



أوراق العمل

الأمن السيبراني

ورقة عمل (١-١-٢-١)

جدول التعلم K.W.L. عن مفهوم الأمن السيبراني

عزيزي المشارك، أمامك جدول التعلم K.W.L. في ضوء معلوماتك وخبراتك السابقة، قم بتعبئة العمود الأول والثاني في بداية النشاط، ثم قم بتعبئة العمود الثالث والرابع بعد الانتهاء منه.

ماذا أعرف؟	ماذا أريد أن أكتشف؟	ماذا تعلمت؟	كيف أستطيع أن أتعلم أكثر؟
.....
.....

ورقة عمل (١-١-٢-٢)

مفهوم الأمن السيبراني

عزيزي المشارك، في ضوء المناقشات التي تمت مع المجموعات، تعاون مع مجموعتك و استكمل نموذج فراير الآتي عن مجال الأمن السيبراني

التعريف	خصائصه
المجالات	التطبيقات

الأمن السيبراني

ورقة عمل (٣-٢-١-١):



تهديدات الأمن السيبراني

عزيزي المشارك، في ضوء ما تعلموته عن مفهوم الأمن السيبراني تعاون مع مجموعتك في استكمال المخطط الذي أمامك لاستنتاج أهم التهديدات التي تواجهه الأمن السيبراني

.....

.....

.....

.....

.....

.....

.....

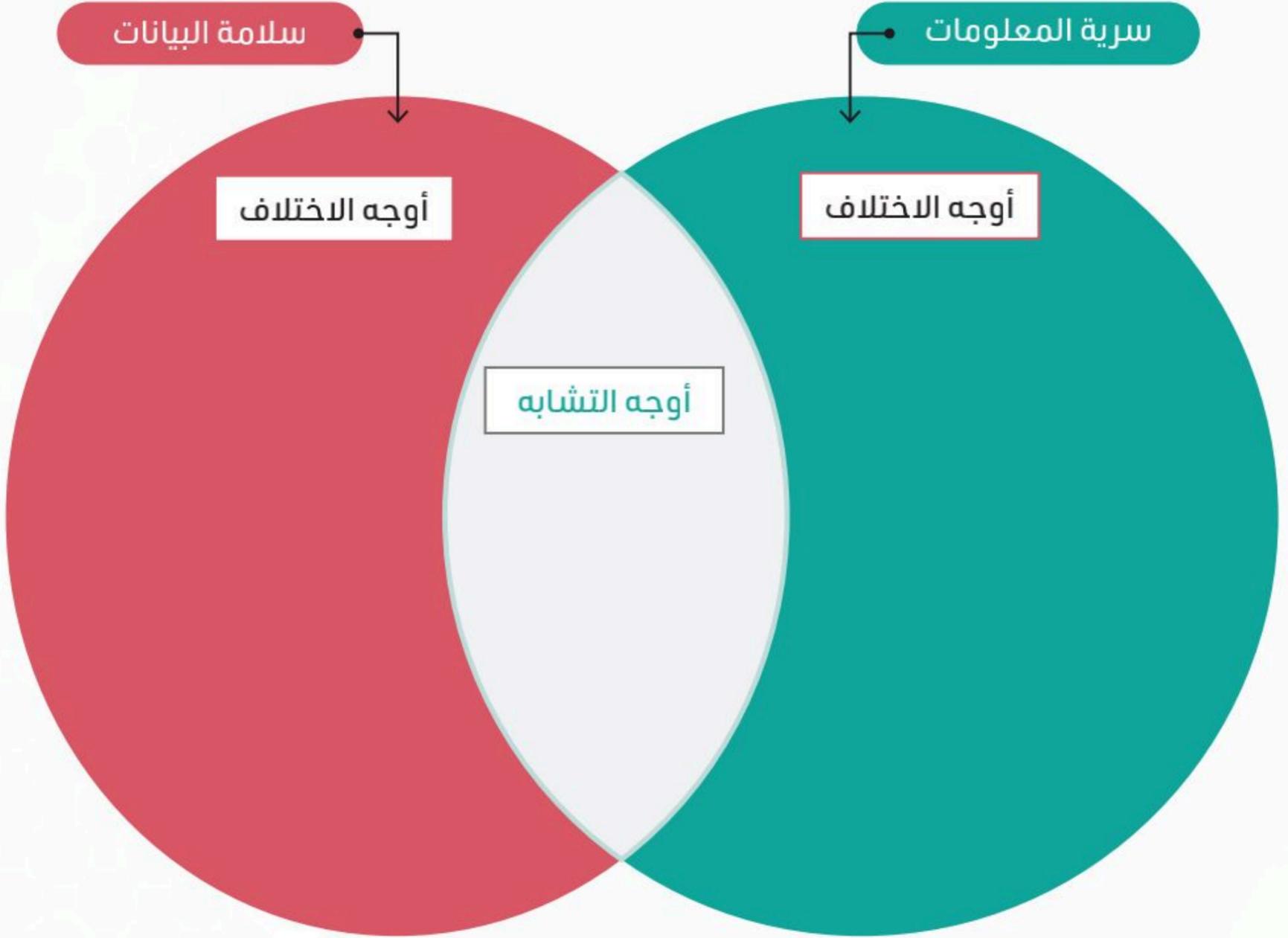
.....

