Ονοματεπώνυμο : Ιωάννης Μπασδέκης
Ομάδα: 3
‘Ονομα PC: DESKTOP-0BU537U
Ημερομηνία: 23/4/2023

Μέρος 1ο

1.1) kldload ipfw

1.2) kldstat

1.3) Όχι
sendto: permission denied

1.4) ipfw list

1.5) ipfw show

1.6) ipfw zero

1.7) ipfw add 100 allow all from any to any via lo0

1.8) Ναι

1.9) Όχι
sendto: permission denied

1.10) ipfw add allow icmp from any to any

1.11) 1100

1.12) Ναι και στις δύο κατευθύνσεις

1.13) Στην υλοποίηση του traceroute στο FreeBSD χρησιμοποιούνται UDP πακέτα όχι icmp
Πρέπει να βάλουμε την παράμετρο -I

1.14) ipfw add allow udp from me to any

1.15) Όχι

1.16) ipfw add 200 allow tcp from any to any established
ipfw add 210 allow tcp from me to any setup

1.17) ipfw zero
ssh lab@192.168.1.3
ls
exit

1.18) ipfw add 210 allow tcp from me to any setup = 1 (Για το πακέτο με σημαία SYN χωρίς ACK της τριπλής χειραψίας)
ipfw add 200 allow tcp from any to any established = 76
Για τα πακέτα tcp που είναι μέρος κάποιας σύνδεσης

1.19) Όχι γιατί στον κανόνα για το setup έχουμε βάλει from me οπότε δεν δεχόμαστε συνδέσεις tcp μόνο αν τις αρχίσουμε εμείς

1.20) Ναι ftp lab@192.168.1.3

Μέρος 2ο

2.1) kldload ipfw

2.2) Όχι

2.3) ipfw add allow from any to any via lo0

2.4) ipfw add allow icmp from me to any icmptypes 8

2.5) Όχι

2.6) Μόνο τα ICMP request περνούν καθώς στον κανόνα του firewall του PC1 έχουμε τις διπλάσιες μετρήσεις από ότι στο PC2

2.7) ipfw delete 1100
ipfw add allow icmp from me to any icmptypes 8 keep-state
Ναι

2.8) Ναι

2.9) Όχι γιατί πλέον δεν υπάρχει ο δυναμικός κανόνας

2.10) ipfw add allow icmp from any to me icmptypes 8 keep-state

2.11) Έχει προστεθεί δυναμικός κανόνας

2.12) Διαγράφηκε ο κανόνας

2.13) ipfw add allow udp from any to me
ipfw add allow icmp from me to any icmptypes 3,11

2.14) ipfw add allow udp from me to any
ipfw add allow icmp from anyto meicmptypes 3,11

2.15) ipfw add allow icmp from me to any icmptypes 3,11

2.16) ipfw add allow tcp from 192.168.1.0/24 to me 22 keep-state

2.17) ssh@192.168.1.3
Συνδεθήκαμε

2.18) ipfw add allow tcp from me to any 22 keep-state

2.19) ipfw add allow tcp from 192.168.1.3 to me 22

2.20) Ναι

2.21) Όχι (λόγω διαφορετικής θύρας (ftp port = 21))
ipfw add allow tcp from 192.168.1.2 to me 21 keep-state

2.22) Η πρώτη εντολή είναι σε passive mode και χρησιμοποιείται η θύρα 20 για την επικοινωνία πελάτη - εξυπηρετητή. Ο κανόνας που θέσαμε μας καλύπτει για την θύρα 21

2.23) ipfw add allow tcp from 192.168.1.2 to me 20 keep-state

2.24) όχι

2.25) PC1 = ipfw add allow tcp from 192.168.1.3 20 to me
PC2 = ipfw add alow tcp from me 20 to 192.168.1.2

2.26) Χρειάζεται η χρήση firewalls στο ftp καθώς πρόκειται για απομακρυσμένη σύνδεση και δεν έχει κρυπτογράφηση

2.27) kldunload ipfw
kldstat

Μέρος 3ο

3.1) hostname {PC1,PC2}
route add default 192.168.1.1

3.2) cli
configure terminal
hostname R1
interface em0
ip address 192.0.2.2/30
exit
interface em1
ip address 192.0.2.6/30
exit

