MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

Departamentul Ingineria Software și Automatică

Admis la susținere
Șef departament: conf. univ., dr. Ion FIODOROV

_____

"____" _____ 2022

Eficiența unui sistem de securitate informațională a administrării comunicațiilor mobile

Teză de master

The efficiency of an information security system of the administration of mobile communications

Student: **Roșca Florin**

Conducător: **Prof. univ. Ion Bolun**

Chișinău, 2023

ADNOTARE

În procesul de efectuare acestei lucrării, sa anlizat nivelul de securitate sistemelor informaționale „Remote Desktop Work" cu scopul de a obține o viziune concreta a posibilitatilor acestot tipuri de sistem. În mare parte scopul acestui proiect este nu atât analiza sistemelor informaționale de administare a retelelor mobile dar obținerea accesului către ele cu ajutorul diferitor modalitați de securizare a accesului la anumite resurse. Dacă vorbind depre această lucrare ca un studiu de caz vom avea un articol complex, explicat prin 3 proceduri de analiza bine cunoscute în modelarea securitatii resurselor informaționale: analiza caracteristicilor de baza, metode de securizare și analiza a securității sistemului

Cercetarile efectuate au dat ca rezultat o analiză formală de verificare a protocolului de autentificare inter - domeniu bazat pe cheia publice si private, dar și folorirea diferitor Firewall-urile de generație următoare. Folosind metoda de analiză a protocolului de securitate care constă în modelarea protocolului și a adversarului, specificarea criteriilor de securitate și demonstrarea sau verificarea criteriilor de securitate cu diferite instrumente de analiza a gradului de securitate.

Cred că ajunge despre partea abstractă a acestei lucrări și este timpul de a trece la metodele de rezolvare a scopurilor propuse de acest proiect. Nu este de mirare că exista o mulțime de limite a securitații oricarui tip de sisteme informaționale, mai ales daca accesul la aceste resurse se efectueaza online.Insa acesta modalitate de acces este strict necesara petru timpurile date cind oricare catastrofa ori naturala ori generata de om pot stopa procesul de lucru a sistemelor,deci accesul distant este un instrument vulnerabil dar destul de sigur din punct de vedere al utilizarii in diferite condiții.

Parte de practica și-a luat asupra asa resurse ca "Citrix Analytics for Security" și „VMware Horizon" care foarte bine au astupat fiecare componentă vulnerabilă din interiorul acestui sistem complex, iar partea de analiza fiind acoperită de așa distributive ca "Nessus" fiind efectuată la un grad înalt de preluare a datelor si analiza lor după diferite principii de securitate. Pentru a folosi aceste sisteme la fel a fost folosit un model de analiza a cuantificarii costurilor folosite pentru securizarea sistemelor date, furnizarea de linii directoare cu privire la cât se poate cheltui, clasificarea pentru a oferi comparabilitate internă, orientarea către bazele generale de control și contabilitate.

Iată și am ajuns la expunerea rezultatelor obținute de acestă lucrare, și din punct de vedere tehnic a fost îndeplinite toate obiectivele dar din punct de vedere al practicii cred că nu a fost deajuns analizat domeniul concret de securizare a sistemelor,adica pe partea delinii generale sa discutat o mare parte a domeniului dat dar pe linii concrete, la nivel de cod nu a fost deajuns analizate sisteme aleste ca prototip.

ANNOTATION

In the process of carrying out this work, the security level of the "Remote Desktop Work" information systems was analyzed in order to obtain a concrete vision of the possibilities of this type of system. To a large extent, the purpose of this project is not so much the analysis of information systems for the administration of mobile networks, but obtaining access to them with the help of different ways of securing access to certain resources. If we talk about this work as a case study, we will have a complex article, explained by 3 well-known analysis procedures in information resource security modeling: analysis of basic characteristics, security methods and system security analysis.

The research carried out resulted in a formal verification analysis of the inter-domain authentication protocol based on the public and private key, but also the use of different next-generation Firewalls. Using the security protocol analysis method that consists of modeling the protocol and the adversary, specifying the security criteria, and proving or verifying the security criteria with various security analysis tools.

I think that's enough about the abstract part of this work and it's time to move on to the methods of solving the goals proposed by this project. It is not surprising that there are many limits to the security of any type of information systems, especially if access to these resources is carried out online. But this method of access is strictly necessary for the given times when any natural or man-made catastrophe can it stops the work process of the systems, so remote access is a vulnerable but quite safe tool from the point of view of use in different conditions.

Part of the practice took on such resources as "Citrix Analytics for Security" and "VMware Horizon" which very well plugged every vulnerable component inside this complex system, and the analysis part being covered by such distributions as "Nessus" being carried out at a high level of data retrieval and their analysis according to different security principles. To use these systems as well, a model was used to analyze the cost quantification used to secure the given systems, providing guidelines on how much can be spent, categorizing to provide internal comparability, orienting towards general control and accounting bases .

Here we come to the exposition of the results obtained by this work, and from a technical point of view all the objectives were met, but from a practical point of view, I think that the concrete area of securing the systems was not sufficiently analyzed, that is, on the part of its general delineation a large part of the given domain was discussed, but on concrete lines, at the code level, the systems chosen as a prototype were not analyzed enough.