.....

ورقة عمل (١-١-٣-١)

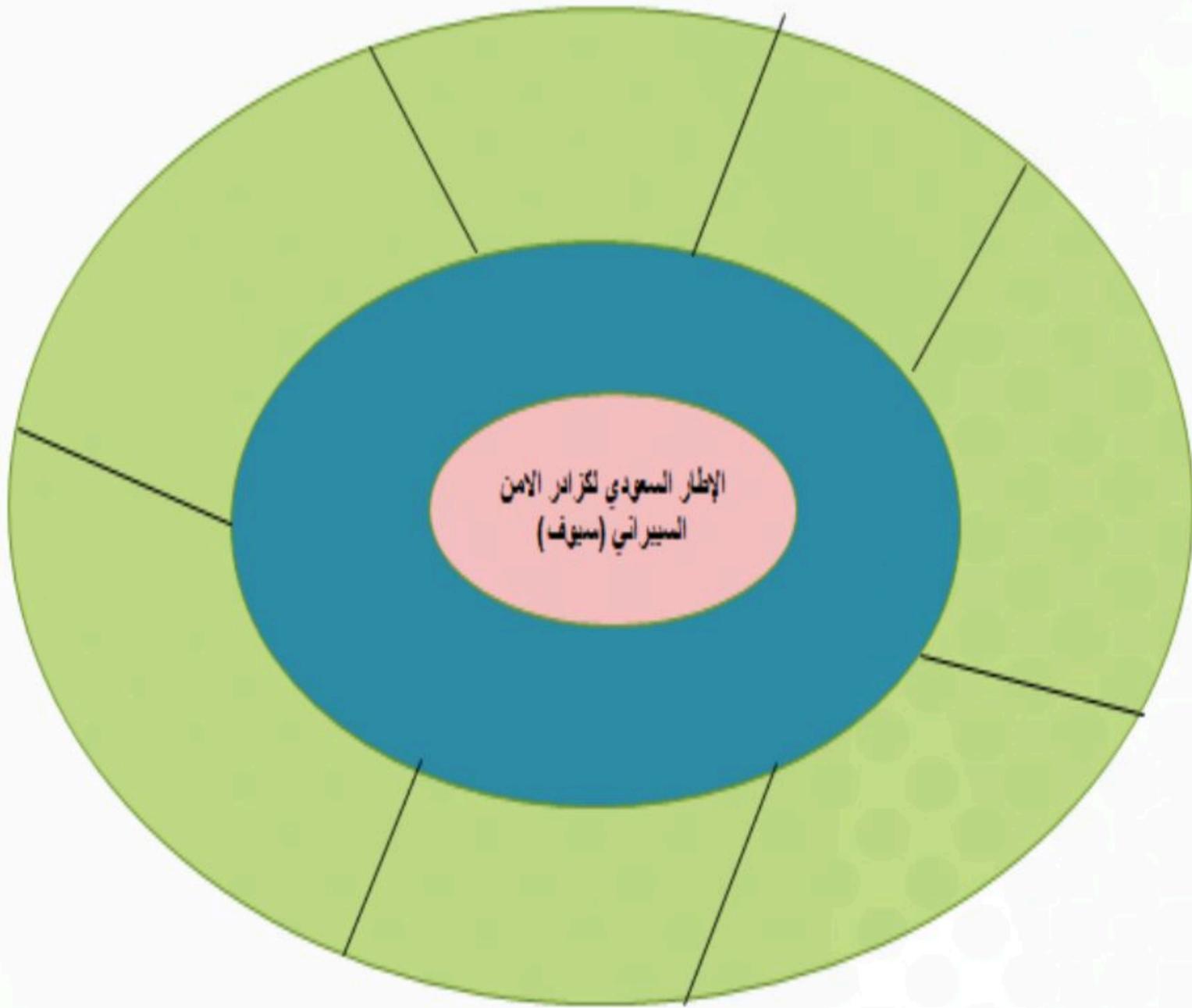
المقارنة بين سرية المعلومات وسلامة البيانات

عزيزي المشارك، أمامك خريطة الفقاعة المزدوجة للمقارنة بين مفهومي سرية المعلومات وسلامة البيانات حاول أن تستنتج أوجه الشبه والاختلاف بين كلٍّ منهما



ورقة عمل (١-١-٤-١) 
الإطار السعودي سيوف

عزيزي المشارك، بعد قراءتك للإطار السعودي لكوادر الأمن السيبراني، أمامك مخطط البيت الدائري عن إطار سيوف، تعاون مع مجموعتك في استكمال هذا المخطط



ورقة عمل (٢-٤-١-١)

لعبة تعليمية لتصنيف الأدوار الوظيفية حسب المجال

عزيزي المشارك، أمامك مجموعة من الأدوار الوظيفية في مجال الأمن السيبراني قم بتصنيفها حسب مجال التخصص المعبر عنها.

