**3. laboratorinis darbas Linux tarpsegmentinio ekrano tyrimas**

**Darbo tikslas:** patikrinti tinklo nustatymus, susipažinti su iptables sintakse, nustatyti paprastą tarpsegmentinį ekraną.

**Darbo eiga:**

1. Patikrinkite nustatytą virtualaus kompiuterio konfigūraciją: IP adresus *ifconfig -a*, turėtų būti eth0 192.168.10.1X/24 ir eth0:1 10.10.10.X/24; maršrutizacijos lentelę route –n, turėtų būti tik vartai pagal nutylėjimą Gateway 192.168.10.254. Jei nustatymai ne tokie pataisykite juos faile /etc/network/interfaces. Aktyvuokite pakeistus nustatymus: *ifup eth0* , *ifup eth0:1*.

2. Įdiekite grafinę paslaugų įjungimo / išjungimo priemonę: *apt-get install sysvconfig*, susipažinkite su jos veikimu: *sysvconfig*, naudodami Enable/Disable galite įjungti ar išjungti paslaugos automatinį paleidimą, nieko nekeiskite. Įdiekite saugaus nuotolinio pasiekimo paslaugą: *apt-get install ssh*.

3. Patikrinkite teikiamas tinklo paslaugas: *netstat –an*. Pabandykite prisijungti prie kaimyno per ssh: *ssh 192.168.10.(1X-1)*, pastebėkite kaip pasikeitė paslaugų būvis: *netstat –an*.

4. Skenuokite kaimyno virtualų kompiuterį ir užsirašykite gautus rezultatus: *nmap –sS –P0 –n –F 192.168.10.(1X-1).* S reiškia, kad skanavimo tipas SYN Stealth, P0 – patikrinti ar įjungtas į mazgą nebus siunčiamas ping paketas, -n – nespręsti vardų, -F greitas skenavimas.

5. Įjunkite IP paketų persiuntimą faile /etc/sysctl.conf padarydami įrašą net/ipv4/ip\_forward = 1 . Peržiūrėkite užkrautus modulius *lsmod*. Nustatykite automatinį iptable\_nat ir ip\_conntrack užkrovimą įrašydami šių modulių pavadinimus į /etc/modules. Šios vertės atsiras tik perkrovus virtualų kompiuterį, neperkraudami nustatysime šias vertes: *echo „1“ > /proc/sys/net/ipv4/ip\_forward* ir *modprobe iptable\_nat*. Patikrinkime ar nustatymas įvyko: *cat /proc/sys/net/ipv4/ip\_forward* ir *lsmod.*

6. Pažiūrėkite iptables nustatymus pagal nutylėjimą: *iptables --list* arba *iptables –L*. Uždrauskite visus įeinančius paketus: *iptables –A INPUT –j DROP*, išbandykite ar veikia ir pažiūrėkite kaip pasikeitė iptables nustatymai: *iptables –L*. Išvalykite iptables: *iptables –F*. Patikrinkite ar išsivalė. Uždrauskite ICMP protokolą: iptables –A INPUT –p icmp –j DROP, patikrinkite ar atsirado taisyklė ir ar ji veikia. Išvalykite iptables.

7. Apsaugokite virtualų kompiuterį nuo resursus išnaudojančio ping srauto. Paleiskite ping srautą į virtualų kompiuterį, stebėkite kaip vykdoma komanda, sustabdykite jį *Ctrl+C*. Nustatykite ribojimą, kad vienas šaltinis galėtų atsiųsti vieną ping paketą per sekundę: *iptables -A INPUT –p icmp –m limit --limit 1/s --limit-burst 1 –j ACCEPT.* Vėl paleiskite ping srautą ir įvertinkite kaip pasikeitė elgsena. Išvalykite iptables: *iptables –F*.

8. Registruokite žurnale telnet užklausas ir jų neleiskite: *iptables –A INPUT –d 192.168.10.1X –p tcp --dport 23 –j LOG --log-prefix ‘TELNET ATTEMPT: ‘* . Kreipkitės iš realaus ir kaimyno kompiuterių į savo virtualų kompiuterį telnet protokolu: *telnet 192.168.10.1X*. Peržiūrėkite įrašus žurnale *less /var/log/messages*.

9. Įrašykite taisykles į automatinio užsikrovimo scenarijų, skurkite direktoriją ir konfigūracijos failą: *mkdir /etc/iptables*, sukonfigūruokite iptables: išvalykite buvusius nustatymus *iptables –F* ; nustatykite taisykles pagal nutylėjimą *iptables -P INPUT DROP ; iptables -P FORWARD DROP ; iptables -P OUTPUT ACCEPT ;* leiskite reikiamų paslaugų pasiekimą *iptables -A INPUT -s 0/0 -d 192.168.10.1X -p tcp --dport 22 -j ACCEPT ; iptables -A INPUT -s 0/0 -d 192.168.10.1X -p tcp --dport 443 -j ACCEPT*. Patikrinkite konfigūraciją: *iptables –L*. Konfigūraciją įrašykite į failą*: /sbin/iptables-save > /etc/iptables/iptables.conf*. Sukurkite failą myfirewall su tokiu turiniu:

#! /bin/sh

case "$1" in

start)

echo "Starting firewall (iptables)."

/sbin/iptables-restore</etc/iptables/iptables.conf

 ;;

stop)

echo "Stopping firewall (flushing rules)"

/sbin/iptables –F

/sbin/modprobe –r iptable\_filter

 ;;

show)

echo "Current firewall rules:"

/sbin/iptables-save

 ;;

\*)

echo "Usage: /etc/init.d/myfirewall {start|stop|show}"

exit 1

 ;;

esac

exit 0

Nukopijuokite jį į paleidimo sritį: *cp myfirewall /etc/init.d/,* suteikite vykdymo teises: *chmod 755 /etc/init.d/myfirewall*.

Panagrinėkite kaip veikia myfirewall scenarijus, užkraukite taisykles, patikrinkite ar užsikrovė ir veikia reikiamos taisyklės. Perkraukite virtualų kompiuterį ir patikrinkite ar taisyklės užsikrovė bei veikia. Esant veikimo problemų naudokite komandą *tcpdump* tinklo srauto stebėjimui.

10. Skenuokite apsaugotą kaimyno virtualų kompiuterį: *nmap –sS –P0 –n –F –max\_rtt\_timeout 6 192.168.10.(1X-1),* palyginkite gautus rezultatus su gautais darbo pradžioje.

**Ataskaitos turinys:**

1. Darbo tikslas,
2. Trumpas atlikto darbo aptarimas,
3. Aprašykite duodas iptables komandą ir tikslą.
4. Iptables tarpsegmentinio ekrano scenarijaus analizė (darbas grupėje):

a) http://networking.ringofsaturn.com/Unix/iptables.php

b) http://danieldegraaf.afraid.org/info/iptables/complex

c) http://www.homepage.montana.edu/~unixuser/031705/iptables.fedora.html