CUPRINS

INTRODUCERE 8

1. ANALIZA DOMENIULUI DE STUDIU 9

1.1. Cele mai puțin eficiente norme 10

1.2. Norme eficiente: rețele private virtuale 11

1.3. Cea mai eficientă soluție: desktop virtual 12

2. APLICAȚIILE INFORMATICE DE MONITORIZARE ȘI ADMINISTRARE A REȚELELOR MOBILE 14

2.1. Caracteristici de bază VMware 15

2.2. Cel mai bun soft de gestionare a spațiului de coworking 16

3. METODE MODERNE DE ANALIZĂ A SECURITĂȚII APLICAȚIILOR INFORMATICE 18

3.1. Capacități importante de care va avea nevoie softul de securitate 19

3.2. Metodă de analiză a securității aplicațiilor informatice 20

4. ANALIZA COMPARATIVĂ A EFICIENȚEI APLICAȚIILOR INFORMATICE 24

4.1. Controale cuprinzătoare ale politicii 26

4.2. Analiza securității sistemelor informationale de monitorizare 27

4.3. Analiza securitătii dupa modul de acces la sistem 28

4.4. Revizuirea securității 31

CONCLUZII 34

BIBLIOGRAFIE 35

INTRODUCERE

În timpul lucrarilor la calculator, trebuie de respectat unele cerințe de siguranță și de organizat corect locul de muncă. Incepind de la regulile cele mai simple, de exemplu efectuarea lucrarilor pe tastatură cu mâini curate și uscate,apasarea tastelor correct, evitând loviturile ascuțite și fără a ține tastele în poziția apăsată, dar si nu uitind de alte reguli ce ne salveasa sanatatea cum ar fi pozitia corecta a ecranului și a corpului față de echipamentele folosite în procesul efectuării lucrarilor. La fel și securitatea electronică a procesului de lucru se efectuează dupa anumite reguli destul de simple dar nu mai puțin de importante, figura 1.

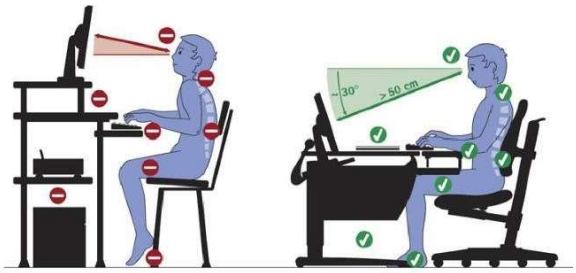

Fig. 1 Siguranța și organizarea locului de muncă

Majoritatea problemelor legate de configurarea protocolului de securitate desktop la distanță (RDP)pentru lucrul la distanță au de a face cu furnizarea de acces la RDP prin internetul public. RDP în sine nu este o setare sigură și, prin urmare, necesită măsuri de securitate suplimentare pentru a proteja stațiile de lucru și serverele. Fără protocoale de securitate adecvate, organizațiile se confruntă cu o serie de riscuri potențiale, inclusiv un risc crescut de atacuri cibernetice.

Fig. 2 Remote desktop security [1]

Pentru acest proiect sa propus ca scopul de a analiza mai multe sisteme securizat de obținere a accesului la resursele unei companii de telecomunicați în mare parte penru a rezolva acest scop se va analiza caracteristicile de baza a sistemelor date și rezolvarea vulnerabilităților acestora. Etapele de analiza este modelarea care în rezultatul modelării sistemului crează o viziune mai amănunțita a sistemului ce necesită a fi securizat. Modelele obținute în rezultatul acestor acțiuni încep de la alegerea generală a motodelor de obținere a accesului și ajung până la descrierea amănunțită a claselor care vor fi rezolvate de sistemul ales.

BIBLIOGRAFIE

1. Remote desktop security,
   https://biz30.timedoctor.com/images/2021/03/remote-desktop-security.jpg (accesat 12/22/2022)
2. Catedra Telecomunicatii
   ceee.md (accesat 12/22/2022)
3. Standard Access-List
   www.geeksforgeeks.org (accesat 12/22/2022)
4. Ce este un VPN? Ce face un VPN? | Digital Citizen
   www.digitalcitizen.ro (accesat 12/22/2022)
5. How Does Remote Desktop Work?
   www.cyberlinkasp.com (accesat 12/22/2022)
6. Citrix vs VMware
   www.inapps.net/ (accesat 12/22/2022)
7. The Importance of MS12-020
   www.trendmicro.com (accesat 12/22/2022)
8. What is VMware?
   www.educba.com (accesat 12/22/2022)
9. Best Coworking Management Software Reviewed
   coworkingresources.org (accesat 12/22/2022)
10. Cyber Threats
    fncyber.com (accesat 12/22/2022)
11. Common attack vectors
    www-techtarget-com (accesat 12/22/2022)
12. Windows DMZ VS Gateway-ul Netscaler
    https://docs.citrix.com/en-us/citrix-gateway (accesat 12/22/2022)
13. Sistema Bridge și interconectarea Serverelor externe
    https://docs.microfocus.com/OMi/10.62/Content/OMi/ConceptsGuide (accesat 12/22/2022)
14. Data Center
    https://m247.com/ro-ro/blog/ (accesat 12/22/2022)
15. Tenable Network Security Vulnerability Management
    www.infoguard.ch/en/partners (accesat 12/22/2022)