- ١) أخصائي الخصوصية وحماية البيانات (.....)
- ٢) أخصائي تشفير (.....)
- ٣) أخصائي التحليل الجنائي الرقمي (.....)
- ٤) مصمم معمارية الأمن السيبراني (.....)
- ٥) أخصائي اختبار الاختراقات (.....)
- ٦) مدير الموارد البشرية للأمن السيبراني (.....)
- ٧) أخصائي تطوير أمن النظم (.....)
- ٨) أخصائي الذكاء الاصطناعي للأمن السيبراني (.....)
- ٩) أخصائي الحوسبة السحابية الآمنة (.....)
- ١٠) مقيم البرمجيات الآمنة (.....)
- ١١) مطور المناهج التعليمية للأمن السيبراني (.....)
- ١٢) محلل أمن النظم (.....)
- ١٣) محلل معلومات التهديدات السيبرانية (.....)
- ١٤) أخصائي قانون الأمن السيبراني (.....)
- ١٥) مستشار الأمن السيبراني (.....)

ورقة عمل (١-٢-٧-١)

ربط المعارف والمفاهيم بمواقف الحياة اليومية

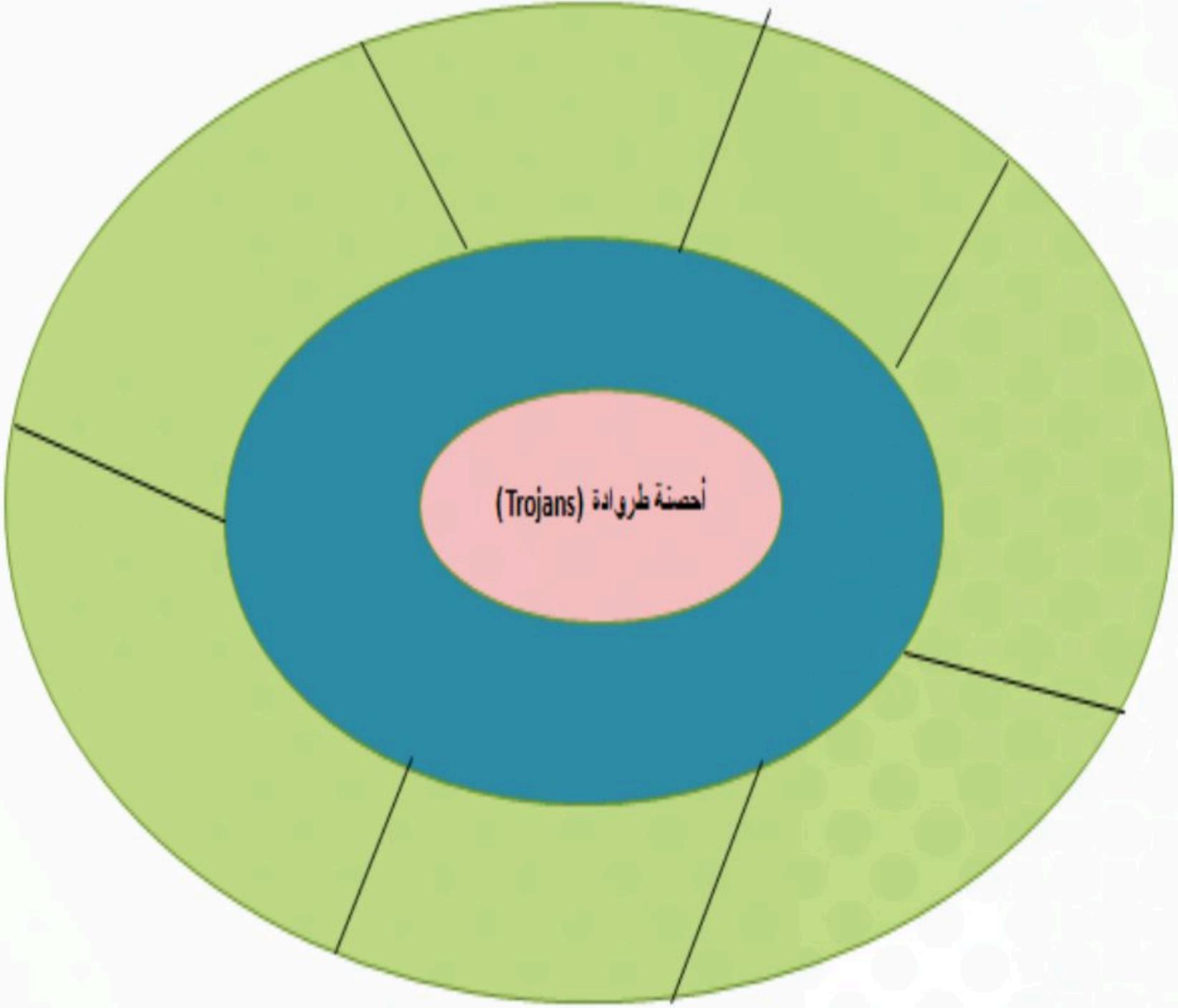
عزيزي المشارك فيما يأتي مجموعة المعارف الخاصة بالتصميم الهندسي، اقترح طرق لربط هذه المعارف بمواقف الحياة اليومية:

