MINISTERUL EDUCATIEI, CULTURII ȘI CERCETARII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Calculatoare Informatică ȘI Microelectronică

Ingineria Software ȘI Automatică

Admis la susținere

Șef de departament:

Fiodorov I. dr., conf.univ.

_____

TESTAREA PENETRĂRII INFRASTRUCTURII INFORMATICE A UNIVERSITATII TEHNICE A MOLDOVEI

TESTING THE PENETRATION OF THE IT INFRASTRUCTURE OF THE TECHNICAL UNIVERSITY OF MOLDOVA

Student:_____ Nazaria Vladislav, SI-201M

Consultant:_____Bulai Rodica, asist. Univ.

Coordonator:_____ Antohi Ionel, asist. univ.

Chişinău 2021

UNIVERSITATEA TEHNICĂ A MOLDOVEI

Rezumat

Această teză de master a fost efectuată de studentul Nazaria Vladislav, grupa SI- 201M la tema "Testarea penetrării infrastructurii informatice a Universitatii Tehnice a Moldovei" . Însăși teza este alcătuită din Introducere, Rezumat, 3 capitole și Concluzii.

Tematica acestei teze de master constă din afișarea problemelor de securitate a datelor neprotejate și a problemelor corporative prin multitudinea acaturilor cibernetice și strângerea datelor din resurse publice (utm.md) folosind tehnologii asemănătoare cu inginerii psihologice si ininerii reverse. Sa studiat, proiectate și realizat un sistem de evidențiere a problemelor de securitate a resurselor informatice folosind diverse limbaje de programare și servicii tehnice.

Lucrarea este destinată în special administrației universității tehnice dar și pentru dezvoltatorii resurselor informatice a universității tehnice. Scopul cercetării fiind scoaterea la iveală a problemelor securității a resurselor informaționale și comportamentului în mediul virtual, dar și la fel instruirea personalului dar și a simplilor utilizatori cu scopul crearei unor abilități tehnice de protejare, profilaxie și reacționare, dar și contracatarea gaurilor și vulnerabilităților care permit obținerea unor date de pe resursele informaționale prin plasma problemelor de securitate existente și prin multitudinea problemelor factorului uman.

Obiectivele acestei lucrări au fost atinse cu succes, la fel cum fundamentarea și familiarizarea cu informațiile din sectorul securității cibernetice și a sistemelor tehnice la general, dar și a tehnologiilor de transfer de informații prin sectorul internetului

Valoarea teoretica se limiteaza în un rezumat analitic a cunoștințelor personale care au fost obținute în urmarea multitudinilor de teste de penetrarea a diverselor sisteme și a actualizărilor din sectorul informațiilor cibernetice

Valoarea aplicată a studiului este evidențiată prin analiza diferitelor tipuri de atacuri și vulnerabilități la care este expusă arhitectura de rețea și software în timpul funcționării.

Această teză de master este un studiu al celor mai recente probleme de securitate și date moderne pe care utilizatorii le postează online prin aplicațiile mobile și FAANG. Au fost testate și sistemele de operare Windows, Linux, MacOS.

Abstract

This master's thesis was performed by the student Nazaria Vladislav, group SI -201M on the topic "Testing the penetration of the IT infrastructure of the Technical University of Moldova". The thesis itself consists of Introduction, Summary, 3 chapters and Conclusions.

The theme of this master's thesis is to display the security issues of unprotected data and corporate issues through the multitude of cyber attacks and the collection of data from public resources (utm.md) using technologies similar to psychological engineers and reverse engineering. A system for highlighting the security problems of IT resources was studied, designed and developed using various programming languages and technical services.

The paper is intended especially for the administration of the technical university but also for the developers of the IT resources of the technical university. The aim of the research is to reveal the problems of security of information resources and behavior in the virtual environment, but also the training of staff and simple users in order to create technical skills for protection, prophylaxis and reaction, but also to counteract holes and vulnerabilities that allow obtaining data from information resources through the plasma of existing security problems and through the multitude of human factor problems.

The objectives of this paper have been successfully achieved, as well as substantiating and familiarizing with information in the field of cybersecurity and technical systems in general, but also information transfer technologies through the Internet sector.

The theoretical value is limited in an analytical summary of the personal knowledge that has been obtained as a result of the multitude of tests of penetration of various systems and updates in the cyber information sector.

