

# Ασφάλεια Δεδομένων και Ιδιωτικότητα

Θέματα 2023 -2024 (11/6/2024)

ηλεκτρονικά στο moodle του cnlab - διάρκεια περίπου 1:00

Επιτρέπονταν βιβλία και εκτυπωμένες διαφάνειες (όχι προσωπικές σημειώσεις, χειρόγραφες ή εκτυπωμένες)

Δεν είχαμε όλοι τα ίδια θέματα, σύνολο ερωτημάτων = 10.

Τα θέματα από μνήμης :

- 1) Αλγόριθμος RSA με  $n = 143$  και ιδιωτικό κλειδί  $d=77$ . Βρείτε το δημόσιο κλειδί  $e$ . Έδινε πολλαπλής.

Λύση :  $143 = 11 \times 13$ .  $\phi(n) = (11 - 1) \times (13 - 1) = 120$

$ed \bmod 120 = 1$ , από τα πολλαπλής που έδινε ταίριαζε  $e=53$

2)

Να αντιστοιχήσετε τη σωστή ονομασία σε κάθε μια από τις παρακάτω περιπτώσεις:

Ένας χάκερ μπήκε μέσω δικτύου στο σύστημα μιας εταιρίας κινητής τηλεφωνίας, απέκτησε δικαιώματα admin στο υποσύστημα νόμιμης παρακολούθησης και εγκατέστησε λογισμικό με το οποίο μπορούν να γίνουν χειρισμοί πάνω στο σύστημα χωρίς να υπάρχουν οι νόμιμες προϋποθέσεις.

Rootkit

Ο Γιώργος προχθές έψαχνε να βρει δωρεάν λογισμικό για επεξεργασία video. Κατέβασε ένα πρόγραμμα, αλλά μόλις το ξεκίνησε σβήστηκε ο σκληρός του δίσκος.

Δούρειος Ίππος

Ο τεχνικός επισκευής μιας συγκεκριμένης μάρκας υπολογιστών mini κατά τη δεκαετία του '80 μπορούσε να χρησιμοποιήσει το γενικό password zykhwnuts για να αποκτήσει δικαιώματα administrator.

Κερκόπορτα

- 3) Playfair με κλειδί INFORMATIONSECURITY. Έδινε ένα κείμενο που έπρεπε να αποκρυπτογραφήσεις και το αποκρυπτογραφημένο κείμενο έβγαινε OPERATIONB

4)

4 (5)

Ποιο ή ποια από τα παρακάτω αποτελεί(ούν) χαρακτηριστικό(ά) των signature-based IDS (να επιλέξετε όλες τις σωστές από τις παρακάτω δηλώσεις);

- ☒ a. Ανιχνεύουν με βάση την υπογραφή
- ☐ b. Δεν ανιχνεύουν νέες επιθέσεις
- ☒ c. Τα περισσότερα βασίζονται σε απλούς αλγόριθμους αντιστοίχισης προτύπων (pattern matching algorithms)
- ☐ d. Μοντελοποιούν την κανονική χρήση του δικτύου ως χαρακτηριστικό θορύβου
- ☒ e. Μοντελοποιούν την φυσιολογική χρήση του δικτύου και ανιχνεύουν τις αποκλίσεις από αυτήν συμπεριφορές
- ☐ f. Είναι προγραμματισμένα να ερμηνεύουν συγκεκριμένες σειρές πακέτων

- 5) Άσκηση τύπου firewall:

Δίδεται ο ακόλουθος πίνακας κανόνων, με τον οποίο έχει παραμετροποιηθεί ένα firewall. Ζητείται να προσδιορίσετε τις ενέργειες εφαρμοστούν για τα ακόλουθα πακέτα, σε περίπτωση που το firewall ακολουθεί πολιτική first match (ή top-down ή in order):

| UDP | s:66.68.80.90:9300 | d:23.45.68.5:53 | Data... |  
| TCP | s:66.68.80.90:7800 | d:23.45.68.10:80 | Data... |

