KAUNO TECHNOLOGIJOS UNIVERSITETAS

KOMPIUTERIŲ KATEDRA

Saugumo patikros ir etiško įsilaužimo technologijos

T120M154

Laboratoriniai darbai

NR. 4

Atliko

Grupė: IFN-1/3

Studentas (-ė): Eligijus Kiudys

Kaunas, 2022

**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)

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/>

RAV kalkuliatorius <https://moodle.ktu.edu/mod/resource/view.php?id=91074>

**Užduotis**

Atlikti kibernetinę ataką. Aprašyti kaip nustatytas pažeidžiamumas, jei pavyko pažeisti sistemą arba koks yra silpnumas, jei nepavyko pažeisti sistemos, nors toks pažeidžimumas egzistuoja. Pateikti sėkmingos arba nesėkmingos atakos įrodymo aprašą ir pasiūlyti sprendimą, kad nebūtų galimybės pasinaudoti pažeidžiamumu ir paveikti informacinę sistemą. Parašyti darbo išvadas.

# Darbo rezultatų vertinimas

|  |  |  |  |
| --- | --- | --- | --- |
| Studento Vertinimas  (balais) | Galimas maksimalus vertinimo balas | Vertinimo objektas | Pastabos |
|  | 8 | Pateikti informacinių sistemų pažeidžiamumų įrodymai ir rizikos vertinimas | Informacija sėkmingas ar nesėkmingas atakas.  Rizikos apskaičiuotos naudojantis RAV |
|  | 2 | Pateikta rekomendacija ir parašytos išvados. |  |
|  | 10 |  | |

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

**PAŽEIDIMO INFORMACIJA IR ĮRODYMAI**

**I SISTEMA**

**IP (10.10.1.2) ADRESAS**

|  |
| --- |
| **Domeno pavadinimas** **(jei nustatytas)** |
| Nenustatytas, kadangi nėra prieigos prie sistemos |

**Nustatyto pažeidžiamumo aprašymas**

|  |
| --- |
| **Pažeidžiamumas ar silpnybė (aprašyti, kaip nustatytas pažeidžiamumas, jei pavyko pažeisti sistemą arba koks yra silpnumas, jei nepavyko pažeisti sistemos, nors toks pažeidžimumas egzistuoja).** |
| „Backdoors“: gaunama prieiga prie komandinės eilutės |
| **Pavyzdys, rezultatas (pateikti sėkmingos arba nesėkmingos atakos įrodymo aprašą, pvz. darbalaukio nuotrauka, išrašas iš atakos, atliktos komandos, išbandytas pažeidžiamumas iš metaploit karkaso)** |
| Į sistemą įsibrauti nepavyko, kadangi kažkas yra palikę sukurtą sesiją ir jos neuždarę. |
| **Sprendimas (ką reikia padaryti, kad nebūtų galimybės pasinaudoti pažeidžiamumu ir paveikti informacinę sistemą?)** |
| Išanalizavus sistemą buvo atrastas pažeidimą, kuriuo galima pasinaudoti, reikėtų atnaujinti programos versiją arba nesinaudoti paslauga. |

**II SISTEMA**

**IP (10.10.1.4) ADRESAS**

|  |
| --- |
| **Domeno pavadinimas** **(jei nustatytas)** |
| Naudojant hostname -d ir hostname komandas galima gauti domeno pavadinimą:  dmz.mail.nksp.lt |

**Nustatyto pažeidžiamumo aprašymas**

|  |
| --- |
| **Pažeidžiamumas ar silpnybė (aprašyti, kaip nustatytas pažeidžiamumas, jei pavyko pažeisti sistemą arba koks yra silpnumas, jei nepavyko pažeisti sistemos, nors toks pažeidžimumas egzistuoja).** |
| Yra paliktas shell, kuris yra pririštas prie IP adreso ir prievado. |
| **Pavyzdys, rezultatas (pateikti sėkmingos arba nesėkmingos atakos įrodymo aprašą, pvz. darbalaukio nuotrauka, išrašas iš atakos, atliktos komandos, išbandytas pažeidžiamumas iš metaploit karkaso)** |
| Galima prisijungti prie atviro prievado kuris susietas su kompiuterio konsole |
| **Sprendimas (ką reikia padaryti, kad nebūtų galimybės pasinaudoti pažeidžiamumu ir paveikti informacinę sistemą?)** |
| Uždaryti prievadą, arba sukonfigūruoti taip kaip būtu prieiga tik specifiniams IP adresams. |

**III SISTEMA**

**IP (10.10.3.2) ADRESAS**

|  |
| --- |
| **Domeno pavadinimas** **(jei nustatytas)** |
| Nenustatytas, kadangi nėra prieigos prie sistemos |

