מגישים: 200878627 יניב לידן
204736961 דן אברהם

עבודה 2 – אבטחה

שאלה 1:

1. במידה והתוקף (נניח C) מאזין לקשר הוא יכול לבצע התקפת Man in the middle בצורה הבאה:

$A \rightarrow B: A$ (C intercepts the message)
$B \rightarrow A: N_B$ (C intercepts the message)
$A \rightarrow B: \{N_B, K_{AB}\}_{K_{AS}}$ (C intercepts the message)
$C \rightarrow S: \{A, C, \{N_B, K_{AB}\}_{K_{AS}}\}_{K_{CS}}$
$B \rightarrow S: \{A, B, \{N_B, K_{AB}\}_{K_{AS}}\}_{K_{BS}}$
$S \rightarrow C: \{N_B, K_{AB}\}_{K_{CS}}$
$S \rightarrow B: \{N_B, K_{AB}\}_{K_{BS}}$

נוצר מצב בו A, B ו-C מכירים את מפתח ההצפנה K_{AB} ו-C יכול ליירט ולפרש כל הודעה שעוברת בין A ל-B ומוצפנת באמצעות מפתח זה.

2. היכולות הנדרשות מן התוקף כדי לבצע התקפה זו הן האזנה לקשר בין A ל-B ויירוט החבילות.

3. נתקן את הפרוטוקול כך:

Note: *Here B^* and B both are the public key of B*
$A \rightarrow B: A$
$B \rightarrow A: \{B, N_B\}_{K_{BS}}$
$A \rightarrow B: \{\{B, N_B\}_{K_{BS}},\ K_{AB}\}_{K_{AS}}$
$B \rightarrow S: \{A, B^*, \{\{B, N_B\}_{K_{BS}},\ K_{AB}\}_{K_{AS}}\}_{K_{BS}}$
$S \rightarrow B: \{\{B^*, N_B\}_{K_{BS}}, K_{AB}\}_{K_{B^*S}}$ $\quad if\ B^* == B$

כך שכש-B שולח לשרת את ההודעה השרת יחזיר לו אותה מוצפנת עם המפתח הפומבי שהוא שלח לו רק אם הוא שווה למפתח הפומבי שמוצפן בפנים. ובמידה שהתוקף ישלח את המפתח הפומבי של B הוא יקבל את ההודעה מוצפנת בעזרת K_{BS} ולא יוכל לפענח אותה ולחלץ את המפתח K_{AB}.

מגישים: 200878627 יניב לידן
204736961 דן אברהם

שאלה 2:

1. Kerberos הוא מנגנון מבוסס הצפנה סימטרית המיועד לצורך שיתוף מפתחות סודיים באופן מאובטח.

i. מטרת הפרוטוקול הינה אוטנטיקציה של משתמשים אל מול שירות מסוים.
ii. השחקנים והרכיבים במערכת הינם לקוח המעוניין לקבל שירות מסוים, השירות עצמו, ומרכז הפצת המפתחות (Key Distribution Center = KDC) המחולק לשרת אימות (Authentication Server = AS) ומשרת להענקת כרטיסים (Ticket Granting Server = TGC).
iii. התהליך שמבוצע מרגע התחלת הבקשה לשירות:

$$** \boldsymbol{C - Client, AS - Authentication\ Server, TGS - Ticket\ Granting\ Server, Svc = Service} **$$

$C \rightarrow AS$: $\{C_{ID}, Service - Request\}_{K_{C-AS}}$

$AS \rightarrow C$: $\{TGT\}_{K_{AS-TG}}$ $\quad *if\ C\ is\ authenticated$

$C \rightarrow TGS$: $\{TGT\}_{K_{AS-T}}$, $Service - Request$

$TGS \rightarrow C$: $\{Token_{TimeStamp}\}_{K_{TGS-Service}}$ $\quad *if\ Token\ is\ valid$

$C \rightarrow Service$: $\{Token_{TimeStamp}\}_{K_{TGS-Servic}}$ $\quad while\ Service\ approved\ Token$

כאן, הלקוח ישלח את ה-Token המוצפן לשירות בכל בקשה לשירות והשירות יאשר ללקוח את השימוש כל עוד חותמת הזמן על ה-Token תקפה.

2. **i.** פרוטוקול Needham-Schroeder הינו פרוטוקול המבוסס על הצפנה סימטרית באמצעות מפתח פומבי בין המשתמשים לשרת אמון המוכר לכלל משתמשי המערכת. תהליך הפרוטוקול מתבצע כך:

$$** \boldsymbol{A, B - Alice\ and\ Bob\ (2\ users).\ S - Server,\ N_x - random\ number\ from\ x,}$$
$$\boldsymbol{K_x - x's\ public\ key, K_x^{-1} - x's\ private\ key, Request_{xy} - x\ request\ to\ send\ y\ a\ message} **$$

$A \rightarrow S$: $Request_{AB}$

$S \rightarrow A$: $\{K_B, A\}_{K_S^{-1}}$

$A \rightarrow B$: $\{N_A, A\}_{K_B}$

$B \rightarrow S$: $Request_{BA}$

$S \rightarrow B$: $\{K_A, A\}_{K_S^{-1}}$

$B \rightarrow A$: $\{N_A, N_B, K_{AB}\}_{K_A}$

$A \rightarrow B$: $\{N_B, K_{AB}\}_{K_B}$

כעת A ו-B יכולים לדבר ביניהם באמצעות מפתח ההצפנה K_{AB} שמורכב מ- N_A, N_B.

