KAUNO TECHNOLOGIJOS UNIVERSITETAS

KOMPIUTERIŲ KATEDRA

NUSIKALTIMAI ELEKTRONINĖJE ERDVĖJE IR JŲ TYRIMŲ METODIKOS

T120M152

Laboratorinio darbo ataskaita

PROGRAMINĖ TINKLO ĮRENGINIŲ ANALIZĖ

Atliko: gr.

Stud.

Patikrino:

Kaunas, 2022

# Laboratorinis darbas

**Programinė tinklo įrenginių analizė**

## Darbo priemonės

* 1. Virtualizavimo aplinka: Oracle „VirtualBox“ 6.1 arba naujesnė;
  2. Tyrimo operacinė sistema: Kali Linux 2021.1 arba naujesnė;
  3. Tyrimo įrankis: binwalk 2.2.0 arba naujesnis;
  4. Tyrimo objektas: Programinis Archer C7 V5 maršrutizatoriaus branduolys (Archer C7(EU)\_V5\_210519).

## Darbo scenarijus:

Iš žvalgybos struktūrų gauta informacija, kad Lietuvoje fiksuoti tinklo įrenginiai, kuriuose įdiegta programinė įranga turi spragų. Tuo metu Europos Komisija išplatino pranešimą, kviečiantį įvairių šalių tyrėjus atlikti pasirinkto įrenginio analizę ir pateikti išvadas. Kauno technologijos universitetas atsiliepė į kvietimą ir pradėjo tyrimą.

Jūs, kaip kibernetinio saugumo analitikas (-ė), gavote užduotį prisidėti prie atliekamo tyrimo ir atlikti preliminariąją vieno įrenginio analizę. Jūsų tyrimui buvo paskirtas „TP-Link“ gamintojo įrenginys „Archer C7 V5“, kuriame veikia „Archer C7(EU)\_V5\_210519“ sisteminis branduolys.

Iš Jūsų tikimasi gauti atsakymus: ar nagrinėjamame įrenginyje yra kibernetinio saugumo spragų, kokios jos ir kaip nuo jų apsisaugoti.

Atsakymus Universitetas prašo pateikti raštu, ataskaitos forma.

## Darbo tikslas

Susipažinti su kibernetinio saugumo tyrimuose naudojama programine aplinka, programiniais analizės įrankiais ir atlikti maršrutizatoriaus branduolio analizę.

## 

## Darbo uždaviniai

1. Susipažinti su atliktų tyrimų informacija, ja remiantis nustatyti kylančias rizikas, pateikti jas mažinančias rekomendacijas;
2. Pasirengti programinę tyrimo aplinką;
3. Atlikti tyrimą, nustatyti reikšminius elementus;
4. Pateikti tyrimo išvadas;
5. Parengti tyrimo ataskaitą.

## Darbo planas

1. Naudojant virtualizaciją, pasirengti tyrimo aplinką. Aplinkos schema pateikta 1 paveiksle.



**1 pav.** Tyrimo aplinkos schema

1. Pasirengus tyrimo aplinką, įsitikinti, kad programiniai paketai veikia. Tai padės padaryti Linux aplinkos komandos:
   1. *uname -a*
   2. *binwalk -h*
   3. *dd --version*
2. Į tyrimo aplinką atsisiųsti tyrimo objektą – „TP-Link“ maršrutizatoriaus branduolį. Tyrime naudojamas originalus gamintojo „TP-Link“ branduolys iš oficialaus šaltinio:

*https://www.tp-link.com/en/support/download/archer-c7/#Firmware*

1. Išpakuojamas atsiųstas tyrimo objektas, atliekama analizė. Rekomenduojama analizės struktūra pateikta 2 paveiksle.



**2 pav.** Rekomenduojama analizės struktūra

## UŽDUOTYS

**Remiantis tyrimo metu naudotų įrankių išvestimis ir gautais rezultatais, pateikite atsakymus:**

1. Kokia operacinė sistema buvo panaudota atliekant tyrimą? Pateikite tyrimo operacinės sistemos versiją, jos branduolio versiją. Informaciją papildomai iliustruokite ekranvaizdžiu (*angl.* Screenshot).

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Būtu galima suinstaliuoti kitą operacinę sistemą routeriui, jeigu dabartinei sistemai nebeleidžia atnaujinimų. Bet tada iškyla kitos problemos, atnaujinti reikės pačiam sistemą, galimai ne bus galima gryžti į sensnę versiją operacinės sistemos, tokiu atvėju jei norima gryžti prie senos operacinės sistemos versijos, reikės perrašyti operacinę sistemą ir viską iš naujo sukonfigūruoti.