3.3) hostame SRV1
ifconfig em0 192.0.2.5/30
route add default 192.0.2.6

3.4) service ftpd start

3.5) kernel
ipfw
ipfw_nat
libalias

3.6) ipfw

3.7) sysrc firewall_tpye = UNKNOWN

3.8) 11
deny ip from any to any

3.9) ipfw nat show config

3.10) όχι

3.11) όχι

3.12) ipfw nat 123 config if em1 unreg_only reg

3.13) ipfw add 50 nat 123 ip from any to any

3.14) Ναι

3.15) tcpdump -vvv -i em0

3.16) ipfw show
ipfw zero

3.17) Η ip του FW1 στο WAN1

3.18) 192.0.2.1

3.19) allow ip from any to any

3.20) 12 (6 πακέτα και για κάθε πακέτο 2 φορές (reply, request))

3.21) Ναι

3.22) allow ip from any to any

3.23) Ναι καθώς είναι ιδιωτική διεύθυνση

3.24) Ναι

3.25) Ο R2 δεν γνωρίζει κάτι για το LAN1
Αυτό το διαπιστώσαμε απο το μήνυμα που λάβαμε = no route to host
Είναι δηλαδή πρόβλημα δρομολόγησης

3.26) ipfw nat 123 config if em1 unreg_only reset redirect_addr 192.168.1.3 192.0.2.1

3.27) Ναι
Με hostname

3.28) ipfw nat 123 if em1 unreg_only reset redirect_addr 192.168.1.3 192.0.2.1 redirect_port tcp 192.168.1.2:22 22

3.29) PC1
Με hostname

3.30) Στο PC2 καθώς στο PC1 κατευθύνεται κίνηση μόνο για την θύρα 22 (ssh)

3.31) Ναι

3.32) PC2

3.33) PC1

Μέρος 4ο

4.1) όχι

4.2) Ναι αλλά λόγω του φιλταρίσματος εξετάζονται όλοι οι κανόνες και εν τέλει απορρίπτεται από τον τελευταίο

4.3) ipfw delete 50
ipfw add 1100 allow all from any to any via em0

4.4) Ναι

4.5) FW1 αφού διαγράψαμε τον κανόνα προώθησης στον πίνακα NAT

4.6) Ο κανόνας του 4.3

4.7) ipfw add 3000 nat 123 ip from any to any xmit em1

4.8) ipfw add 3001 allow all from any to any

4.9) ipfw add 2000 nat 123 ip from any to any recv em1

4.10) ipfw add 2001 check-state

4.11) FW1

4.12) PC2

4.13) FW1

4.14) PC1

4.15) PC2

4.16) Ναι

4.17) Ναι

4.18) Ναι

4.19) ipfw add 2999 deny all from any to any via em1

4.20) Μόνο απο LAN1

4.21) ipfw add 2500 skipto 3000 icmp from any to any xmit em1 keep-state

4.22) Ναι

4.23) ipfw add 2500 skipto 3000 tcp from any to any 22 out via em1 keep-state

4.24) Ναι

4.25) ipfw add 2100 skipto 3000 icmp from any to any in via em1 keep-state

4.26) PC2

4.27) ipfw add 2200 skipto 3000 tcp from any to any 22 recv em1 keep-state

4.28) PC1

4.29) Όχι

4.30) ipfw add 2300 skipto 3000 tcp from any to any 21 setup recv em1 keep-state
ipfw add 2400 skipto 3000 tcp from any 20 to any setup out via em1 keep-state

Μέρος 5ο

5.1) 192.168.1.1

5.2) 10.0.0.1

5.3) 65%

5.4) 4 διεπαφές δικτύου

5.5) 172.22.1.1

5.6) fw.lab.ntua.gr

5.7) hostname = fw1
save

5.8) Όχι

5.9) -

5.10) Ναι

5.11) Όχι

5.12) -

5.13) -

5.14) dhclient em0
IP Address 192.168.1.2
Default Gateway 192.168.1.1
DNS Server 192.168.1.1

5.15) Για να φαίνεται ότι το m0n0wall είναι DNS server και όχι οι DNS servers που χρησιμοποιεί πραγματικά το m0n0wall

5.16) Diagnostics -> DHCP Leases

5.17) 7

5.18) Όχι

5.19) Τα πακέτα που φιλτράρονται

5.20) 1

5.21) Κανένα

5.22) -

5.23) Ναι

5.24) Όχι

5.25) Ναι

5.26) -

5.27) Ναι

5.28) Όχι ο R1 δεν ξέρει για το 192.168.1.0/24

5.29) Ναι γιατί γίνεται μετάφραση των ιδιωτικών διευθύνσεων με την διεύθυνση του FW1 στο WAN1

5.30) SRV1: ifconfig em0 172.22.1.2/24
Δεν μπορούμε γιατί δεν έχουμε ορίσει default gateway

5.31) route add 0.0.0.0/0 172.22.1.1

5.32) Ναι

5.33) Όχι γιατί δεν έχουμε ορίζει κάποιον κανόνα στο firewall

5.34) Όχι γιατί δεν μπορούμε να στείλουμε πακέτο από την διεπαφη στο DMZ

5.35) -

5.36) Ναι

5.37) Ναι

5.38) Όχι
no route to host

5.39) Ναι γιατί έχουν οριστεί default gateways στο SRV1 και στο FW1

5.40) dhclient em0
IP Address 192.168.1.3
Default Gateway 192.168.1.1
DNS Server 192.168.1.1

5.41) -

5.42) Πρέπει να το τοποθετήσουμε πάνω πάνω

5.43) Όχι

5.44) Ναι δεν υπάρχει κανόνας που να το απαγορεύει

Μέρος 6ο

6.1) route add 203.0.118.0/24 192.0.2.1

6.2) -

6.3) -

6.4) -

6.5) tcpdump -vvv -i em0

6.6) Ναι
PC1 = 203.0.118.14
PC2 = 203.0.118.15

6.7) Η μετάφραση NAT είναι μόνο outbound οπότε δεν λειτουργεί

6.8) -

6.9) -

6.10) TCP * * 172.22.1.2 22 NAT με την επιλογή ‘Auto-add a firewall rule to permit trafic’

6.11) SRV1

6.12) Όχι γιατί ο κανόνας είναι μόνο για την πόρτα 22 (SSH)

6.13) Ναι μέσω R1
tcpdump

6.14) Όχι γιατί στο firewall υπάρχει κανόνας που μπλοκάρει τις ιδιωτικές διευθύνσεις

6.15) Ναι

6.16) Ναι αλλά δεν μπορώ στα PC1, PC2

6.17) Δεν υπάρχει εσωτερική μετάφραση οπότε ο FW1 δεν προωθεί τα μηνύματα που στέλνει το SRV1 πίσω στο PC2

6.18) Ο κανόνας για DMZ

Μέρος 7ο

7.1) -

7.2) -

7.3) -

7.4) Ναι

7.5) -

7.6) -

7.7) -

7.8) -

7.9) -

7.10) -

7.11) ifconfig em0 192.168.2.2/24
route add 0.0.0.0/0 192.168.2.1

7.12) Ναι

7.13) Ναι

7.14) Όχι αφού ο R1 δεν γνωρίζει το LAN2

7.15) -

7.16) * * * * * Default IPsec VPN

7.17) Όχι

7.18) Ναι

7.19) -

7.20) Όχι

7.21) Ναι

7.22) Ναι

7.23) Ναι

7.24) Προστέθηκαν 2 εγγραφές

7.25) Προστέθηκαν 2 εγγραφές

7.26) tcpdump -vvv -i em0

7.27) Όχι

7.28) ESP πακέτα
Source = 192.0.2.1
Dest = 192.0.2.5

7.29) Όχι

7.30) Ναι αφού το PC2 ανήκει στο LAN2 και δεν υπάρχει κάποιος κανόνας στο firewall να το μπλοκάρει

7.31) TCP
Source = 192.0.2.5
Dest = 203.0.118.18

7.32) Ναι