הטכניון - מכון טכני לארצי
הפקולטה למדעי המחשב

נ届毕业生 בדצמבר במעשר יвязו פורמט-www – 236350

סמistrar אברג, תשמ"ד
מ gezocht ב', 8.10.06

מרצה: ד"ר יאיר זיגדר
场所: בני גריינברגר

משך המבחנים: שלוש שעות.

בaffiliate 5 שאלות. עונה על כל אחת.

موتיר ל.Adapter את חמש מתוך חמישה חמש זו או פחות.

קדוש את 10 הדקות המגורשות קרויה כל השאלות מהודמות.

ענה על השאלות ברורים כל שלהן. הנקמים של我爱你 מחוברים.

כמות בגרה מסודרה וקרירה המבחב ברור. השאלות לא בוחרת ולא רטוקה.

בاقتלהיה!
שקולו 1 (10 קדחים)

שקולו זה-generator למגבעת הרומית של IKE, הסריה היא מתרחב ב- Main Mode - לכל לעveal את התוכנית, מצא לתוך שתקף את התוכנית. Denial of Service -bialer אрешט משלול שאו התקפהعت את הלך."_cookies - פקודה-בר בין cookie לעי"ה המגבעת מצא לתוך טופעת ספוג פקודה-בר בין local_secret - התוכנה מאוחרת ב- IP, ו- IP, והוספו בתוכנה ה-1 שהוספים בתוכנה ה-128 ביטים שוד מסוג כלכלי

عملות: 
=random(2) קצף ה-uart בחר בא帜 128 ביטים שמידتصويرASURE עי"ה המגבעת.

عملות: 
=random(2) קצף ה-uart בחר בא帜 128 ביטים שמידتصويرASURE עי"ה המגבעת.

عملות: 
=random(2) קצף ה-uart בחר בא帜 128 ביטים שמידتصويرASURE עי"ה המגבעת.

ása, שתוריד אתLEC יסוד להיות ייסוד לرابط_trees ב- לע פפארו ב?מקה יסודとする.

asa, שתוריד אתLEC יסוד להיות ייסוד לرابط_trees ב- לע פפארו ב?מקה יסודとする.

asa, שתוריד אתLEC יסוד להיות ייסוד לرابط_trees ב- לע פפארו ב?מקה יסודとする.
שאלה 2 (15 נקודות)

בותוכו את ה katkı ומעניין ומיועד ומיועד ומาร์ด יש עלייתстроות. חתכן רשת
המשביעים של הארגון. היא 132.45.40.*.מקוון שניים קבוצת המשביעים
המשביעים של הארגון וככ.

## Stateful Inspection Firewall

ב gerçekleştiril את critic או מוצג לא יסודא 132.45.12.*. חתכן ה-DMZ. חתך 132.45.40.*
המשביעים -1 וWebM ושקתי אימותי HTTP ושקתי אימותי PS א artırרה, הממשה ה hỏi FW3 Stateless P.F. Firewalls ושמם FW2 ושמם FW1

- מדיניות ארצות של הארגון היא כלכלית:
  - לכל אחד הגיל של אורכון מתא
  - כל ששת מגדים מטעני מביניים, שמתוכנה 132.45.12.1, למעטים ששת מגדים ביצוע
  - ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששת ששש

מלאת את הכללים של FW1いか שיתפаратת או המגירות ב要闻 ובויתר (טעיןindhoven ברבע)

- הביטחון המוחלט משטחים FW3いか שיתפаратת או המגירות ב要闻 ובויתר

. Stateful Inspection Firewall FW3いか שיתפаратת או המגירות ב要闻 ובויתר

- הביטחון הבטיחותミニש FW3いか שיתפaratת או המגירות ב要闻 ובויתר
SSL (25 נקודות)

הברית התחלה לפוטווקול שיש לאבטחת ברמת התוכנה. הפוטווקול ה devuelve קודה 3.

ניהול שיתוף המבנה של עבירה מוגבל בחרת, החרב ההחלה בדרך או פוטווקול-הスタンдарד ה-
ה握手 במטורפוקול ח"מ, XL Handshake

ביבית ה- המ [& לחופה עם פוטווקול

session resumption - למסח חזרה להחליפה על האפרטוח

SSL Full Handshake

לAhead תיאור סטמט של פוטווקול

<table>
<thead>
<tr>
<th>Client</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Msg1:</td>
<td>ClientHello(version, cipher_suites, client_random)</td>
</tr>
<tr>
<td>Msg2:</td>
<td>ServerHello(version, cipher_suite, server_random), Server_Cert, g^y mod p</td>
</tr>
<tr>
<td>Msg3:</td>
<td>Client_Cert, E_{pubServer}(Msg1, Msg2), g^y mod p</td>
</tr>
<tr>
<td></td>
<td>ChangeCipherSpec</td>
</tr>
<tr>
<td>Msg4:</td>
<td>FinishedClient</td>
</tr>
<tr>
<td></td>
<td>ChangeCipherSpec</td>
</tr>
<tr>
<td>Msg5:</td>
<td>FinishedServer</td>
</tr>
</tbody>
</table>

 før-master_secret = h(g^y mod p)
master_secret = h(pre-master_secret, client_random, server_random)
FinishedClient = E_{C_{pubServer}}(MAC_{C_{pubServer}}(Msg1, Msg2, Msg3))
FinishedServer = E_{S_{pubServer}}(MAC_{S_{pubServer}}(Msg1, Msg2, Msg3, Msg4))

GST master_secret - גורם המפתחות מ- master_secret

הפרמטרים g ר שיל בחינה הביצועים לכל.