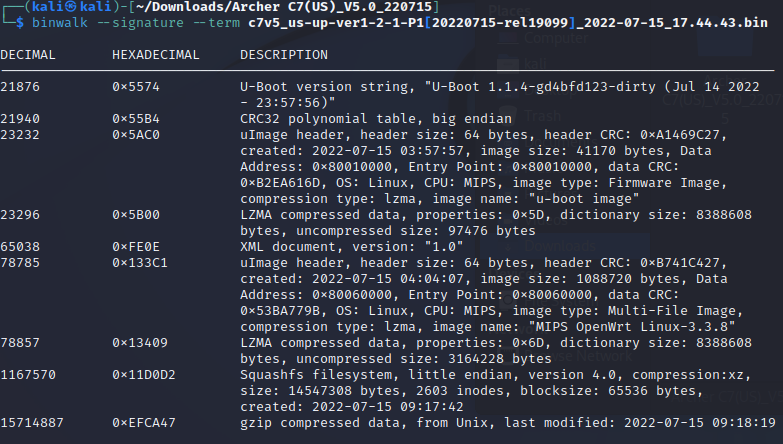
1. Kokios rinkmenos buvo gautos išpakavus .zip „TP-Link“ branduolio archyvą? Pateikite rinkmenų pavadinimus ir jų kontrolines sumas SHA-256 formatu. Kontrolinių sumų gavimui rekomenduojama naudoti *sha256sum* programą.

Text

Description automatically generated

|  |  |
| --- | --- |
| Failo pavadinimas | SHA256 suma |
| c7v5\_us-up-ver1-2-1-P1[20220715-rel19099]\_2022-07-15\_17.44.43.bin | 14bab8d9cfe2062205ec6a3975d83b8dc1f770688008b8024a8bf214bfc7fcaa |
| GPL License Terms.pdf | 7019854dd9304be13952d1adfd49a142d3773b22edce05ed1fcb4f34df385d65 |
| How to upgrade TP-Link Wireless Router.pdf | 955b7fe57333387c03b25197c0dcb97ffa0b6bf4705a758b6a5ab9ee99d961a8 |

1. Išpakavus branduolio .bin rinkmeną įrankiu *binwalk* gaunama informacija. Pateikite ekranvaizdį, iliustruojantį išpakuotą turinį.



1. Kokia yra išpakuoto branduolio Linux versija? Naudojant išorinius šaltinius, nustatykite preliminarią branduolio išleidimo datą.

Nustatyta versija yra Linux-3.3.8, šita linux versija buvo išleista 2012 metais kovo 18 dieną.

1. Naudojant atviras pažeidžiamumų CVE duomenų bazes (<https://www.cvedetails.com>, <https://cve.mitre.org/>,), nustatykite, ar naudojama branduolio versija turi pažeidžiamumų. Jeigu buvo nustatyta pažeidžiamumų, pateikite juos lentele nurodant pažeidžiamumo lygį. Nurodyti tik tuos pažeidžiamumus, kurių lygis didesnis nei 6.

|  |  |  |
| --- | --- | --- |
| Nuoroda | CVE kodas | Pažeidžeidiamumo lygis |
| https://www.cvedetails.com/cve/CVE-2013-0310/ | CVE-2013-0310 | 6.6 |
| https://www.cvedetails.com/cve/CVE-2013-1858/ | CVE-2013-1858 | 7.2 |
| https://www.cvedetails.com/cve/CVE-2013-3301/ | CVE-2013-3301 | 7.2 |
| https://www.cvedetails.com/cve/CVE-2013-6383/ | CVE-2013-6383 | 6.9 |
| https://www.cvedetails.com/cve/CVE-2012-4467/ | CVE-2012-4467 | 6.6 |

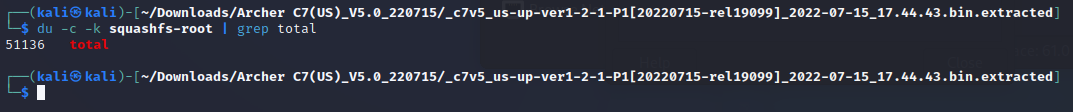
1. Kokia yra išpakuoto branduolio GCC kompiliatoriaus versija? Nustatykite preliminarią jos išleidimo datą.

U-BOOT 1.1.4-gd4bfd123-dirty Jul 14 2022

Taip pat pasidomėjau, kodėl prie rastos versijos yra parašyta „dirty“.

Priežodis „dirty“ reiškia, kad yra pakeitimų, kurių nėra oficialoje versijoje, kitaip sakant, yra pakaitimų, kurie nėra oficialioje repozitorijoje.

1. Kiek vietos diske užima išpakuota maršrutizatoriaus rinkmenų sistema (*angl.* Filesystem, *squashfs-root*)?



Išpakuota rinkmenų sistema užema 51136 kilobaitai

1. Išvardykite išpakuotos maršrutizatoriaus rinkmenų sistemos katalogus.

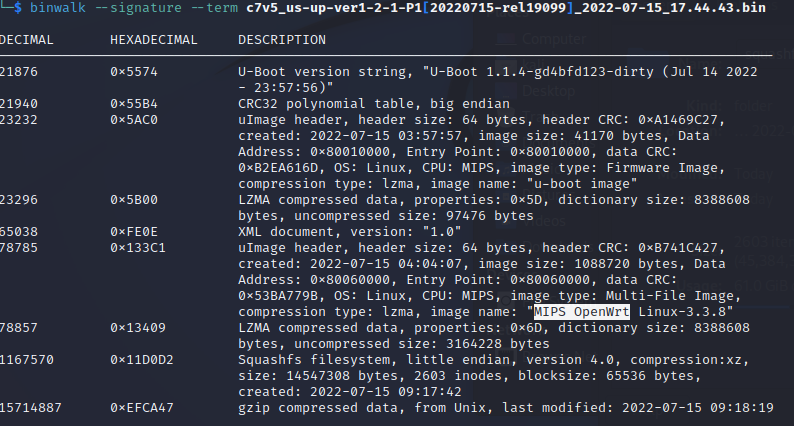
A picture containing text

Description automatically generated

|  |
| --- |
| bin |
| dev |
| etc |
| lib |
| mnt |
| overlay |
| proc |
| rom |
| root |
| sbin |
| sys |
| tmp |
| usr |
| www |

