Ministerul Educatiei, Culturii i Cercetarii al Republicii Moldova
Universitatea Tehnica a Moldovei
Facultatea Electronica i Telecomunicatii
Programul de masterat "Mentenanta i Managementul Retelelor de Telecomunicatii"

Admis la susiinere
ef departament TLC:
conf.univ.dr. B JAN N.

„4" 05 2018

SIMULAREA VARIANTELOR DE REALIZARE A TUNELELOR VPN iN SECURIZAREA COMUNICAȚIILOR DIGITALE

Teza de master

Masterand: Bulat Cristian

Conducator: Leet.sup.univ., Magistru,
Chihai Andrei

Chiinau 2018

REZUMAT

Dezvoltarea extraordinară pe care a cunoscut-o industria calculatoarelor a fost însoţită pas cu pas de apariţia şi extinderea reţelelor. Dezvoltarea unei reţele private de calculatoare asigură securitatea şi integritatea transportului de date, uşurează munca angajaţilor instituţiei prin folosirea noilor tehnologii de comunicare şi transmisie de date, iar reţelele private pot fi dezvoltate în orice organizaţie privată sau publică.

În această lucrare voi încerca sa evidenţiez clar procesul de configurare a diferitelor tipuri de tuneluri de securitate, dar şi importanţa deosebita care trebuie acordata problemei securităţii, deoarece internetul se confruntă cu ameninţări de securitate din ce în ce mai avansate.

Se va simula în emulatorul GNS3 o reţea TCP/IP. Aceasta va transfera date în text clar (necriptate), printr-un tunel IPSec (atît tunel LAN-to-LAN cît şi remote-access), printr-un tunel GRE şi printr-un tune! GR E over IPSec. De asemenea se va analiza conectarea la un echipament de reţea cu ajutorul protocolului SSH configurat cu chei asimetrice. Se va compara cantitatea de date suplimentare pe care îi adaugă unui pachet de date ,.e?antion".

SUMMARY

The extraordinary development that has known computer industry has been accompanied by the emergence step and extension. Developing a private network of computers institution employees work easier by using new technologies of communication and data transmission, and private networks can be developed in any public or private organization.

In this document, I will try to highlight the process of configuring various types of security tunnels, but also the special importance that should be given to the security problem, as the Internet is increasingly threatened with security.

I will simulate a TCP / IP network in the GNS3 emulator. It will send data in clear form through the IPSec tunnel (LAN-to-LAN tunnel and remote access tunnel) through the GRE tunnel and through the GRE tunnel over IPSec. I will also consider connecting to network equipment using the SSH protocol configured with asymmetric keys. I will compare the amount of data that it adds to the data packet.

BIBLIOGRAFIE

1. *Reţele private virtuale pentru interconectarea diferitelor sisteme autonome* - Emilia- Andreea Nicolae, Victor Croitoru, Marius Iordache, Editura A.G.I.R., Seria Studii şi cercetări, 2013.
2. Reţea virtuală IT-C pentru unităţi de învăţământ şi cercetare dispersate geografic CERVIT,
   Proiect coordonat de I.N.S.C.C, 2009.
3. Modul de funcționare a protocolului SSH, Sarath Pillai, blog post, 2013, http://www.slashroot.in/secure-shell-how-does-ssh-work
4. *Virtual Private Network, Pre-Shared Key, Certificate Authority, NetBSD, FreeBSD, OpenBSD, Linux, Solaris (Operating System), Transport Layer Security* - Lambert M. Surhone, Miriam T. Timpledon and Susan F. Marseken, publicat : Betascript Publishing (February 4, 2010).
5. *Network Security, Firewalls, and VPNs* - J. Michael Stewart, **Publisher:** Jones & Bartlett Learning, September 15, 2010.
6. Bogdan Groza, “Introducere in Sisteme Criptografice cu Cheie Publica”, Curs
7. Alexandru Isar, “Curs securitatea transmiterii informatiei prin internet”, Curs
8. Luminita S. , Ion B. , “Securitatea Retelelor de Comunicatii”, Casa de editura “Venus” Iasi 2008
9. Revista 52 Informatica Economică nr. 2(30)/2004 An Overview of the Attack Methods Directed Against the RSA Algorithm
10. Bogdan Groza, „Introducere în Sistemele Criptografice cu Cheie Publică”,
11. http://www.aut.upt.ro/~bgroza/iccp.pdf accesat la data 18.06.2012
12. Methods Directed Against the RSA Algorithm
13. Martin W. Murhammer, "A Comprehensive Guide to Virtual Private Networks", International Technical Support Organization 1999
14. http://www.netaccess.ro/retele_virtuale_private.html accesat la data 15.03.2012
15. http://ro.wikipedia.org/wiki/Vpn http://en.wikipedia.org/wiki/Secure_Sockets_Layer

CUPRINS

INTRODUCERE

În primii ani ale existenţei lor, reţelele de calculatoare au fost folosite de către cercetătorii din universităţi pentru trimiterea poştei electronice (serviciul de e-mail) sau pentru a permite conexiuni multiple la un server şi de către funcţionarii corporaţiilor pentru a partaja imprimantele. În aceste condiţii, problema securităţii nu atrăgea prea mult atenţia. De aceea majoritatea protocoalelor de atunci nu aveau posibilitatea de a cripta datele (ex. Telnet, RIP, etc.).

Cu timpul, oamenii cu văzut potențialul extraordinar al rețelelor de calculatoare și multiplele beneficii pe care le pot aduce: oamenii pot împărtăși cunoștințe, pot trimite poze, pot ține legătură cu persoanele dragi, putînd chiar să își plătească facturile sau să plaseze comenzi de produse on- line, doar stînd în fața computerului personal. Însă aceste beneficii aduc și o serie de consecinte negative. Potrivit buletinului de securitate Kaspersky numțrul atacurilor informatice bazate pe browser (browser-based attacks) – cum ar fi phising, Java exploits, cross-site scripting, etc. au crescut.

Atunci când oamenii folosesc Internet-ul aproape non-stop pentru a plăti facturi, pentru a achiziționa diferite produse, pentru a posta poze personale sau pentru a trimite mesaje celor dragi și în plus, folosesc parole simple și ușor de ghicit la conturile pe care le dețin, securitatea rețelelor devine o mare problemă potențiala.

Securitatea este un subiect vast și asigură o gamă de imperfecțiuni. În forma sa cea mai simpla ea asigură ca un răufăcător nu va poate citi sau chiar modifica mesajele. De asemenea ea vă poate garanta faptul că atunci când ați primit un mesaj de la persoana X, acel mesaj este într-adevar de la acea persoană și nu de la un răuvoitor. Securitatea informatică este o artă. Trebuie asigurat un echilibru între nevoia de comunicații și conectivitate și pe de altă parte, necesitatea asigurării confidențialității, integrității și autenticității informațiilor.

Așa cum medicina încearcă să prevină noi afecțiuni în timp ce le tratează pe cele actuale, securitatea informatică încearcă să prevină potențiale atacuri în timp ce minimizează efectele atacurilor actuale.

În această lucrare voi încerca să evidențiez clar procesul de configurare a diferitelor tipuri de tuneluri de securitate, dar i importanța deosebită care trebuie acordată problemei securității.