoltat de Microsoft, care utilizează criptarea SSL/TLS pentru a crea un tunel securizat între două dispozitive. SSTP este adesea utilizat pentru conexiuni remote-access la rețelele de companii.
3. **OpenVPN:** Este un protocol open-source, care oferă o conexiune securizată între dispozitive prin intermediul tunelării traficului datelor prin intermediul protocolului SSL/TLS. Acest protocol este adesea utilizat în aplicații comerciale și în rețelele de companii.

**Efectul de tunel,** se referă la procesul de criptare și încapsulare a datelor transmise între dispozitive într-un tunel securizat, care trece prin intermediul rețelei publice sau a internetului.

Aceasta asigură confidențialitatea și integritatea datelor transmise între dispozitive și protejează împotriva interceptării și a manipulării de către terți rău intenționați.

**3. Tehnologiile IDS și IPS**

* Configurarea unui IDS (Intrusion Detection System)

Configurarea unui IDS (Sistem de detectare a intruziunilor) implică următoarele etape:

1. Definirea obiectivelor: Este important să se definească ce se dorește să se detecteze și să se monitorizeze. Aceasta poate include tipuri specifice de atacuri, trafic suspect sau comportament neobișnuit al utilizatorilor.
2. Alegerea IDS-ului: Există o varietate de IDS-uri disponibile pe piață, de la cele open-source la cele comerciale. Este important să se aleagă un IDS care să se potrivească nevoilor organizației și să ofere funcționalitățile necesare.
3. Configurarea senzorilor: IDS-ul va necesita senzori care să monitorizeze traficul de rețea sau să colecteze date de la sistemele monitorizate. Acești senzori trebuie să fie configurate corespunzător pentru a monitoriza traficul și pentru a colecta datele necesare.
4. Configurarea regulilor de detecție: Regulile de detecție sunt utilizate pentru a detecta comportamentul suspect sau atacurile cunoscute. Aceste reguli trebuie să fie configurate pentru a se potrivi cu obiectivele IDS-ului și pentru a minimizează alarmele false.
5. Configurarea alertelor: Atunci când IDS-ul detectează un comportament suspect sau un atac, trebuie să se emită alerte. Alertele trebuie să fie configurate într-un mod care să permită personalului de securitate să le gestioneze eficient.
6. Testarea IDS-ului: IDS-ul trebuie să fie testat înainte de a fi implementat în producție pentru a se asigura că funcționează corespunzător și că detectează atacurile cunoscute și comportamentul suspect.
7. Monitorizarea și actualizarea: IDS-ul trebuie să fie monitorizat în mod constant pentru a se asigura că funcționează corespunzător și că detectează noile amenințări. Este important să se mențină IDS-ul actualizat cu cele mai recente semnături de atac și reguli de detecție pentru a se asigura că detectează noile amenințări.

* Configurarea unui IPS (Intrusion Prevention System)

Un sistem de prevenire a intruziunilor (IPS) este similar unui sistem de detectare a intruziunilor (IDS), dar are și capacitatea de a opri sau bloca activitatea suspectă sau periculoasă.

Pentru a configura un IPS, următorii pași ar putea fi luați:

1. **Selecționarea IPS-ului potrivit:** Există mai multe tipuri de IPS-uri disponibile pe piață, cum ar fi IPS bazat pe semnături, IPS bazat pe comportament și IPS bazat pe politici. Este important să alegeți IPS-ul potrivit pentru afacerea dumneavoastră și să îl configurați în mod corespunzător.
2. **Configurarea regulilor:** Odată ce ați ales IPS-ul, trebuie să configurați regulile. Regulile definește comportamentul IPS-ului, cum ar fi blocarea traficului suspect sau alertarea administratorului.
3. **Configurarea politicilor:** Politicile definesc setările de securitate pentru sistemul sau rețeaua dumneavoastră. Acestea pot include setări precum reglementările de conformitate, tipurile de trafic care trebuie blocat sau monitorizat și altele.
4. **Actualizarea semnăturilor:** IPS-ul bazat pe semnături utilizează o bază de date de semnături pentru a detecta activitatea suspectă. Este important să actualizați această bază de date pentru a detecta cele mai recente amenințări.
5. **Testarea IPS-ului:** Înainte de a-l implementa pe scară largă, este important să testați IPS-ul pentru a vă asigura că acesta funcționează corespunzător și că nu interferează cu activitatea normală a rețelei.

Configurarea unui IPS poate fi un proces complex și este important să aveți experiență în domeniul securității cibernetice sau să colaborați cu un specialist pentru a vă asigura că sistemul este configurat în mod corespunzător și că oferă protecție adecvată împotriva amenințărilor.

Concluzie

În cadrul laboratorului 5 la Tehnologii de securitate informațională, am abordat subiecte importante în ceea ce privește protejarea rețelelor și a sistemelor împotriva atacurilor cibernetice. Am învățat despre configurarea firewall-urilor în diferite sisteme de operare și despre importanța acestora în protejarea rețelelor de traficul nedorit și de accesul neautorizat.

De asemenea, am explorat conceptul de VPN și am învățat despre diferitele tipuri de protocoale VPN și aplicații, precum și despre setarea unui VPN pentru a proteja traficul de rețea și a accesa rețelele de la distanță în siguranță.

Am învățat, de asemenea, despre tehnologiile IDS și IPS și despre diferența dintre ele. Am explorat configurarea acestora și am înțeles cum acestea pot ajuta la protejarea sistemelor și rețelelor împotriva atacurilor cibernetice.

În general, laboratorul 5 a furnizat cunoștințe importante despre protejarea sistemelor și rețelelor și despre diferitele tehnologii și instrumente disponibile pentru a asigura securitatea informațiilor.