KAUNO TECHNOLOGIJOS UNIVERSITETAS

KOMPIUTERIŲ KATEDRA

Saugumo patikros ir etiško įsilaužimo technologijos

T120M154

Laboratoriniai darbai

NR. 3

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**

**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/>

**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. | 21/tcp open ftp | ftp | vsftpd 2.0.5 | CVE-2007-5962 |  |
| 2. | 22/tcp open ssh | ssh | OpenSSH 4.3 (protocol 1.99) | openSSH versions 4.3p1 and below CRC compensation attack detection remote denial of service exploit. CVE-2006-5051 | Gali būti naudojama atspėti prisijungimus pastoviai naudojant kitą prisijungimo informaciją |
| 3. | 111/tcp open rpcbind | rpcbind | 2 (RPC #100000) |  |  |

Service Info: Host: Welcome

**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. | 22/tcp open ssh | ssh | OpenSSH 4.3 (protocol 2.0) | CVE-2006-5051 | Gali būti naudojama atspėti prisijungimus pastoviai naudojant kitą prisijungimo informaciją |
| 2. | 111/tcp open rpcbind | rpcbind | 2 (RPC #100000) |  |  |
| 3. | 8080/tcp open http-proxy | shell | ROOT SHELL (\*\*BACKDOOR\*\*) | Galima prisijunti naudojant telenet komandą IP adresą ir atidarytą prievadą |  |

Service Info: OS: Unix

**III SISTEMA**

**IP (10.10.3.2) ADRESAS**

3 lentelė

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Eil. Nr.** | **Prievadas**  **(port)** | **Paslauga**  **(service)** | **Versija** | **Pažeidžiamumas**  **(CVE, EDB-ID, EDB)** | **Pastabos**  **(pvz. domain vardas, antraštės „banner“ informacija, kita.** |
| 1. | 135/tcp open msrpc | msrpc | Microsoft Windows RPC88 |  |  |
| 2. | 139/tcp open netbios-ssn | netbios-ssn | Microsoft Windows netbios-ssn |  |  |
| 3. | 445/tcp open microsoft-ds | netbios-ssn | Microsoft Windows XP microsoft-ds | MS08-067 |  |
| 4. | 3389/tcp open ms-wbt-server | ms-wbt-server | Microsoft Terminal Service | MS12-020 |  |

Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows\_xp

**IV SISTEMA**

**IP (10.10.4.5) ADRESAS**

4 lentelė

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Eil. Nr.** | **Prievadas**  **(port)** | **Paslauga**  **(service)** | **Versija** | **Pažeidžiamumas**  **(CVE, EDB-ID, EDB)** | **Pastabos**  **(pvz. domain vardas, antraštės „banner“ informacija, kita.** |
| 1. | 7/tcp open echo | echo |  | CVE-1999-0635  nc -uvn <IP> 7  galima atlikti DOS ataką |  |
| 2. | 9/tcp open discard | discard |  | CVE-1999-0636 |  |
| 3. | 13/tcp open daytime | daytime | Microsoft Windows USA daytime | CVE-1999-0638 |  |
| 4. | 17/tcp open qotd | qotd | Windows qotd (English) | Quote of the Day Traffic Amplification DOS or DDOS |  |
| 5. | 19/tcp open chargen | chargen |  | CVE-1999-0103 |  |
| 6. | 80/tcp open http | http | Microsoft IIS httpd 7.0 | CVE-2009-2521 |  |
| 7. | 88/tcp open kerberos-sec | kerberos-sec | Microsoft Windows Kerberos (server time: 2022-05-07 17:54:16Z) | MS11-013 |  |
| 8. | 135/tcp open msrpc | msrpc | Microsoft Windows RPC |  |  |
| 9. | 139/tcp open netbios-ssn | netbios-ssn | Microsoft Windows netbios-ssn |  |  |
| 10. | 389/tcp open ldap | ldap | Microsoft Windows Active Directory LDAP (Domain: svc-master.nksp.lt, Site: Default-First-Site-Name) | CVE-2013-1282 |  |
| 11. | 445/tcp open microsoft-ds | microsoft-ds | Microsoft Windows 2003 or 2008 microsoft-ds | MS08-067 – netinka blt |  |
| 12. | 464/tcp open kpasswd5 | kpasswd5 |  |  |  |
| 13. | 593/tcp open http-rpc-epmap | ncacn\_http | Microsoft Windows RPC over HTTP 1.0 | MS03-026 – netinka blt |  |
| 14. | 636/tcp open ldapssl | tcpwrapped |  | CVE-2011-2014 |  |
| 15. | 2522/tcp open windb | windb |  |  |  |
| 16. | 3268/tcp open globalcatLDAP | globalcatLDAP | Microsoft Windows Active Directory LDAP (Domain: svc-master.nksp.lt, Site: Default-First-Site-Name) |  |  |
| 17. | 3269/tcp open globalcatLDAPssl | globalcatLDAPssl - tcpwrapped |  |  |  |
| 18. | 3389/tcp open ms-wbt-server | ms-wbt-server | Microsoft Terminal Service | CVE-2019-0708 |  |
| 19. | 5357/tcp open wsdapi | wsdapi | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) | MS15-034 – ne lygtais |  |
| 20. | 8500/tcp open fmtp | fmtp |  | Wget komanda parsisiųsti internetinį puslapį kuris naudoja – „Coldfusion V9,0,2,282541“ |  |
| 21. | 20000/tcp open dnp | dnp |  | Dos? |  |
| 22. | 49152/tcp open unknown | msrpc | Microsoft Windows RPC |  | default dynamic port |
| 23. | 49153/tcp open unknown | msrpc | Microsoft Windows RPC |  | default dynamic port |
| 24. | 49154/tcp open unknown | msrpc | Microsoft Windows RPC |  | default dynamic port |
| 25. | 49155/tcp open unknown | msrpc | Microsoft Windows RPC |  | default dynamic port |
| 26. | 49157/tcp open unknown | ncacn\_http | Microsoft Windows RPC over HTTP 1.0 |  | default dynamic port |
| 27. | 49158/tcp open unknown | msrpc | Microsoft Windows RPC |  | default dynamic port |