	Source	Destination	Protocol	Source Port	Destin. Port	Action
1	Any	23.45.68.5/32	UDP	Any	53	Allow
2	Any	23.45.68.0/32	TCP	Any	80	Allow
3	Any	23.45.68.11/32	TCP	Any	80	Allow
4	Any	23.45.68.0/24	ALL	Any	Any	Deny
5	23.45.67.0/24	23.45.68.0/24	TCP	Any	Any	Allow
6	23.45.67.3/32	23.45.68.3/32	UDP	8000	4058	Allow
7	128.59.0.0/16	23.45.68.5/32	TCP	Any	Any	Reject
8	128.59.17.0/24	23.45.68.0/24	TCP	Any	1099	Allow
9	128.59.16.2	Any	ALL	5589	Any	Reject
10	66.68.80.90	23.45.68.0/5	UDP	1025:65535	53, 6010	Allow
11	128.59.0.4	Any	ALL	Any	3306	Allow
12	Any	23.45.68.3	UDP	Any	6000:6010	Reject
13	Any	23.45.68.10/32	TCP	Any	0:1024	Reject
14	Any	Any	Any	Any	Any	Deny

6)

**15 (5)**

Έστω ότι μια συνάρτηση κατακερματισμού  $H$  οδηγεί σε κωδικό μήκους  $N$  bits. Ένας επιτιθέμενος προσπαθεί να βρει δύο μηνύματα  $x, y$  τέτοια ώστε  $H(x)=H(y)$  και υλοποιεί τον εξής αλγόριθμο: Βρίσκει ένα τυχαίο  $z$ , υπολογίζει το  $H(z)$  και κρατάει το ζεύγος  $(z, H(z))$  σε μια λίστα. Κάθε φορά συγκρίνει το νέο  $H(z)$  με αυτά που έχει ήδη στη λίστα και σταματάει όταν βρει ένα ίδιο. Πόσες περίπου προσπάθειες (κληρώσεις του  $z$ ) θα χρειαστεί;

- ☐ a. 2 στην  $N$
- ☐ b. 2 στην  $N-2$

☐ c. 2 στην  $N-1$

☒ d. 2 στην  $N/2$

7) Πότε χρησιμοποιείται ο Diffie – Hellman αλγόριθμος; Πολλαπλής, σωστή ήταν ώστε οι χρήστες να συμφωνήσουν σε κοινό κλειδί για συμμετρική κρυπτογραφία;

8) Πότε μειώνεται η ασφάλεια σε συστήματα virtual machine? Πολλαπλής με παραπάνω από μια σωστές. Δεν έχω ιδέα, Προπο

9) Όταν εκδίδεις loyalty card σε ένα κατάστημα και στους όρους αναφέρεται ότι το κατάστημα μπορεί να χρησιμοποιήσει τα στοιχεία σου για τις συναλλαγές σου στο κατάστημα και για να σου προωθήσει προϊόντα του καταστήματος, ποια από τα παρακάτω σενάρια δεν αποτελούν παραβίαση ιδιωτικότητας. Έδινε διάφορα σενάρια

10) Feistel τύπου, αλλά δεν είχε διπλάσιους γύρους:

**14 (10)**

Θεωρήστε τροποποιημένη δομή αλγορίθμου Feistel, η οποία είναι πανομοιότυπη με την κλασσική δομή, αλλά έχει διπλάσιους γύρους συνολικά. Η έξοδος του 18<sup>ου</sup> γύρου της τροποποιημένης δομής αλγορίθμου Feistel κατά την αποκρυπτογράφηση συμβολίζεται με LD18||RD18. Εάν η έξοδος αυτή συμπίπτει με την είσοδο του  $N^{\text{ου}}$  γύρου της τροποποιημένης δομής αλγορίθμου Feistel κατά την κρυπτογράφηση, όταν αυτή υποστεί αντιστροφή των δύο μερών της (32-bit swap), εντοπίστε για ποιο  $N$  ισχύει αυτό (αν ισχύει).