1. Paveikslėlis, kuriame yra juodas, tamsa

   Automatiškai sugeneruotas aprašymas
2. **Kauno technologijos universitetas**
3. Informatikos fakultetas
4. **T120B181 Kompiuterių tinklų ir interneto sauga**
5. **Laboratorinis darbas Nr.3.**

|  |  |
| --- | --- |
|  |  |
| **Nedas Liaudanskis IFF-1/9**  Studentas | (parašas) (data) |
|  |  |
| **dėst. Rimkus Dangis**  Dėstytojas | (parašas) (data) |
|  |  |

**1. Darbo eiga.**

1. ***OpenVPN serverio įdiegimas ir konfigūravimas***
   1. Į sistemą įdiegiamas openvpn paketas:

*apt-get install openvpn*

* 1. Sukuriamas katalogas raktams, visi pakeitimai laboratorinio darbo metu bus atliekami šiame kataloge

*mkdir /root/secret*

* 1. Nukopijuojami raktų kūrimo įrankiai į sukurtą katalogą ir pakeičiamas darbinis katalogas

*cp -R /usr/share/doc/openvpn/examples/easy-rsa/2.0/\* /root/secret/*

*cd /root/secret/*

* 1. Prieš pradedant raktų ir sertifikatų generavimą, reikia nustatyti pradinius sertifikatų parametrus. Šie parametrai saugomi *vars* faile. Failo redagavimui naudosime *nano* programą nano vars.

Numatytąjį rakto dydį 1024 pakeiskite į 2048, ilgesnis raktas suteikia didesnį saugumą, tačiau nuo rakto ilgio priklauso Diffie-Hellman parametrų generavimo laikas, bei TLS sujungimo laikas. KEY\_SIZE turi būti suderintas abiejuose ryšio užmezgime dalyvaujančiuose kompiuteriuose.

*export KEY\_SIZE=2048*

*export KEY\_COUNTRY="LT"*

*export KEY\_PROVINCE=""*

*export KEY\_CITY="Kaunas"*

*export KEY\_ORG="KTU"*

*export KEY\_EMAIL=*[*vardas.pavarde@stud.ktu.lt*](mailto:vardas.pavarde@stud.ktu.lt)

* 1. Nuskaitomi raktų ir sertifikatų parametrai

*source ./vars*

* 1. Išvalomas katalogas

*./clean-all*

* 1. Generuojami Diffie-Hellman parametrai, kadangi rakto dydis buvo padidintas iki 2048 bitų, todėl šių parametrų generavimas gali užtrukti keletą minučių, turėkite kantrybės ir palaukite kol bus baigtas parametrų generavimas.

*./build-dh*

* 1. Sukuriamas CA (certificate authority) sertifikatas. Serverio CA sertifikatas saugomas CA.crt faile.

*./pkitool --initca KEY\_SIZE*

* 1. Sugeneruojamas serverio sertifikatas. Serverio sertifikatas saugomas K[nr].crt o raktas K[nr].key faile.

*./pkitool --server K[nr]*

* 1. Sugeneruojamas statinis raktas. Statinis raktas saugomas ta.key faile.

*openvpn --genkey --secret keys/ta.key*

* 1. Sukuriame katalogą konfigūracijai ir raktams

*mkdir /root/openvpn*

* 1. Nukopijuojame CA sertifikatą, serverio sertifikatą, serverio raktą, statinį raktą, ir sugeneruotus pirminius skaičius

*cd keys*

*cp ca.crt K[nr].crt K[nr].key ta\_K[nr].key dh2048.pem /root/openvpn*

* 1. Į savo katalogą nukopijuojame standartinį serverio konfigūracinį failą

*cd /root/openvpn*

*zcat /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz > server.conf*

* 1. Atliekame konfigūracijos pakeitimus. OpenVPN serverio konfigūracija saugoma server.conf faile. Failo redagavimui naudojama nano programa *nano server.conf*

Konfigūraciniame faile aktyvūs parametrai eilutės pradžioje neturi kabliataškio (`;`). Nereikalingi parametrai išjungiami eilutės pradžioje parašius kabliataškį.