ii. במידה והתוקף (נניח C) יכול לגרום ל-A להתחיל איתו שיחה הוא יכול לבצע את ההתקפה הבאה:

1. $A \rightarrow S$: $Request_{AC}$
2. $S \rightarrow A$: $\{K_C, A\}_{K_S^{-1}}$
3. $A \rightarrow C$: $\{N_A, A\}_{K_C}$
4. $C \rightarrow S$: $Request_{CB}$
5. $S \rightarrow C$: $\{K_B, C\}_{K_S^{-1}}$
6. $C \rightarrow B$: $\{N_A, A\}_{K_B}$
7. $B \rightarrow S$: $Request_{BA}$
8. $S \rightarrow B$: $\{K_A, B\}_{K_S^{-1}}$
9. $B \rightarrow C$: $\{N_A, N_B, K_{AB}\}_{K_A}$
10. $C \rightarrow A$: $\{N_A, N_B, K_{AB}\}_{K_A}$
11. $A \rightarrow C$: $\{N_B, K_{AB}\}_{K_C}$

כעת C גרם ל-B לחשוב שהוא A ויכול לדבר עם B תוך כדי התחזות ל-A ולגרום ל-B לשלוח לו הודעות שמיועדות ל-A.

מגישים: 200878627 יניב לידן
204736961 דן אברהם

iii. נשנה את הפרוטוקול כדי שיעבוד כך:

$\underline{Note}$: $Here\ K_B\ and\ K_B^*\ are\ both\ the\ public\ key\ of\ B$

1. $A \rightarrow S:\ \ Request_{AB}$
2. $S \rightarrow A:\ \ \{K_B, A\}_{K_S^{-1}}$
3. $A \rightarrow B:\ \ \{N_A, A\}_{K_B}$
4. $B \rightarrow S:\ \ Request_{BA}$
5. $S \rightarrow B:\ \ \{K_A, A\}_{K_S^{-1}}$
6. $B \rightarrow A:\ \ \{N_A, N_B, K_{AB},\ K_B^*\}_{K_A}$
7. $A \rightarrow B:\ \ \{N_B, K_{AB}\}_{K_B^*}$

כעת כש-C יקבל את ההודעה מ-B (בשלב 6 של הפרוטוקול, שלב 9 בתהליך התקיפה מתת סעיף קודם) ויעביר אותה ל-A לפענוח, A יחזיר את ההודעה מוצפנת באמצעות המפתח הפומבי של B אותו הוא מקבל בתוך ההודעה.

שאלה 3:

1. **i.** לא נכון, פנייה מתוך הארגון (עמדות קצה A,B,C) לא עוברת דרך חומת אש בכלל.
   ii. לא נכון, בקשה שירות משרת המיילים MS עוברת רק דרך חומת האש PF2.
   iii. נכון, כפי שניתן לראות ה-PRX משמש כשרת פרוקסי וכל חיבור לשרת ה-HS קורה דרכו.
   iv. נכון, כיוון שכל גישה מעמדת קצה לשרת MS עוברת דרך PF1. כיוון ש-PF1 הוא packet filter ניתן לקבוע כי כל החבילות שב-header שלהן המקור הוא C לא תעבורנה לשרת ה-MS.

2. הארגון יכול לחסום כל בקשת HTTP מעמדה A באמצעות חומת האש PF1 ע"י זיהוי החבילה של בקשת ה-HTTP מה-header לפי המקור והיעד.

3.

Rule ID	In/Out	Src. IP	Dst. IP	Protocol	Src. Port	Dst. Port	Action
1	In	*	10.0.0.9	TCP	*	80	Allow
2.1	In	211.*	10.0.0.5	*	*	*	Drop
2.2	In	*	10.0.0.5	TCP	*	25	Allow
2.3	In	*	10.0.0.5	TCP	*	465	Allow
2.4	In	*	10.0.0.5	TCP	*	587	Allow
3.1	Out	*	*	*	*	*	Allow
4	*	*	*	*	*	*	Drop

מגישים: 200878627 יניב לידן
204736961 דן אברהם

שאלה 4:

	accounts			cv.txt			exam			solutions		
	R	*W*	*A*	*R*	*W*	*A*	*R*	*W*	*A*	*R*	*W*	*A*
alice	V		V	V	V					V		
bob			V	V			V					
charlie			V	V			V			V		

שאלה 5:

א.

Capabilities				Owner	Group	File Name
Type	User	Group	Other			
-	rws	--x	---	root	it	ITUpdatePassword
-	rws	--x	---	root	bank	UserUpdatePassword
-	rw-	rw-	---	root	sudo	password

ב.

Capabilities				Owner	Group	File Name
Type	User	Group	Other			
d	rwx	-w-	---	root	bank	PendingTransactions
d	rwx	-w-	--T	root	privileges	ApprovedTransactions
-	rws	--x	---	root	it	ApprovedAllPendingTransactions