**Nustatyto pažeidžiamumo aprašymas**

|  |
| --- |
| **Pažeidžiamumas ar silpnybė (aprašyti, kaip nustatytas pažeidžiamumas, jei pavyko pažeisti sistemą arba koks yra silpnumas, jei nepavyko pažeisti sistemos, nors toks pažeidžimumas egzistuoja).** |
| Yra du galimi pažeidžiamumai MS08-067 ir MS12-020 |
| **Pavyzdys, rezultatas (pateikti sėkmingos arba nesėkmingos atakos įrodymo aprašą, pvz. darbalaukio nuotrauka, išrašas iš atakos, atliktos komandos, išbandytas pažeidžiamumas iš metaploit karkaso)** |
| Buvo bandyta įsilaužti naudojant MS08-67 pažeidžiamumą, bet įsilaužti į sistemą nepavyko    Buvo tikrinama kita spraga, patikrinus spragą buvo parašyta, kad naudojant šį pažeidžiamumą galima įsilaužti į sistemą.    Naudojant kitą pažeidžiamumą pavyko padaryti DOS ataką. |
| **Sprendimas (ką reikia padaryti, kad nebūtų galimybės pasinaudoti pažeidžiamumu ir paveikti informacinę sistemą?)** |
| Atnaujinti operacinę sistemą arba nenaudoti paslaugų, kurių prievadai yra atviri. |

**IV SISTEMA**

**IP (10.10.4.5) ADRESAS**

|  |
| --- |
| **Domeno pavadinimas** **(jei nustatytas)** |
| Nenustatytas, kadangi nėra prieigos prie sistemos |

**Nustatyto pažeidžiamumo aprašymas**

|  |
| --- |
| **Pažeidžiamumas ar silpnybė (aprašyti, kaip nustatytas pažeidžiamumas, jei pavyko pažeisti sistemą arba koks yra silpnumas, jei nepavyko pažeisti sistemos, nors toks pažeidžiamumas egzistuoja).** |
| DOS, „Coldfusion V9,0,2,282541“ |
| **Pavyzdys, rezultatas (pateikti sėkmingos arba nesėkmingos atakos įrodymo aprašą, pvz. darbalaukio nuotrauka, išrašas iš atakos, atliktos komandos, išbandytas pažeidžiamumas iš metaploit karkaso)** |
| Pasinaudojus atidaryta echo paslauga galima padaryti DDos ataką    Pasinaudojus „Quote of the Day Traffic Amplification“ paslauga galima DDOS sistemą pastoviai kviečiant tą pačią komandą.  Galima nulaužti „Coldfusion“ programinę įrangą, jei būtu naudotojo sąsaja. |
| **Sprendimas (ką reikia padaryti, kad nebūtų galimybės pasinaudoti pažeidžiamumu ir paveikti informacinę sistemą?)** |
| Uždaryti nenaudojamas paslaugas, atnaujinti paslaugas arba atnaujinti programinę įrangą. |

Trust - 2x ssh

Authentication - 2x SSH 2x RDP 1x kerberos

Access – atidaryti prievadai neskaitant “Unknown” arba “TCPwraped” prievadų - 28

Non - Repudiation - IP adresu kiekis - 4x

Confidentiality – mašinos prie kurių galima prisijungti - 4x

Alarm – sistemos kurios turi antivirusines t.y „Windows“ mašinos - 2x

Vulnerabilities - ten kur yra CEV/spragos kur leidžia prisijungti 2x

Weakness - bendrai nesaugūs prievadai

Concern – versijos ar prievadai kurie yra galimai pažeidžiami - 1x SSL naudoja 1.99 versa

Exposure - nutekintos naudojamos įrangos versijos - 5x

**Table

Description automatically generated with medium confidence**

|  |
| --- |
| **Rizika (naudojamas RAV)** |
| 74.5 |

**IŠVADA**

Apibendrinus buvo bandyta laužtis į keturias sistemas. Į pirmąją sistemą įsilaužti nepavyko, kadangi kažkas paliko atidarytą sesiją. Antrojoje sistemoje buvo paliktas atidarytas prievadas, kuris yra pririštas prie „root shell“, todėl galėjau įsilaužti ir gauti „domain“ vardą. Bandant laužtis į trečią sistemą. Trečia sistema neatsako, nei „ping“ komanda, nei bandant laužtis į sistemą, jei sistema atsakytu, greičiausiai eitu į ją įsilaužti naudojant MS08-067 pažeidžiamumą. Bandant laužtis į ketvirtą sistemą, įsilaužti nepavyko. Supratau, kad nors ir yra pažeidžiamumas, bet jis gali būti sustabdytas, taip yra užkertama įsibrovėliui prieiti prie sistemos.