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).
2. 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.
3. Išpakavus branduolio .bin rinkmeną įrankiu *binwalk* gaunama informacija. Pateikite ekranvaizdį, iliustruojantį išpakuotą turinį.
4. Kokia yra išpakuoto branduolio Linux versija? Naudojant išorinius šaltinius, nustatykite preliminarią branduolio išleidimo datą.
5. 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.
6. Kokia yra išpakuoto branduolio GCC kompiliatoriaus versija? Nustatykite preliminarią jos išleidimo datą.
7. Kiek vietos diske užima išpakuota maršrutizatoriaus rinkmenų sistema (*angl.* Filesystem, *squashfs-root*)?
8. Išvardykite išpakuotos maršrutizatoriaus rinkmenų sistemos katalogus.
9. Kokios sistemos pagrindu (pvz. pfSense, Tomato Firmware, IPFire, OpenWRT, DD-WRT) parengta šio maršrutizatoriaus sistema?
10. 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.
11. 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.
12. Remiantis išoriniais šaltiniais, įvertinkite informacijos nutekėjimo riziką įrenginyje naudojant DNS serverius, registruotus šalyse, kuriose negalioja Europos Sąjungos Bendrasis duomenų apsaugos reglamentas.
13. Remiantis konfigūracinėmis rinkmenomis, nagrinėjamoje sistemoje savarankiškai suraskite ir pateikite vieną naują elementą, kuris Jūsų nuomone gali turėti įtakos tyrimo išvadoms. Savo nuomonę pagrįskite.

**Atsakymai į užduotus klausimus**

1. .
2. .
3. .
4. .
5. .
6. .
7. .
8. .
9. .
10. .
11. .
12. .
13. .

## IŠVADA

*Iš surinktos informacijos suformuoti išvadą dėl įrenginyje galimai naudojamų pažeidžiamų paketų. Išvadoje remtis tyrimo metu gauta informacija, pažymėti konkrečius faktus (pvz. nagrinėtų versijų numerius, pažymėti nustatytus pažeidžiamumus, nurodyti jų kiekį, pavojingumo laipsnį).*