Εργαστήριο Δικτύων
Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

Ερωτήσεις κατανόησης και Εργασία για το μάθημα:
Σύγχρονες Εφαρμογές Ασφάλειας Δικτύων

---

1) Επίδειξη μηχανισμού 3-WAY HANDSHAKE με χρήση tcpdump

Η εντολή tcpdump (https://www.tcpdump.org/) είναι ένα μοναδικό εργαλείο ανάλυσης της δικτυακής κίνησης. Στο διαδίκτυο μπορείτε να βρείτε πολλά tutorials χρήσης όπως αυτό.
Θα χρησιμοποιήσουμε το tcpdump για την καταγραφή του μηχανισμού σύνδεσης του TCP πρωτοκόλλου (3-WAY HANDSHAKE).
Θα πρέπει να κλείσετε όλες τις εφαρμογές που συνδέονται στο διαδίκτυο για την απλοποίηση της εξόδου των εντολών.

- Στο τερματικό του υπολογιστή σας συνδεθείτε στο VM που έχετε υλοποιήσει πχ ssh root@@192.168.122.XX
- Σε άλλο τερματικό εκτελέστε την εντολή tcpdump -vvv -nn -i ***wlan0*** -s 1500 -S -X -c 5 ’src ***IP_source***’ or ’dst ***IP_destination***’ and ’port 22’ με τις σωστές παραμέτρους της διεπαφής, διεύθυνση πηγής (του υπολογιστή σας) και destination (του VM εσάς).
- Δείξτε τα πακέτα που καταγράψατε και δείξτε τα flags (SYN/FIN/RST/ACK) κάθε πακέτου.

---

2) Πειραματιστείτε και εκτελέστε τις Παρακάτω εντολές. Εξηγείστε την έξοδο που δίνουν.

- tcpdump -v -n host 192.168.1.105
- tcpdump -vvv -nn -i eth0 -s 1514 host 192.168.1.105 -S -X -c 5
- tcpdump -vvv -nn -i wlan0 -s 1514 host 192.168.1.105 -S -X -c 5
- tcpdump -nnvvvXSs 1514 host 192.168.1.105 and dst port 22
- tcpdump -vvv -nn -i eth0 -s 1514 -S -X -c 5 'src 192.168.1.102' or 'dst 192.168.1.102 and port 22'
- tcpdump -vvv -nn -i eth0 -s 1514 -S -X -c 5 src or dst 71.98.70.149
- tcpdump -vvv -nn -i wlan0 -s 1514 -S -X -c 5 'src 192.168.1.102' or 'dst 192.168.1.102 and port 22'
- tcpdump udp -i wlan0
- tcpdump udp -i any -c 10

---

3) Επίδειξη κακόβουλης επίθεσης DoS μέσω IP ADDRESS SPOOFING και SYN FLOODING με IP διευθύνσεις που ανήκουν στο ίδιο LAN.

Στην σελίδα του μαθήματος στο eclass έχουν αναρτηθεί δύο προγράμματα “*port_scan.py*” και “*DoS5.py*”, γραμμένα σε python. Το 1ο πρόγραμμα κάνει ανίχνευση ανοικτών θυρών και εκτελείτε δίνοντας την IP διεύθυνση του στόχου, την πρώτη και την τελευταία θύρα που θα δοκιμάσει: δλδ

port_scan.py <IP_address> <port_start > <port_end > πχ
port_scan.py 192.168.122.88 22 443

Μια θύρα θα είναι ανοικτή εφόσον γίνεται εγκατάσταση σύνδεσης και κάποια διεργασία/πρόγραμμα ακούει αυτήν την θύρα.

Το δεύτερο πρόγραμμα, *DoS5.py* εκτελεί DoS επίθεση με την μέθοδο SYN flooding.
Για να καταλάβετε τι κάνει αυτό το σενάριο, πρέπει να ξέρετε πως δουλεύει το module scapy της python. Το Scapy είναι ένα ισχυρό εργαλείο για τη δημιουργία πακέτων σε οποιοδήποτε από τα πρώτα τέσσερα επίπεδα της στοίβας πρωτοκόλλου TCP / IP - και αυτό περιλαμβάνει τα πλαίσια Ethernet που βρίσκονται στο Layer 2. Μπορεί το Scapy να δημιουργήσει ένα πακέτο, να ορίσετε τα διάφορα πεδία του, και να καταγράψει το πακέτο απόκρισης εάν υπάρχει.
Το εν λόγω πρόγραμμα, δημιουργεί πρώτα μια κεφαλίδα IP με συγκεκριμένη διευθύνση IP πηγής και προορισμού, μετά δημιουργείμια TCP κεφαλίδα με συγκεκριμένες θύρες προέλευσης και προορισμού και με το σύνολο σημαιών SYN ενεργοποιημένο, ώστε τελικά να κατασκευάσει ένα φαινομενικό σωστό πακέτο στο IP Layer. Το script εκτελείτε με την εντολή:

DoS5.py <IP_source> <IP_destination> <port_to_attack> <number_of_packets>

1. Εκτελέστε το port_scan.py από τον υπολογιστή για να ανιχνεύσετε ποιος θύρες είναι ανοικτές στην εικονική μηχανή debian που έχετε υλοποιήσει. Η εντολή είναι: Ποιες πόρτες είναι ανοικτές? Δώστε την έξοδο του προγράμματος.

2. Εκτελέστε το script *DoS5.py* εκκινώντας μια DoS επίθεση στην εικονική σας μηχανή με την εντολή, στην θύρα 22 με αριθμό πακέτων μεγαλύτερο από τον αριθμό των προσπαθειών που έχετε ορίσει στο fail2ban πακέτο. Δώστε την έξοδο σε όλες τις προσπάθειες.