معارف الأمن السيبراني	طرق الربط بمواقف الحياة اليومية
مفهوم الأمن السيبراني
الجرائم الإلكترونية
الهجمات السيبرانية
عملية التشفير
فئات البرمجيات الضارة
أمن العتاد والبرمجيات

ورقة عمل (٢-١-١-١) 

خريطة البيت الدائري عن أحصنة طروادة

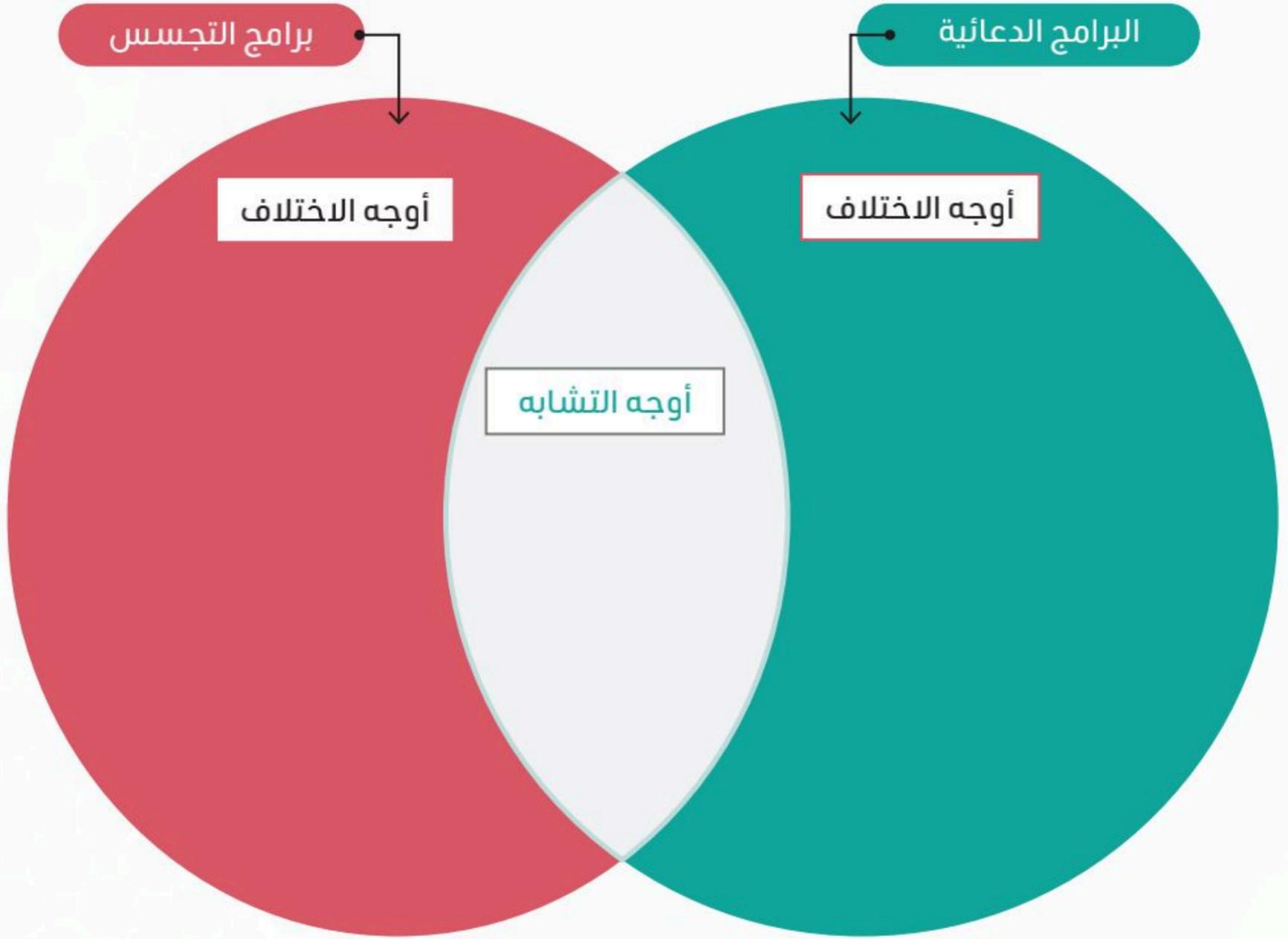
عزيزي المشارك، أمامك خريطة للبيت الدائري عن أحصنة طروادة، تعاون مع مجموعتك لاستكمال هذا المخطط.