The applied value of the study is highlighted by analyzing the different types of attacks and vulnerabilities to which the network and software architecture is exposed during operation.

This master's thesis is a study of the latest security and modern data issues that users post online through mobile and FAANG applications. Windows, Linux, MacOS operating systems were also tested.

CUPRINS

INTRODUCERE

În acesta lucrare se vor lua în considerare toate metodele de exploatare si evidențiere a problemelor legate de infrastructura informațională a universitatii tehnice.

Încă din epoca antică a fost dezvoltat un mod de a proteja informația prin secretizarea acesteia. Cel mai cunoscut algoritm a fost aplicat de împăratul Caesar pentru a proteja mesajele expediate.În secolul XXI-lea la fel se protejează datele la fel prin metode de criptare, ele oricum pot fi exploatate în scopuri malefice, fiindcă în prezent informația este putere și cel care deține informația are contolul asupra lumii din motiv ca ne aflăm la începutul erei ciberbetice.

În prezent sunt efectuate o mulțime de atacuri cibernetice asupra tuturor infrastructurilor existente începînd cu comunicații pînă la infrastructurile de alimentare cu produse si resurse energetice. Acest lucru este datorat nivelului prost de învățămînt mai ales în mediul virtual și a propagandei simple și complexe , iar in fața acestei propagande stind grupul FAANG. FAANG în real time folosesc complexul de informație pe care o distribuie toți utilizatorii ca astfel colectînd date și manipulînd utilizatorii chiar si in lumea reală nu numai și în cea virtuală.

De abia acum recent cîțiva ani in urma a început a se pune la evidență problemele legate de securitate și ca rezultat au început sa apară informatie cu acces liber in tematica securitate informațională. Au apărut astfel de site ca cyberranges.org sans.org s.a. ele toate propun resurse informatice pentru invățare si detectare a vulnerabilităților la orice nivel și la fel exploatarea lor, acest fapt a creat o bombă în cyberhacking mai ales în diviziunea black hat ceia ce lea oferit o majuscula prosibilitatea de a și realiza abilitatile pentru oamenii interesați de acest domeniu, dar la fel au si crescut numarul de doritori de a folosi cunoștințele în scopuri malițioase. La etapa acutală sistemele existente au o mutitudine de gauri de securitate din motive de instruire necalificativa a profesorilor si mentorilor, absența evidențierii pe problemele de securitate din partea sistemelor de predare și comunicare în diversitatea de domenii, începînd cu domeniile legate de tehnologii pînă la management și productie. Astfel orice nou inginer venit in companie este dezechilibrate cu cunoștințe în domeniul securității informatice și procedeul de lucru în care este implicat noul inginer, ne întelegînd cu ce poate fi testat produsul și cum de facut acest lucru . O alta cauză ca sistemele existente sunt atît de vulnerabile la diferite tipuri de atacuri prin exploatare este azartul dupa resursele monetare, în care timpul este cel mai mic resurs pentru lucru, principalul resurs aparținînd funcțiilor pe care produsul trebuie să îl ofere, în cazurile date cel mai usor este

de a introduce cod în produs pentru a avea acces la masina cu produs și la toate resursele de pe stație.

Astfel ca urmare in cadrul acestei lucrări se va efectua un proces de scanare si altul de penetrare asupra ifrastructurii informationale a universității tehnice a Republicii Moldova in comparare cu alte resurse informationale din alte țări și la fel vor fi evidențiate probleme infrastructurii și vulnerabilitățile

Bibliografie

https://www.wordstream.com/black-hat-seo

https://www.investopedia.com/terms/c/carding.asp

https://www.upguard.com/blog/cybersecurity-important

https://www.redteamsecure.com/blog/why-is-information-security-important

https://www.hackerone.com/vulnerability-management/what-are-bug-bounties-how-do-they-work-examples

https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html

https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability

https://portswigger.net/web-security/sql-injection

https://swoopnow.com/sso-authentication/

https://labs.detectify.com/2012/11/07/how-to-exploit-an-xss/

https://portswigger.net/web-security/cross-site-scripting/exploiting

https://www.techtarget.com/searchsecurity/definition/single-sign-on

https://auth0.com/learn/how-to-implement-single-sign-on/