KAUNO TECHNOLOGIJOS UNIVERSITETAS

KOMPIUTERIŲ KATEDRA

Saugumo patikros ir etiško įsilaužimo technologijos

T120M154

Laboratoriniai darbai

NR. 3

Kaunas, 2021

**TRINTI, KEISTI, NUSTATYMUS, PARAMETRUS DRAUDŽIAMA!!!**

**Studento darbo vieta Nr. STUSER\_\_**

Kiekvienas studentas pasitikrina jam priskirtą naudotojo **prisijungimo vardą** <https://moodle.ktu.edu/mod/page/view.php?id=126352>

**Prisijungimui reikia:**

Prisijungimui naudoti: Putty (Windows OS); OpenSSH (Linux, Apple OS)

Jungtis per VPN **vpn.ktu.lt** (jei tai darote ne iš Lietuvos). Jei jungiatės iš KTU tinklo arba Lietuvos tinklų VPN galite nenaudoti.

Laboratorijos IP adresas: **193.219.61.183**

Naudotojo vardas: **STUSER**XX ("sudo” - administratorius, teises nepridėtos, nereikalingos užduočiai atlikti, XX – yra kiekvieno individualus)

Slaptažodis: TJCWzcMWGfRRFL

Pasikeisti slaptažodį (privaloma)!

Galite įsikelti savo sukurtą ssh raktą

Vidinė ugniasienė FW (firewall) ir tinklų sietuvas (gateway): **10.10.1.1**

Braižymas (topologijos): <http://draw.io>

Įrankiai: nmap, metasploit (papildomai: pasirinktinai)

Duomenų bazės: CVE - <https://cve.mitre.org/>, exploit-db - <https://www.exploit-db.com/>

Prisijungimo pvz.

**$ ssh STUSER01@193.219.61.183**

**Užduotis**

**I dalis**

Ištirti kompiuterinį tinklą, nustatant tinkle veikiančias paslaugas („service“), prievadus („port“). Atlikus tyrimą, išsiaiškinti ir aprašyti paslaugos pažeidžiamumą.

**II dalis**

Pasiūlyti priemonę (-es) (organizacinę arba techninę), kurios padėtų užtikrinti (padidinti) individualios informacinės sistemos apsaugą ir parašyti išvadą.

# Darbo rezultatų vertinimas

|  |  |  |  |
| --- | --- | --- | --- |
| Studento Vertinimas  (balais) | Galimas maksimalus vertinimo balas | Vertinimo objektas | Pastabos |
|  | 5 | Ištirtas kompiuterinis tinklas, nustatytos veikiančios paslaugos ir prievadai. | Informacija apie paslaugas, versijos, prievadai (services, versions, ports) |
|  | 3 | Aprašyti pažeidžiamumai pagal CVE, EDB-ID, EDB rizikos vertinimą. | Aprašyti pažeidžiamumai atitinkantis nustatytas paslaugų versijas ir prievadus. |
|  | 2 | Pateikta rekomendacija ir parašytos išvados. |  |
|  | 10 |  | |

**P I L D Y M U I**

**I dalis**

(pastaba: lentelės laukas **„pastabos“ neprivalo** būti užpildytas)

**IS SISTEMOS INFORMACIJA**

**I SISTEMA**

**IP (10.10.1.2) ADRESAS**

1 lentelė

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Eil. Nr.** | **Prievadas**  **(port)** | **Paslauga**  **(service)** | **Versija** | **Pažeidžiamumas**  **(CVE, EDB-ID, EDB)** | **Pastabos**  **(pvz. domain vardas, antraštės „banner“ informacija, kita.** |
| 1. |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**II SISTEMA**

**IP (10.10.1.4) ADRESAS**

2 lentelė

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Eil. Nr.** | **Prievadas**  **(port)** | **Paslauga**  **(service)** | **Versija** | **Pažeidžiamumas**  **(CVE, EDB-ID, EDB)** | **Pastabos**  **(pvz. domain vardas, antraštės „banner“ informacija, kita.** |
| 1. |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**III SISTEMA**

**IP (10.10.2.3) ADRESAS**

3 lentelė

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Eil. Nr.** | **Prievadas**  **(port)** | **Paslauga**  **(service)** | **Versija** | **Pažeidžiamumas**  **(CVE, EDB-ID, EDB)** | **Pastabos**  **(pvz. domain vardas, antraštės „banner“ informacija, kita.** |
| 1. |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**IV SISTEMA**

**IP (10.10.3.2) ADRESAS**

4 lentelė

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Eil. Nr.** | **Prievadas**  **(port)** | **Paslauga**  **(service)** | **Versija** | **Pažeidžiamumas**  **(CVE, EDB-ID, EDB)** | **Pastabos**  **(pvz. domain vardas, antraštės „banner“ informacija, kita.** |
| 1. |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**II dalis**

(pastaba: lentelės laukai **privalo** būti užpildyti)

**ORGANIZACINĖS IR TECHNINĖS PRIEMONĖS**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sistema** | **Aprašyto pažeidžiamumo metai**  **(metai kada paskelbtas pažeidžiamumas)** | **Aprašyto pažeidžiamumo ID (CVE, EDB-ID, EDB) numeris (ID)** | **Organizacinės, techninės priemonės apsaugai didinti (ištaisyti pažeidžiamumą / silpnumą)** |
| **I sistema** |  |  |  |
| **II sistema** |  |  |  |
| **II sistema** |  |  |  |
| **IV sistema** |  |  |  |

**TINKLO TOPOLOGINĖ SCHEMA**

**<pateikiama tinklo topologijos schema>**

**<naudojamas įrankis draw.io arba Microsoft Visio, arba bet kokį kitą>**

**IŠVADA**

**dokumentų ruošimo ataskaitai gali būti pateikti:**

* Pateikti veiksmų istoriją (~/.bash\_history).
* Pateikti visų rastų IP (sistemų) paslaugų ir prievadų informaciją.
* Aprašyti metodą, kuriuo buvo gauta informacija apie sistemas.