ورقة عمل (٢-١-١-٢)

خريطة تفكير للمقارنة بين البرامج الدعائية وبرامج التجسس

عزيزي المشارك، أمامك خريطة تفكير (الفقاعة المزدوجة) للمقارنة بين البرامج الدعائية وبرامج التجسس، تعاون مع مجموعتك لاستكمال هذا المخطط.



مرفق (٢-١-١-١): اللعبة التعليمية

عزيزي المشارك، أمامك مجموعة من مجموعة من برامج والمواقع المختلفة تعاون مع مجموعتك حسب الفئة التي تنتمي إليها من البرمجيات الضارة

- ١) ماي دووم (.....)
- ٢) زيوس (.....)
- ٣) واناكراي (.....)
- ٤) قاتور (.....)
- ٥) كول ويب سيرش (.....)

ورقة العمل (٢-١-٢-١)

أدوات تحديد مخاطر الأمن السيبراني

عزيزي المشارك ، أمامك جدول يوضح أدوات تحديد مخاطر الأمن السيبراني وتقليلها وإدارتها، تعاون مع مجموعتك لاستكمال الجدول ووصف كل أداة

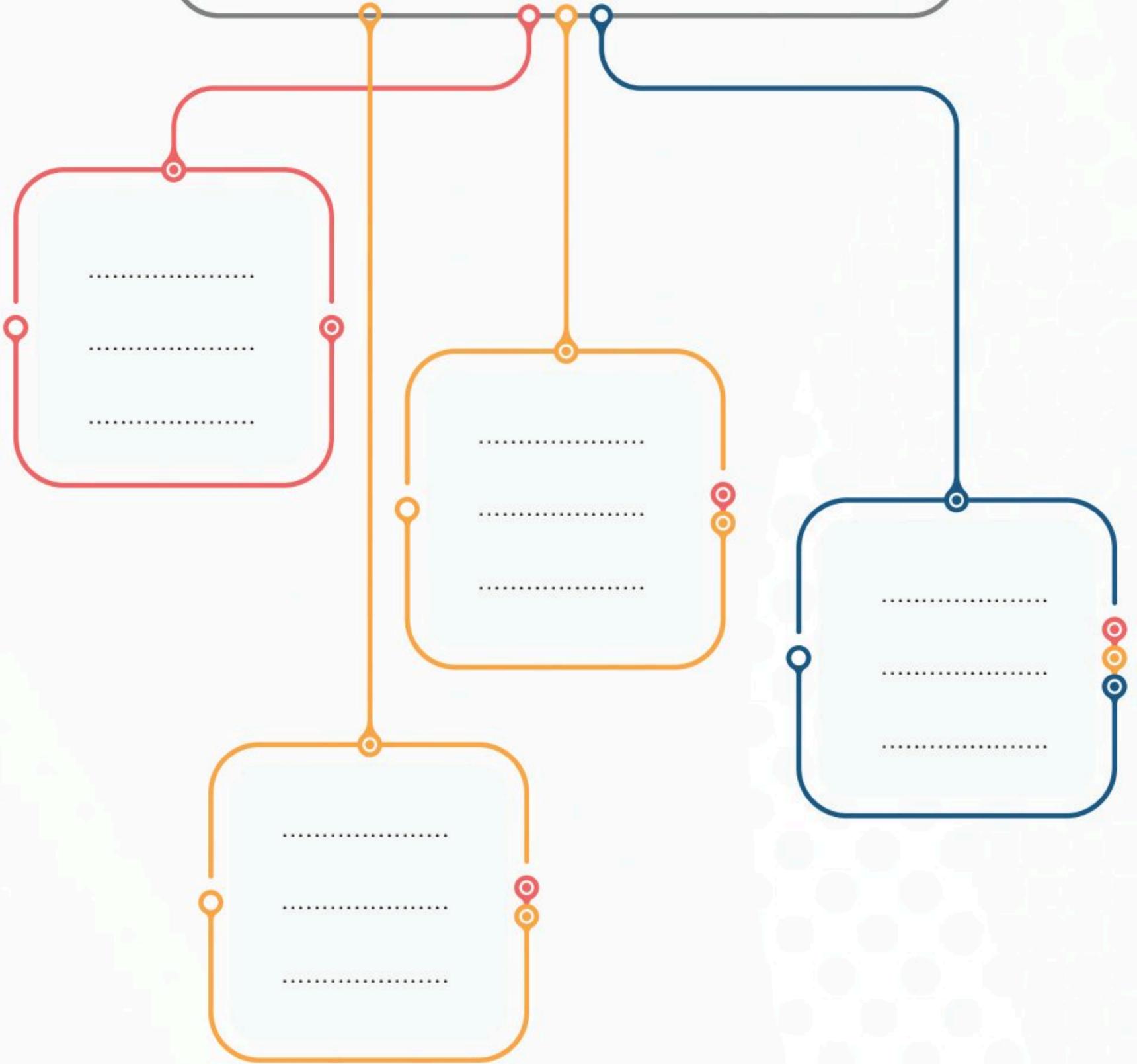
الوصف	الأداة
.....	نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني
.....	أدوات اختبار الاختراق
.....	تقييم المخاطر الأمنية
.....	منع فقدان البيانات
.....	جدار الحماية ونظام الحماية من الاختراق
.....	حماية النقطة الطرفية