Konfigūraciniame faile atliekami tokie pakeitimai:

*dev tap0* # Bus naudojamas L2 VPN

*;dev tun* # Išjungiamas L3 VPN parametras

*ca /root/openvpn/ca.crt* # Nurodomas CA sertifikatas

*cert /root/openvpn/K[nr].crt* # Nurodomas serverio sertifikatas

*key /root/openvpn/K[nr].key* # Nurodomas serverio sertifikatas

*dh /root/openvpn/dh2048.pem* # Nurodomas DH parametrų failas

*;server 10.8.0.0 255.255.255.0* # Išjungiami L3 VPN nustatymai

*ifconfig-pool-persist /root/openvpn/ipp.txt* # Nurodome IP adresų DB

*server-bridge 172.16.K[nr].254 255.255.255.0 172.16.K[nr].1 172.16.K[nr].128* # Serverio IP, serverio netmask, klientų IP pradinis, klientų IP paskutinis

*tls-auth /root/openvpn/ta\_K[nr].key 0*

* 1. Sukuriamas virtualaus tinklo interfeisas

*openvpn --mktun --dev tap0*

* 1. Sukonfigūruojamas serverio virtualaus interfeiso IP adresas

*ip link set tap0 up*

*ip addr add 172.16.K[nr].254/24 bro + dev tap0*

* 1. Paleidžiame OpenVPN serverį, parametruose nurodant kelią iki serverio konfigūracinio failo

*openvpn --config /root/openvpn/server.conf*

1. Pasirašykite sertifikatą (**nurodant pasirašomą sertifikatą, failo pavadinimą nurodykite be plėtinio \*.csr**)

*./sign-req K[?]\_client*

***3. Tinklo adresų priskyrimas***

Kuriant naują VPN tinklą dažniausiai yra apjungiami keli privatūs kompiuterių tinklai, esantys skirtingose vietovėse. IANA (The Internet Assigned Numbers Authority) yra rezervavusi tris IP adresų ruožus skirtus privačių tinklų adresavimui (RFC 1918).

|  |  |  |
| --- | --- | --- |
| 10.0.0.0 | 10.255.255.255 | 10.0.0.0/8 |
| 172.16.0.0 | 172.16.255.255 | 172.16.0.0/12 |
| 192.168.0.0 | 192.168.255.255 | 192.168.0.0/16 |

Nors šie adresai ir gali būti naudojami VPN adresavimui, tačiau yra svarbu pasirinkti tokius IP adresus, kad būtų kiek galima labiau sumažinama IP adresų potinklių konfliktų tikimybė. Yra du pagrindiniai IP adresų potinklių konfliktai, kurių reikėtų stengtis išvengti:

* + Vienodų potinklių naudojimas VPN ir LAN tinklo numeracijai.
  + Nutolusios prieigos sričių apjungimas, kuriose naudojami tų pačių potinklių IP adresai.

Pavyzdžiui, jūs savo VPN tinkle naudojate dažnai sutinkamą 192.168.0.0/24 potinklį. Jūs esate internetinėje kavinėje ir bandote prisijungti prie VPN, naudojantis internetinės kavinės WiFi ryšiu, kuriame naudojamas tas pats 192.168.0.0/24 potinklis. Tokiu atveju įvyks maršrutų parinkimo konfliktas, nes kompiuteris nebežinos ar 192.168.0.1 veikiantis kaip šliuzas (gateway) priklauso WiFi tinklo ar VPN tinklui.

Adresų konflikto galima išvengti nenaudojant populiariausių 10.0.0.0/24 ir 192.168.0.0/24 potinklių VPN potinklių adresavimui. VPN IP adresavimui geriausia naudoti potinklius, kurie turi gerokai mažesnę tikimybę, kad kavinėse, oro uostuose, viešbučiuose ir kt. bus naudojami belaidžio interneto prieigos. Geriausia yra pasirinkti IP adresų sritis, esančius viduryje galimų IP adresų ruožų.

Pabaigoje adresų parinkimą patikrinti su PING komanda tarp serverio-kliento ir kliento serverio.

Padarytos VPN ir kliento konfigūracijos, testavimas naudojant PING komandą:























