**ΕΡΓΑΣΤΗΡΙΟ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ**

**8ο ΕΞΑΜΗΝΟ ΣΗΜΜΥ**
**Εργαστηριακή Άσκηση 10**
**Τείχη προστασίας (Firewalls) και NAT**

Ιωάννης Αλεξόπουλος (03117001)
Όνομα PC/ΛΣ: thinkpad / Ubuntu 20.04.1
Ομάδα: 1

**Άσκηση 1: Ένα απλό τείχος προστασίας**

1. kldload ipfw
2. kldstat
3. Permission denied
4. ipfw list -> deny ip from any to any
5. ipfw -h , ipfw show (?)
6. ipfw zero
7. ipfw add 100 allow all from any to any via lo0
8. Ναι
9. Permission denied
10. ipfw add allow icmp from any to any via em0
11. 200
12. Ναι και από τις δύο κατευθύνσεις
13. Γιατί χρησιμοποιεί UDP πακέτα αντί για ICMP, με -I
14. ipfw allow udp from me to any 33435,33436,33437 via em0
15. Permission denied
16. ipfw add allow tcp from any to any established
    ipfw add allow tcp from me to any setup
17. ipfw zero -> ssh lab@192.168.1.3 -> ls -> exit
18. setup -> 1, established -> 69 (Μια φορά γίνεται η σύνδεση και σε 69 πακέτα ανταλλάσσεται η πληροφορία)
19. Όχι, γιατί για setup έχουμε διεύθυνση προέλευσης me (διεπαφή που έχει ορισθεί σε κάποια διεπαφή του συστήματος)
20. service ftpd onestart
21. Ναι: ftp lab@192.168.1.3, cd /usr/bin, get ztest (passive ftp)

**Άσκηση 2: Ένα πιο σύνθετο τείχος προστασίας**

1. kldload ipfw
2. Permission denied
3. ipfw add allow all from any to any via lo0
4. ipfw add allow icmp from me to any icmptypes 8
5. Όχι

6. Περνούν τα εξερχόμενα πακέτα request και απορρίπτονται τα εισερχόμενα reply
7. Ναι, τώρα γίνεται το ping
8. Ναι
9. Όχι, δεν επιτυγχάνει καθώς ο χρόνος λειτουργίας του stateful κανόνα έληξε
10. ipfw add allow icmp from any to me icmptypes 8 keep-state
11. Βλέπουμε και τον δυναμικό κανόνα (Stateful)
12. Δεν υπάρχει πλέον ο δυναμικός κανόνας
13. ipfw add allow udp from any to me 33435,33436,33437
    ipfw add allow icmp from me to any icmptypes 3
14. ipfw add allow udp from me to any 33435,33436,33437
    ipfw add allow icmp from any to me icmptypes 3
15. ipfw add allow udp from any to me 33435,33436,33437
16. ipfw add allow tcp from 192.168.1.0/24 to me 22 keep-state
17. ssh lab@192.168.1.3
18. ipfw add allow tcp from me to any 22 keep-state
19. ipfw add allow tcp from any to me 22 setup
20. Ναι
21. ipfw add allow tcp from any to me 21 in setup keep-state
    ipfw add allow tcp from me 20,21 to any out keep-state
22. Γιατί η δεύτερη εντολή χρησιμοποιεί την θύρα δεδομένων ftp (data port) ενώ η πρώτη την θύρα ελέγχου (control port)
23. ipf add allow tcp from any to me 1024-65535 in setup keep-state
24. Ναι
25. ipfw add allow tcp from me 20,21 to any out keep-state στο PC2
    ipfw add allow tcp from any 20 to me setup keep-state
26. Επειδή οι θύρες δεν είναι απαραίτητα συγκεκριμένες, επιτρέπεται μεγάλο φάσμα -> χαμηλή ασφάλεια
27. kldunload ipfw

**Άσκηση 3: Απλό Network Address Translation**

1. route add -net 0.0.0.0/0 192.168.1.1
2. cli -> interface em0 -> ip address 192.0.2.2/30, interface em1 -> ip address 192.0.2.6/30
3. ifconfig em0 192.0.2.5/30, route add -net 0.0.0.0/0 192.0.2.6
4. service ftpd onestart
5. kldstat -> kernel, ipfw.ko, ipfw_nat.ko, libalias.ko
6. ipfw
7. UNKNOWN (?)
8. 11 κανόνες -> τελευταίος: deny ip from any to any
9. ipfw nat show config -> δεν έχουν ορισθεί
10. Όχι
11. Όχι
12. ipfw nat 123 config ip 192.0.2.1 reset unreg_only
13. ipfw add nat 123 ip from any to any
14. Ναι

15. Ο κανόνας nat 123 ip from any to any
16. tcpdump -i em0 -vvve
17. ipfw zero
18. 192.0.2.1
19. 192.0.2.1
20. Ο κανόνας nat 123 ip from any to any εφαρμόστηκε 40 φορές (10 ping requests, 10 ping replies εισέρχονται και εξέρχονται από το FW1 = 40)
21. Ναι
22. Ο ίδιος κανόνας, δεν ωθείται προς μετάφραση γιατί δεν είναι ιδιωτική διεύθυνση
23. Ναι
24. Είναι θέμα δρομολόγησης, εφόσον με ping λαμβάνω μήνυμα Destination Unreachable από το R1
25. ipfw nat 123 config ip 192.0.2.1 reset unreg_only redirect_addr 192.168.1.3 192.0.2.1
26. Μέσω του ssh με ifconfig βλέπω την IP του PC2
27. ipfw nat 123 config ip 192.0.2.1 reset unreg_only redirect_addr 192.168.1.3 192.0.2.1 redirect_port tcp 192.168.1.2:22 22
28. Στο PC1
29. Με netstat -an φαίνεται η σύνδεση tcp στο PC2
30. Ναι
31. Το PC2
32. PC1

**Άσκηση 4: Τείχος προστασίας και NAT**

1. Όχι, τα ping δεν είναι επιτυχημένα
2. Αποτυγχάνει λόγω του firewall rule deny ip from any to any
3. ipfw add 1100 allow all from any to any via em0
4. Ναι
5. Στο FW1 αφού έχουμε διαγράψει τον κανόνα που στέλνει την κίνηση στο NAT
6. Ο κανόνας allow ip from any to any via em0
7. ipfw add 3000 nat 123 all from any to any xmit em1
8. ipfw add 3001 allow all from any to any
9. ipfw add 2000 nat 123 all from any to any recv em1
10. ipfw add 2001 check-state
11. Το FW1
12. Το PC2
13. FW1
14. PC1
15. PC2
16. Ναι
17. Ναι
18. Ναι
19. ipfw add 2999 deny all from any to any via em1

20. Κανένα δεν επιτυγχάνει
21. ipfw add 2500 skipto 3000 icmp from any to any xmit em1 keep-state
22. Ναι
23. ipfw add 2600 skipto 3000 tcp from any to any 22 out via em1 keep-state
24. Ναι
25. ipfw add 2100 skipto 3000 icmp from any to any in via em1 keep-state
26. Το PC2
27. ipfw add 2200 skipto 3000 tcp from any to any 22 in via em1 keep-state
28. PC1
29. Όχι

**Άσκηση 5: Τείχος προστασίας και NAT**

1. 192.168.1.1 (Interfaces -> LAN)
2. 10.0.0.1/30 (Interfaces -> WAN)
3. 66% (Status -> System)
4. 4
5. 172.22.1.1/24
6. fw (System -> General setup)
7. System -> General setup
8. Όχι
9. Interfaces -> WAN
10. Ναι: Block private networks (RFC 1918 networks)
11. Όχι
12. Services -> DNS forwarder
13. Services -> DHCP server
14. 192.168.1.2, default 192.168.1.1, DNS (cat /etc/resolv.conf) 192.168.1.1
15. Μέσω της υπηρεσίας DHCP, η LAN IP του FW1 γίνεται DNS server των DHCP clients
16. DHCP leases
17. 7
18. Όχι
19. Βλέπουμε απορριφθέντα ping requests από το firewall
20. 4
21. Κανέναν
22. (Any from any to any + fragmented packets)
23. Ναι
24. Όχι
25. Ναι
26. Destination -> WAN address, Proto -> ICMP
27. Ναι

28. Όχι, γιατί δεν έχει διαδρομή προς το PC1
29. Ναι, συμπεραίνουμε ότι χρησιμοποιείται NAT για κίνηση που εκκινείται από την διεπαφή του LAN
30. Με tcpdump βλέπω ICMP requests με διεύθυνση προορισμού 192.168.1.2 (PC1) άρα δεν χρησιμοποείται NAT
31. route add -net 0.0.0.0/0 172.22.1.1
32. Ναι
33. Όχι, γιατί όλες οι εισερχόμενες συνδέσεις στο DMZ μπλοκάρονται από το firewall
34. Όχι, για τον ίδιο λόγο
35. Source: DMZ net, Destination: ! LAN net
36. Ναι
37. Ναι
38. Όχι, no route to host
39. Ναι, γιατί χρησιμοποείται NAT για την εξερχόμενη κίνηση
40. ip 192.168.1.3, default: 192.168.1.1, nameserver: 192.168.1.1
41. Block -> Source: 192.168.1.3, Destination: 172.22.1.2
42. πρίν, γιατί ο πρώτος κανόνας θα επιτρέψει την κίνηση
43. Όχι
44. Ναι, καθώς έχουμε μπλοκάρει μόνο την διεύθυνση προορισμού του SRV1

**Άσκηση 6: Τείχος προστασίας και προχωρημένο NAT**

1. route add -net 203.0.118.0/24 192.0.2.1
2. ok
3. ok
4. ok
5. tcpdump -i em0
6. Εμφανίζονται με την διεύθυνση 203.0.118.14
7. Εμφανίζονται με την διεύθυνση 203.0.118.15
8. Γιατί το NAT είναι Outbound
9. ok
10. ok
11. Κανόνας που επιτρέπει κίνηση TCP από οποιοδήποτε Source/port και Destination 172.22.1.2:22
12. Στο SRV1
13. Μπλοκάρεται από το Firewall rule (επιτρέπουμε μόνο θύρα 22)
14. Μέσω καταγραφής στο R1, παρατηρώ ότι διέρχονται τα πακέτα από τον R1. Από το PC2 φτάνει στο FW1 το οποίο μεταφράζει την διεύθυνση προέλευσης σε 203.0.118.15 και στην συνέχεια στέλνει τα πακέτα στο default gateway R1 το οποίο έχει static route για το υποδίκτυο 203.9.118.0/24 και λόγω Inbound Nat η διεύθυνση 203.0.118.18 γίνεται 172.22.1.2 και φτάνει στον SRV1. Στην αντίθετη κατεύθυνση ακολουθείται η αντίστροφη διαδρομή αφού τα πακέτα φτάνουν στο FW με διεύθυνση προορισμού 203.0.118.15, στην συνέχεια φτάνουν στον R1 και μετά ξανά στο FW με Inbound NAT στην αρχική διεύθυνση του PC2

15. Δεν έχει διαδρομή για την διεύθυνση 192.168.1.2 (ο R1)
16. Είναι επιτυχές καθώς γίνεται αυτόματα μετάφραση NAT outbound προς το δίκτυο WAN
17. Από το R1 στο SRV1 επιτυχώς (Inbound NAT), Από PC2 όχι
18. 172.22.1.2 -> 192.0.2.1 (διεύθυνση NAT διεπαφής WAN)
19. Note: It is not possible to access NATed services using the WAN IP address from within LAN (or an optional network). (Δεν ενεργοποιείται το outbound NAT στις απαντήσεις του SRV1)

**Άσκηση 7: IPSec site-to-site VPN**

1. ok
2. ok
3. ok
4. Ναι
5. ok
6. ok
7. ok
8. ok
9. * * * * * (Proto, Source, Port, Destination, Port)
10. ICMP 192.0.2.6 * WAN address *
11. ifconfig em0 192.168.2.2/24, route add -net 0.0.0.0/0 192.168.2.1
12. Ναι
13. Ναι
14. Ο R1 δεν έχει διαδρομή για τα δίκτυα LAN
15. ok
16. Κανόνας * * * * * Default Ipsec VPN
17. Όχι
18. Ναι
19. ok
20. Όχι
21. Ναι
22. Ναι
23. Ναι
24. Ναι, εμφανίστηκαν δύο εγγραφές για Source 192.0.2.1 και 192.0.2.5 αντίστοιχα
25. Παρόμοια με 7.24
26. tcpdump -i em1 -vvven
27. Όχι
28. Πακέτα πρωτοκόλλου ESP (5), εμφανίζονται οι IP διευθύνσεις των FW1, FW2 στα WAN
29. Άλλαξε το γεγονός ότι δεν συνδεόμαστε από άλλη διεπαφή του FW1 εκτός του WAN1 και άρα το inbound/outbound NAT στο WAN1 λειτουργεί σωστά
30. Παρατηρώ πακέτα TCP με πηγή 192.0.2.5 και προορισμό 203.0.118.18

χωρίς κρυπτογράφηση από το Ipsec αφού δεν είναι διευθύνσεις των LAN1 ή LAN2 όπου είχαμε κάνει την αντίστοιχη ρύθμιση