KAUNO TECHNOLOGIJOS UNIVERSITETAS

KOMPIUTERIŲ KATEDRA

Saugumo patikros ir etiško įsilaužimo technologijos

T120M154

Laboratoriniai darbai

NR. 1

Atliko

Grupė: IFN-1/3

Studentas (-ė): Eligijus Kiudys

Kaunas, 2022

# Legenda

Kibernetinės atakos metu, buvo pažeista svetainė. Pirminės patikros metu, nebuvo nustatyti svetainės informacijos pakeitimo požymių. Daroma prielaida, kad buvo pasinaudota svetainėje palikta spraga (pažeidžiamumu) ir bandoma užvaldyti tarnybinė stotis.

Tinklų administratorius įvardijo galimus atakų vektorius:

1. IP adresai, tinklo kaukės, paslaugos (“services”), prievadai (“port”);
2. Paliktos saugumo spragos svetainėje;
3. Įsilaužimai į viešai pasiekiamas svetaines, serverius, keičiant turinį, vagiant slaptažodžius.

# Darbo priemonės

1. Tinklo srauto atvaizdas; pcap failas;
2. Wireshark, tcpdump – tinklo srauto analizės programinė įranga;
3. Galima naudoti kitą programinę įrangą.

# Darbo rezultatų vertinimas

|  |  |  |  |
| --- | --- | --- | --- |
| Studento Vertinimas  (balais) | Galimas maksimalus vertinimo balas | Vertinimo objektas | Pastabos |
|  | 5 | Surinkta pagrindinė informacija apie IP adresus | Tik bendra informacija apie IP ir prievadus |
|  | 2 | Surinkta informacija apie WWW paslauga | TVS, IP, versija, prievadas |
|  | 3 | Surinkta informacija apie kenkėjišką kodą | IP, atgrąžos apvalkas (reverse shell), atliekamas veiksmas |
|  | 10 |  | |

UŽDUOTYS

Naudojantis tinklo analizės priemonėmis, atsakyti į žemiau pateiktus klausimus.

1. Koks svetainės tarnybinės stoties IP adresas?

|  |
| --- |
| Tarnybinės stoties IP adresas |
| 10.2.0.7 |

1. Kokia svetainės talpinimo paslauga (angl. k. service/daemon) ir kokia jos versija yra naudojama tarnybinėje stotyje?

|  |  |  |
| --- | --- | --- |
| Tarnybinės stoties IP adresas | Tarnybinės stoties WEB (HTTP) paslauga (service) | Tarnybinės stoties WEB (HTTP) paslaugos (service) versija |
| 10.2.0.7 | Apache | 2.4.29 |

1. Ar galite nustatyti kokia operacinė sistema naudojama svetainės talpinimo tarnybinėje stotyje?

|  |
| --- |
| Tarnybinės stoties operacinė sistema |
| Win 32 |

1. Ar galite nustatyti kokia turinio valdymo sistema yra naudojama svetainės administravimui?

|  |
| --- |
| Aprašyti turinio valdymo sistemą (TVS) ir pateikti įrodymų (atvaizdas – angl. k. screenshot) |
| TVS naudojama WordPress    WordPress sistema naudoja tokius sutrumpinimus, kaip wp-login, wp-json, wp-admin, wp-content. |

1. Ar galite nustatyti kokiu prievadu (angl.k. port) buvo prisijungiama nuotoliniu būdų prie tarnybinės stoties?

|  |  |  |  |
| --- | --- | --- | --- |
| IP adresas iš kur jungtasi | IP adresas į kur jungtasi | Priedas (port) | Paslauga (service) |
| 83.171.9.248 | 10.2.0.7 | 3389 |  |

1. Koks naudojamas atgrąžos apvalkalo IP adresas ir prievadas (angl.k. port)

|  |  |
| --- | --- |
| Atgrąžos apvalkalo IP adresas (angl. k. reverse) | Atgrąžos apvalkalo prievadas (angl.k. port) |
| 10.2.0.4 | 34894 |

**atgrąžos apvalkalo IP kas tai per velnias?**

1. Ką atlieka (paleidžia) programa? (Prašome surašyti komandas ir paaiškinti kokį veiksmą ji atlieka. Pakomentuoti kodėl šis veiksmas yra kenkėjiškas)

|  |  |  |
| --- | --- | --- |
| Programos tipas | Kenkėjiškos programos atliekamas veiksmas | Kenkėjiškos programos atliekami veiksmai |
| Linux shell | uname -a | Gaunama informaciją apie sistemą. Gavus sistemos duomenis galima spręsti apie sistemos pažeidžiamumus ir jais pasinaudoti. |
| w | Gaunama informacija apie prisijungusius vartotojus, bei paleistas programas. Žinant šiuos duomenis atsiranda galimybė galimybe valdyti naudotojus (keisti, ištrinti). Galima pasinaudoti esamomis atidarytomis aplikacijomis, jei jos turi saugumo spragų. |
| id | Gaunama informacija apie esamą naudotoją. Jei naudotojas yra administratorius, atsiranda galimybė vykdyti jo veiksmus. |
| /bin/sh -i | Atidaromas „shell“, kuriame galima vykdyti įvairias komandas. |

1. Kokia žinutė yra užkoduota \*.php faile?

|  |  |
| --- | --- |
| Failo pavadinimas | Žinutės tekstas |
| magic.php | //###{BASE16SUM2019}### |

1. Kokia gaunama reikšmė, ją atkodavus?

|  |  |
| --- | --- |
| Reikšmė užkoduota | Reikšmė atkoduota |
| //###{BASE16SUM2019}### | Sum of 2019 = 2+0+1+9 = 12  12 Base of 16 = 18 |

1. Informacija apie atakuotoją (ar galite nustatyti atakos pradžią?):

|  |  |  |
| --- | --- | --- |
| MAC (tinklo adresas) | Data | Laikas |
| fa:16:3e:29:17:b5 | Wed, 13 Feb 2019 | 06:29:54 GMT |