Duomenų apsaugos LD

1. Susikonfigūruoti tinkle Virtual Box.
2. Susikonfigūruoti tinkle Ubuntu: *nano* */etc/network/interfaces*
3. Nustatykite kompiuterio vardą komanda *hostname kompiuterio\_vardas,* toks nustatymas perkrovus kompiuterį neišliks, todėl kompiuterio vardą įrašykite į failą */etc/hostname*, patikrinkite ar vardas pasikeitė*: hostname.*
4. Patikrinkite vardų išspendimo tarnybines stotis: cat */etc/resolv.conf*.
5. Aprašykite reikalingas vidaus vardų sąsajas su IP adresais.
6. */etc/hosts* faile galima statiškai užduoti tinklo mazgų vardus, papildykite šį failą kaimyninio kompiuterio IP adresu su vardu kaimynas:
7. *192.168.10.****(1X-1)***  *kaimynas*
   1. Išbandykite ar išsprendžia nustatytą vardą *ping kaimynas* .
   2. Skenuokite kaimyninį kompiuterį ***nmap -sS -O 192.168.10.(1X-1)* Išsiaiškinkite ką reiškia gautas atsakymas.**
   3. **Peržiūrėkite kompiuteryje vykstančius procesus *ps –aux*. Kokios komandos ps galimybės: *man ps*. Peržiūrėkite tik žiniatinklio procesą *ps –aux | grep apache*. Pažiūrėkite kokie procesai daugiausia naudoja kompiuterio resursus *top*, iš atsidarosio lango išeikite naudodami *q*. Išsiaiškinkite ką rodo top komanda: *man top*.**
8. 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*.
9. 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.
10. 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*. Jei neveikia googlinkite.
11. 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*.
12. Konfigūraciją įrašykite į failą*: /sbin/iptables-save > /etc/iptables/iptables.conf*. Perkraukite virtualų kompiuterį, ukraukite iptables nustatymus.
13. Skenuokite apsaugotą kaimyno virtualų kompiuterį: *nmap –sS –P0 –n –F –max\_rtt\_timeout 6 192.168.10.(1X-1),* palyginkite gautus rezultatus su gautais pradžioje.
14. Snort tinklo stebėjimo režime stebimos tinklu keliaujančių paketų antraštės arba visi paketai. Stebėkite tinklo srautą ir įrašykite duomenis į failus: *cd /root*, *snort –v > snort1*, stebėjimą sustabdykite *Ctrl+C*, vėl stebėkite: *snort –vde > snort2,* stebėjimą sustabdykite *Ctrl+C*. Analizuokite stebėjimo failus.
15. Snort tinklo paketų rinkimo režimas leidžia rinkti tinklo paketus ir saugoti juos dvejetainiuose failuose tolesnei analizei. Startuokite snort paketų rinkimo režime: *snort –dev –l /var/log/snort*. Gaukite ping užklausas iš kaimyno kompiuterio. Sustabdykite paketų rinkimą *Ctrl+C*. Gautą informaciją galima nuskaityti įvairiais tinklo stebėjimo įrankiais, nuskaitykite informaciją apie sustebėtus ICMP paketus: *snort –dvr /var/log/snort/snort.log.xxxxxx icmp*. Peržiūrėti informaciją esančią ekreno viršuje galima: *Shift+PgUP* , *Shift+PgDOWN*.
16. Atakų atpažinimo režimas yra pagrindinis ir turintis daugiausia galimybių, snort konfigūracija saugoma snort.conf faile, susipažinkite su jo struktūra: *nano /etc/snort/snort.conf*, atkreipkite dėmesį į globalius kintamuosius, naudojamus preprocesorius, išvedimo įskiepius ir naudojamas taisykles. Redaguokite konfigūracinį failą: *nano /etc/snort/snort.conf*, jame įrašykite parametrus:

var RULE\_PATH /etc/snort/rules

var HOME\_NET 192.168.10.0/24

var EXTERNAL\_NET !$HOME\_NET

1. Naudodami simbolį # užkomentuokite visas taisykles išskyrus local.rules. Patikrinkite ar užkomentuotas išvedimas į duomenų bazę: output database: log, mysql.
2. Sukurkite direktoriją: *mkdir /etc/snort/rules*. Parašykite paprastą taisyklę pranešančią apie ICMP paketus: *nano /etc/snort/rules/local.rules*, įrašykite: alert icmp any any -> 192.168.10.1X any (msg:"ICMP test“; sid:10000001;)
3. Startuokite snort paslaugą */usr/local/bin/snort -u snort -g snort -c /etc/snort/snort.conf*. Gaukite ping užklausas iš kaimyno kompiuterio, sustabdykite stebėjimą *Ctrl+C*, stebėkite ar jos buvo atpažintos *cat /var/log/snort/alert*.
4. Instaliuokite telnet serverį: *apt-get install telnetd*. Parašykite taisyklę atpažįstančią telnet prisijungimą su vartotoju root: *nano /etc/snort/rules/local.rules*, įrašykite: alert tcp any any -> 192.168.10.X 23 (content:“root“; nocase; msg:“Suspicious Telnet“; sid:10000002;).
5. Junkitės telnet protokolu prie kaimyno kompiuterio: *telnet 192.168.10.(1X-1)*, bandykite įvesti vartotojo vardą *root* ir jei reikės betkokį slaptažodį. Analizuokite įrašus.
6. Paleiskite Open VPN tunelį tarp dviejų kompiuterių.

Lyginis varianto numeris – serveris, nelyginis – klientas. Serveris direktorijoje /etc/openvpn naudodamas komandą: *openvpn --genkey --secret static.key* sukuria rakto failą static.key ir naudodamas *scp* saugiai per duoda jį klientui. Peržiūrėkite rakto failą.

Sukurkite tunelio sąsajos konfigūracijos failą /etc/openvpn/tun0.conf .

Serveryje šis failas turi būti toks:

dev tun0

ifconfig 10.0.0.X 10.0.0.(X-1)

secret static.key

Kliente šis failas turi būti toks:

remote *192.168.10.1X*

dev tun0

ifconfig 10.0.0.(X-1) 10.0.0.X

secret static.key

Serveryje turi būti atidarytas prievadas UDP 1194, kliente tarpsegmentinis ekranas turi nedrausti komunikacijos su sVPN serveriu.

Paleiskite Openvpn paketą: *openvpn --config /etc/openvpn/tun0.conf* . Ši komanda turi būti įvykdyta tiek serveryje, tiek kliente.

Įsijunkite kitą konsolę Alt+F2. Patikrinkite, naująją tinklo sąsają *ifconfig –a*.

Siųskite ping užklausas į kito ryšio dalyvio tunelio sąsają.

Patikrinkite ryšį naudodami netstat komandą.

Pridėkite maršrutą į kito ryšio dalyvio tinklą 10.(X-1).0.(X-1)/24 : *route add -net 10.(X-1).0.(X-1) netmask 255.255.255.0 gw 10.0.0.X*

1. Bandykite jį pasiekti naudodami ping komandą.
2. Bandykite stebėti tinkle srautą tarp dviejų virtualiu tuneliu atskirtų tinklų naudodami tcpdump komandą.