ورقة العمل (٢-١-٢-٢) 

إستراتيجيات إدارة مخاطر الأمن السيبراني

عزيزي المشارك ، أمامك مخطط يوضح أدوات تحديد مخاطر الأمن السيبراني وتقليلها وإدارتها، تعاون مع مجموعتك لاستكمال هذا المخطط

إستراتيجيات إدارة مخاطر الأمن السيبراني

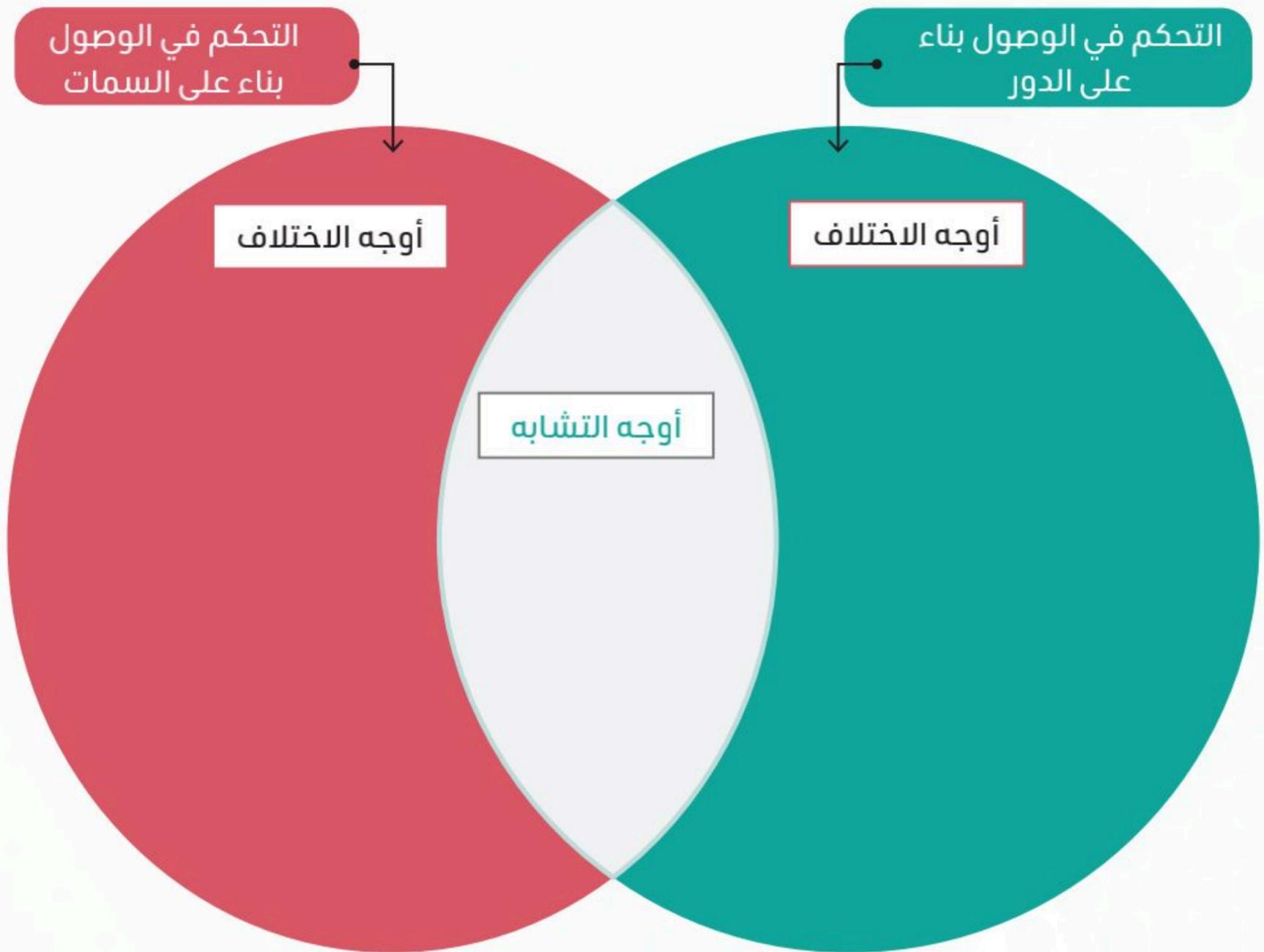


ورقة العمل (٢-١-٣-١)

المقارنة بين التحكم في الوصول بناء على الدور والتحكم

في الوصول بناء على السمات

عزيزي المشارك ، أمامك خريطة الفقاعة المزدوجة لاستنتاج أوجه الشبه والاختلاف بين كل من التحكم في الوصول بناء على الدور والتحكم في الوصول بناء على السمات، تعاون مع مجموعتك لاستكمال هذه الخريطة



ورقة عمل (٢-٢-٤-١)

التحديات التي تواجه أمن العتاد

عزيزي المشارك أمامك منظم تخطيطي يتضمن منظم تخطيطي يوضح أهم التحديات التي تواجه أمن العتاد، تعاون مع مجموعتك لوصف كل تهديد من هذه التحديات .