1. Kokios sistemos pagrindu (pvz. pfSense, Tomato Firmware, IPFire, OpenWRT, DD-WRT) parengta šio maršrutizatoriaus sistema?

MIPS OpenWrt



1. Išpakuotoje sistemoje yra konfigūracinė rinkmena „cloud\_config.cfg“. Pateikite jos turinį, pažymėkite adresą ir prievadą, į kurį maršrutizatorius kreiptųsi aktyvavus paslaugą. Panaudojus išorinius IP geolokacijos nustatymo įrankius (pvz. https://www.maxmind.com/) nustatykite, kokiai šaliai priklauso konfigūracijoje pateiktas adresas. Pateikite šioje rinkmenoje nurodyto sertifikato išrašą.

Pirmiausia buvo surastas failas „cloud\_config.cfg“.



Text

Description automatically generated

Text

Description automatically generated



Atlikus analize naudojant dns įrašus pastebėjau, kad šitie dns yra „Amazon“ O jei tikliau Airija, Dublinas, Unit 4033, Citywest Avenue Citywest Business Park

https://dnschecker.org/ip-whois-lookup.php?query=34.251.53.247

1. Išpakuotoje sistemoje yra rinkmena „yandex\_dns“. Pateikite šios rinkmenos išrašą. Rinkmenoje yra pažymėti IP adresai. Naudojant IP geolokacijos nustatymo įrankius, nustatykite, kokioje šalyje pažymėti IP adresai yra registruoti.

Perėjus visus rastus failus susijusius su „yandex\_dns“ sistema buvo rasti trys ip adresai:

77.88.8.8

77.88.8.88

77.88.8.7

Naudojant šitą puslapį <https://www.iplocation.net/ip-lookup> patikrinus IP adresus, matome kad jie yra registruoti Yandex kompanija, lokacija: Rusija, Maskva.

1. Remiantis išoriniais šaltiniais, įvertinkite informacijos nutekėjimo riziką įrenginyje naudojant DNS serverius, registruotus šalyse, kuriose negalioja Europos Sąjungos Bendrasis duomenų apsaugos reglamentas.

<https://www.malwarebytes.com/blog/news/2021/02/yandex-sysadmin-caught-selling-access-to-email-accounts>

<https://interestingengineering.com/innovation/yandex-hit-by-largest-known-ddos-attack-21m-requests-per-second>

Yandex kompanija, nėra pati saugiausia pasaulyje. Jai neveikia EU sajungos duomenų apsaugos reglamentas. Tokiu atveju dns valdytojas gali pardavinėti ir naudoti duomenis be jokių pasėkmių. Taip pat yra faktas, kad nei vienas dns servisas nera toks saugus kaip atrodo, jei gali buti nulažti, bei užkrauti atakuotoju.

1. Remiantis konfigūracinėmis rinkmenomis, nagrinėjamoje sistemoje savarankiškai suraskite ir pateikite vieną naują elementą, kuris Jūsų nuomone gali turėti įtakos tyrimo išvadoms. Savo nuomonę pagrįskite.

Prie biblioteku buvo rastas paketas „dos\_protection“ ir paketas „firewall“, šitie paketai pades apsaugoti tinkla nuo problemų, bet jų iki galo nesustabdys, kadangi sisteminė įranga įra pasenusi.

## IŠVADA

Ištyrus įrenginį buvo aptikatas ne viena vieta, kurią gali pasinaudoti įsilauiželis. Pirmiausia tai matoma problema yra aptikta sena routerio branduolio Linux versija (3.3.8). Sena operacinė sistema gali turėti daug pažeidimų. Būtu galima įrašyti kitą operacinę sistemą, bet tada reikės prižiūrėti ją daugiau pačiam, konfigūruoit ir tvarkyti atnaujinimus. Patikrinus pažeiždiamumus šitoje versijoje buvo rasti penki pažeidžiamumai, kurių lygis yra didesnis nei šeštas. Kitos problemos buvo rastos, įrenginys naudoja yandex dns servisus, kas gali įtakoti apsaugos pusę tiek į vieną tiek į kitą pusę. Taip pat pranaršius linux branduolį buvo pamatyta kad yra bibliotekos skirtos minimaliai apsaugai, kaip apsauga nuo dos ir ugniasiė. Atsižvelgus į surinktą informaciją, prietaisas yra pažeidžiamas ir nereikėtu juo naudotis.