Service Info: Host: SVC-MASTER; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o: Windows 2008 Standard SP2

**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** | 2007 | CVE-2007-5962 | Atnaujinti vsftpd programinę įrangą |
| 2006 | CVE-2006-5051 | Atnaujinti SSH programinę įrangą |
| **II sistema** | 2006 | CVE-2006-5051 | Atnaujinti SSH programinę įrangą |
|  | ROOT SHELL (\*\*BACKDOOR\*\*) | Jeigu ROOT SHELL yra reikalingas, tada atakas galima tik sumažinti, leidžiant prieiti prie prievado tik specifiniams IP adresams |
| **III sistema** | 2008 | MS08-067 | Atnaujinti Operacinę sistemą |
|  | 2012 | MS12-020 | Pritaikyti saugumo atnaujinimą |
| **IV sistema** | 1999 | CVE-1999-0635 | Išjungti paslaugą |
|  | 1999 | CVE-1999-0636 | Išjungti paslaugą |
|  | 1999 | CVE-1999-0638 | Išjungti paslaugą |
|  | 1999 | CVE-1999-0103 | Išjungti paslaugą |
|  |  | Quote of the Day Traffic Amplification DOS or DDOS | Išjungti paslaugą arba leisti naudotis tik specifiniams IP adresams |
|  |  | MS11-013 | Atnaujinti Operacinę sistemą |
|  | 2013 | CVE-2013-1282 | Atnaujinti operacinę sistemą |
|  | 2011 | CVE-2011-2014 | Atnaujinti operacinę sistemą |
|  |  | connect without credentials | DOS. Atnaujinti įrangą |
|  | 2019 | CVE-2019-0708 | Išjungti nuotolinio darbalaukio paslaugas, jeigu jos nenaudojamos. |
|  | 2015 | MS15-034 | Atnaujinti operacinę sistemą arba Išjungti IIS branduolio „caching“ |
|  |  | coldfusion V9,0,2,282541 | Atnaujinti naudojama įrangą |
|  |  | dnp DOS | Atnaujinti naudojamą įrangą |

**TINKLO TOPOLOGINĖ SCHEMA**

|  |  |  |
| --- | --- | --- |
| **Nr.** | **IP Adresas** | **Tarpiniai mazgai** |
| **1.** | **10.10.1.2** | 1 10.10.1.2 (10.10.1.2) 0.350 ms 0.269 ms 0.241 ms |
| **2.** | **10.10.1.4** | 1 10.10.1.4 (10.10.1.4) 0.308 ms 0.289 ms 0.288 ms3 |
| **3.** | 10.10.3.2 | 1 \* \* \*  2 \* \* \*  3 \* \* \*  4 \* \* \*  5 \* \* \*  6 10.10.3.2 (10.10.3.2) 0.804 ms 0.178 ms 0.177 ms |
| **4.** | 10.10.4.5 | traceroute to 10.10.4.5 (10.10.4.5), 30 hops max, 60 byte packets  1 \* \* \*  2 \* \* \*  3 \* \* \*  4 \* \* \*  5 \* \* \* |

**Diagram

Description automatically generated**

**IŠVADA**

Pagrindiniai analizei buvo naudojama „nmap“ komanda:

nmap -sC -sV --script vuln -oA nmap 10.10.1.2

nmap -sC -sV --script vuln -oA nmap 10.10.1.4

nmap -sC -sV --script vuln -oA nmap 10.10.3.2

nmap -sC -sV --script vuln -oA nmap 10.10.4.5

Tada panaudojus ir išsiaiškinus atidarytus prievadus, jie buvo surašyti į lentelę ir tada buvo bandoma ieškoti pažeidžiamumų. Dalis pažeidžiamumų buvo pateikti „nmap“ komandos naudojimo metu. Kiti pažeidžiamumai buvo ieškoti internete. Pradarius laboratorinį darbą buvo išsiaiškinta, kad naudojant komandas neišėjo surasti visų pažeidžiamumų. Interneto pagalba buvo surasta daug daugiau pažeidžiamumų. „traceroute“ komandos pagalba buvo sudarytas tinklo topologinė schema.