Προτού εκετελέσετε το script *DoS5.py* και για να παρακολουθήσετε την κίνηση (packet sniffer) χρησιμοποιείστε την εντολή tcpdump τόσο στο host όσο και στο VM σας. Ενδεικτικά οι εντολές είναι:
sudo tcpdump -vvv -nn -i wlan0 -s 1500 -S -X 'dst 10.0.0.8' (για τον attacker)
sudo tcpdump -vvv -nn -i wlan0 -s 1500 -S -X 'src 10.0.0.19' (για τον επιτιθέμενο).

3. Για άλλη απόδειξη ότι έχουμε ξεκινήσει με επιτυχία μια DoS επίθεση από SYN flooding, μπορούμε να τρέξουμε την εντολή (σε άλλο παράθυρο στη μηχανή του θύματος): netstat -n | grep tcp
   Δώστε την έξοδο της παραπάνω εντολής. Σε ποια κατάσταση έχει μείνει το επιτιθέμενο VM ως προς την κατάσταση της TCP σύνδεσης?
   Εάν εκτελείτε επανειλημμένα την εντολή netstat - n | grep tcp στον επιτιθέμενο υπολογιστή, θα δείτε την ίδια έξοδο με παραπάνω για περίπου 75 δευτερόλεπτα.
   Τι συμπέρασμα μπορείτε να βγάλετε?

---

4) Άλλες χρήσιμες εντολές για την ανάλυση εισερχόμενης/εξερχόμενης κίνησης είναι η netstat και η netcat.

Το netstat (στατιστικά στοιχεία δικτύου) είναι ένα άλλο εργαλείο γραμμής εντολών για την παρακολούθηση των συνδέσεων δικτύου τόσο εισερχόμενων όσο και εξερχόμενων, καθώς και προβολή πινάκων δρομολόγησης, στατιστικών διεπαφών κ.λπ. Το λογισμικό εγκαθίστανται με την εντολή: ***apt install net-tools***

1. Εκτελέστε τις παρακάτω εντολές (είτε στον host υπολογιστή σας είτε στην εικονική μηχανή) και αναφέρετε την έξοδο τους. Η κεντρική σελίδα του Linux για την εντολή netstat είναι εδώ.

- **netstat-a**
- **netstat -at**
- **netstat -au**
- **netstat -l**
- **netstat -lt**
- **netstat -lu**
- **netstat -s**
- **netstat -st**
- **netstat -su**
- **netstat -tp**
- **netstat -ac 5 | grep tcp**
- **netstat -r**
- **netstat -c**
- **netstat -ap | grep http**

2. Με ποια εντολή μπορούμε να δούμε τα στατιστικά χρήσης της υπηρεσίας ssh και https?
3. Εκτελέστε τις εντολές: netstat -tap | grep LISTEN και netstat -tap | grep ESTABLISHED και αναφέρατε την έξοδο και την σημασία τους.

Άλλα εργαλεία γραμμής για την ανάλυση κίνησης είναι το *iftop* (sudo apt-get install iftop)

---

5) Διαχείριση συνδέσεων και αποστολή UDP/TCP segments με την εντολή netcat.
Το **netcat ή nc** είναι ένα βοηθητικό πρόγραμμα δικτύωσης, το οποίο διαβάζει και γράφει δεδομένα από τη γραμμή εντολών. Χρησιμοποιεί τόσο το TCP όσο και το UDP για επικοινωνία και έχει σχεδιαστεί για να είναι ένα αξιόπιστο εργαλείο back-end για να παρέχει άμεσα συνδεσιμότητα δικτύου σε άλλες εφαρμογές και χρήστες. Το Ncat δεν θα λειτουργεί μόνο με IPv4 και IPv6, αλλά παρέχει στον χρήστη έναν σχεδόν απεριόριστο αριθμό πιθανών χρήσεων. Ενδεικτικές χρήσεις:

- Port Scanning
- Create a Chat or Web Server
- Verbose Scan with Netcat Commands
- HTTP Requests with Netcat Commands
- TCP Server and TCP Client Commands

η βασική χρήση της εντολής είναι:
nc [options] [host] [port] – (port scan)

nc -l [host] [port] – (ενεργοποιεί την ανίχνευση μιας θύρας) . Οι επιλογές είναι:

Μια λίστα με τις επιλογές μπορείτε να βρείτε εδώ, ενώ μερικά παραδείγματα εντολών δίνονται παρακάτω:

- **nc -v -n google.com 1-1000**
- **nc -l -p 1299**
- **printf "GET / HTTP/1.0\r\n\r\n" | nc google.com 80**
- **nc -l 1499 > filename.out**
- **nc -n -v -l -p 5555 -e /bin/bash**
- netcat -u host port

1) Με την χρήση της εντολής netcat κάντε port scanning στην εικονική σας μηχανή πχ με την εντολή: netcat -z -v domain.com 20 -25

2) Στείλτε ένα αρχείο από τον host υπολογιστή σας στο VM εκτελώντας αντίστοιχα τις παρακάτω εντολές:

- netcat -l 4444 (στο VM)
- netcat IP_address_VM 4444 < <αρχείο προς αποστολή> (στο host υπολογιστή)

3) Δημιουργείστε μια backdoor πόρτα στο VMs και εκτελέστε εντολές απομακρυσμένα από τον host υπολογιστή σας.
Με ποια εντολή tcpdump θα μπορούσαμε να ανιχνεύαμε την πόρτα που έχει ανοίξει?