المكونات المزيفة

.....
.....
.....
.....

الهجمات المادية

.....
.....
.....
.....

هجمات القنوات الجانبية

.....
.....
.....
.....

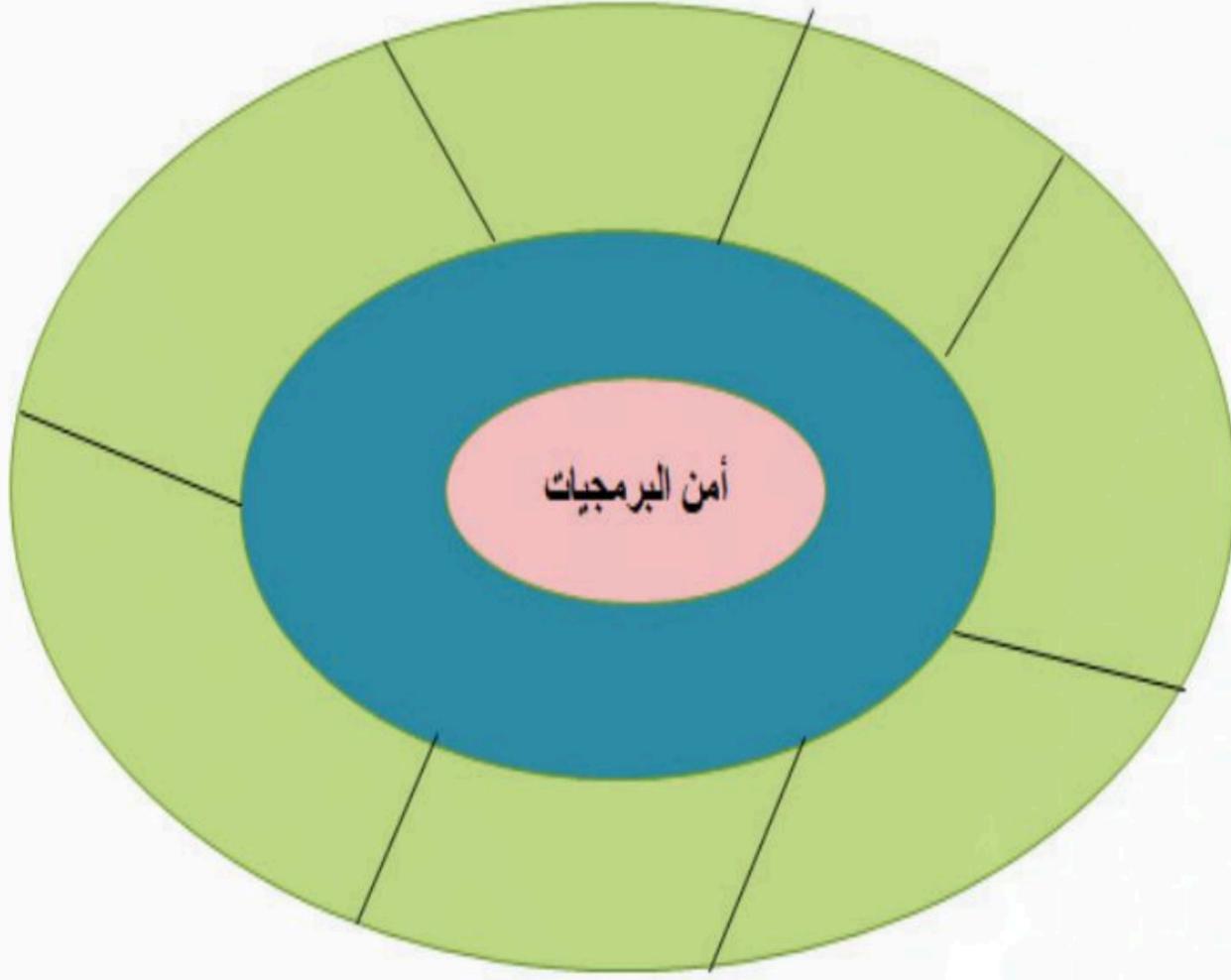
أحصنة طروادة العتادية

.....
.....
.....
.....

ورقة العمل (٢-٢-٤-٢)

البيت الدائري عن مفهوم أمن البرمجيات

عزيزي المشارك ، تعاون مع زملائك لاستكمال مخطط البيت الدائري عن مفهوم أمن البرمجيات



ورقة عمل (٢-٢-٤-٣)

التحديات التي تواجه أمن البرمجيات

عزيزي المشارك أمامك منظم تخطيطي يتضمن منظم تخطيطي يوضح أهم التحديات التي تواجه أمن البرمجيات، تعاون مع مجموعتك لوصف كل تهديد من هذه التحديات .