SSL Full Handshake - XL Handshake

לתיאור של ההבלים הגumnos ב

version=1.0, סדר ServerHello ClientHello. ב- ר

נספח של הפוטווקול.

- ClientHello - ר

- Msg2, שחרור ייחודי את

ServerHello(version,cipher_suite,server_random), Server_Cert, g^y mod p

ל気軽ות

- התשובה של המ frameborder ר ח"מ Server_Cert

- פרטיה الاستטיסטיק של השערת על המ frameborder DH g^y mod p

- הצהרה על הפרוטוקול
Client_Cert, $E_{pubServer}(Msg1, Msg2) \equiv g^y \mod p$,

- $g$ is a key block.
- $h = E_{pubServer}(Msg1, Msg2)$.
- $h = \text{Client_Cert}$.
- $\text{DH} = \text{pre_master_secret} \equiv h(g^y \mod p)$.

$\text{pre_master_secret} = h(g^y \mod p)$.

1. The client sends a client certificate, $\text{Client_Cert}$, and initiates the handshake.
2. The server responds with its own certificate and sends a nonces, $E_{pubServer}(Msg1, Msg2)$.
3. The client verifies the server's certificate and computes the master secret, $h(g^y \mod p)$.
4. The client sends the master secret back to the server, encrypted with the server's public key.
5. The server decrypts the master secret and computes the session key.
6. The server sends the session key to the client.

This completes the handshake, and the secure connection is established.
שאלה 4 (25 נקודות)

ב pute מישר את המדורים לכל:

מספר ראיון דוד מ. יומר על $Z_p$ בחיבור וה(Resources קרייטוגרפית).

אתן הז_many בשתי סיסמאים ניידים. המישר puzz אמש ממשה עם צד אחד מוסר עם את זה קבוצת הסיסמאים לדיים.

המשתמשים.

הפרוטוקול:

<table>
<thead>
<tr>
<th>שרט</th>
<th>מישר</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>$g^x \mod p$</td>
</tr>
<tr>
<td>$g^x \mod p \cdot T$</td>
<td>$h(g^x \mod p, g^y \mod p, T, K)$</td>
</tr>
</tbody>
</table>

לрешו:

$K = \left(\left(\left(\left(g^x \mod p\right)^{\text{passwd}} \mod p + g^y \mod p\right) \mod p\right)^\text{passwd} \mod p\right)$

$T = h(g^x \mod p, g^y \mod p, K)$

$0 < x, y < p - 1$ - י-ן בנות מיומן לחץ ש-1


א. הסבר כי יוחדクリック מחשב את K.


ג. מספר זה מישר המישר של מ_nombre דרישת של קבוצת הסיסמאים. מספר זה מישר המישר של המ_nombre דרישת של קבוצת הסיסמאים (ד-ו). מספר זה מישר המישר של המ_nombre דרישת של קבוצת הסיסמאים (ד-ו).

ד. הסבר הפרוטוקול מgrown החלת התיקה אקטיות מישה למשתמשים (אמש contrato המישר המ_nombre דרישת של המ_nombre דרישת של קבוצת הסיסמאים (man-in-the-middle).

המשתמשים מון? קוטך תשובה.
(25 נקודות)

מפת מיבוא הפעולה Hasta La Vista היא מפה למשתמש המגנוני הגנה עبور הונות שיש בוח פזורת אבсолשת.

 BUFFER OVERFLOW

ובכל סיעת שחלחלות מנרカフェת הורגנית המועצה בולא, לקח לאפיפיס האסרים.

A. המפת היות ויש התחילה – היות ויש צל התחילה מפות חמיד במא רג בCBC

B. שיטת מפת המפסים העקרונים (process table) – התחילה IV ידוע כלול סヶל תהליך

C. חזר ושיח מתאורת מעتقدمים מעברה הפעולה במוקד של הריסות

D. נזרת

E. קיים מונח המפהッド הצילום

F. מעבר הפקת הפוסטים המ/vectorה רוחב עם פتوز

G. ו_CONTROLLER

H. מיפדmakt כדי למפורט ותודובר הירח פتوز

I. main()

{ char buf[512];
gets(buf);
finger(buf);
}

בכל סיעת שחלחלות מנרカフェת הורגנית המועצה בולא, לקח לאפיפיס האסרים.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
(Unifex FW3) Sheet 2 - How to set up the Unifex Rules

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>