تجاوزات سعة المخزن المؤقت	البرمجيات الضارة	الباب الخلفي	استغلال الثغرات الأمنية
.....
.....
.....
.....

ورقة عمل (٢-٢-٥-١)

نموذج فراير عن مبدأ الأمن من خلال التصميم

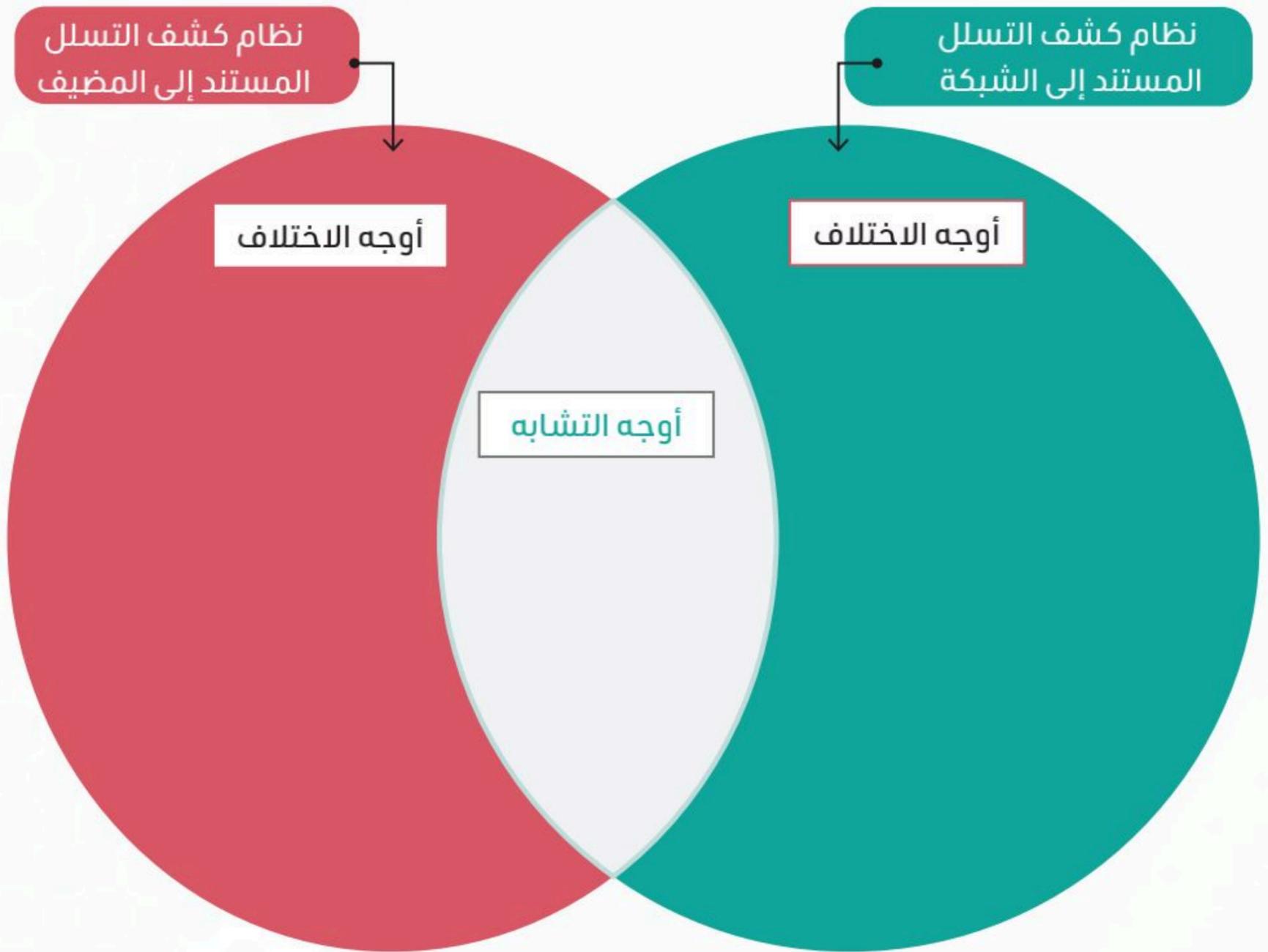
عزيزي المشارك أمامك نموذج فراير عن مبدأ الأمن من خلال التصميم، تعاون مع مجموعتك لاستكمال هذا النموذج بالبيانات المطلوبة

<h3>السمات</h3> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p>	<h3>التعريف</h3> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p>
<h3>الأمثلة</h3> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p>	<h3>الأمثلة</h3> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p>

مبدأ الأمن من خلال التصميم

المقارنة بين نظام كشف التسلل المستند إلى الشبكة ونظام كشف التسلل المستند إلى المضيف

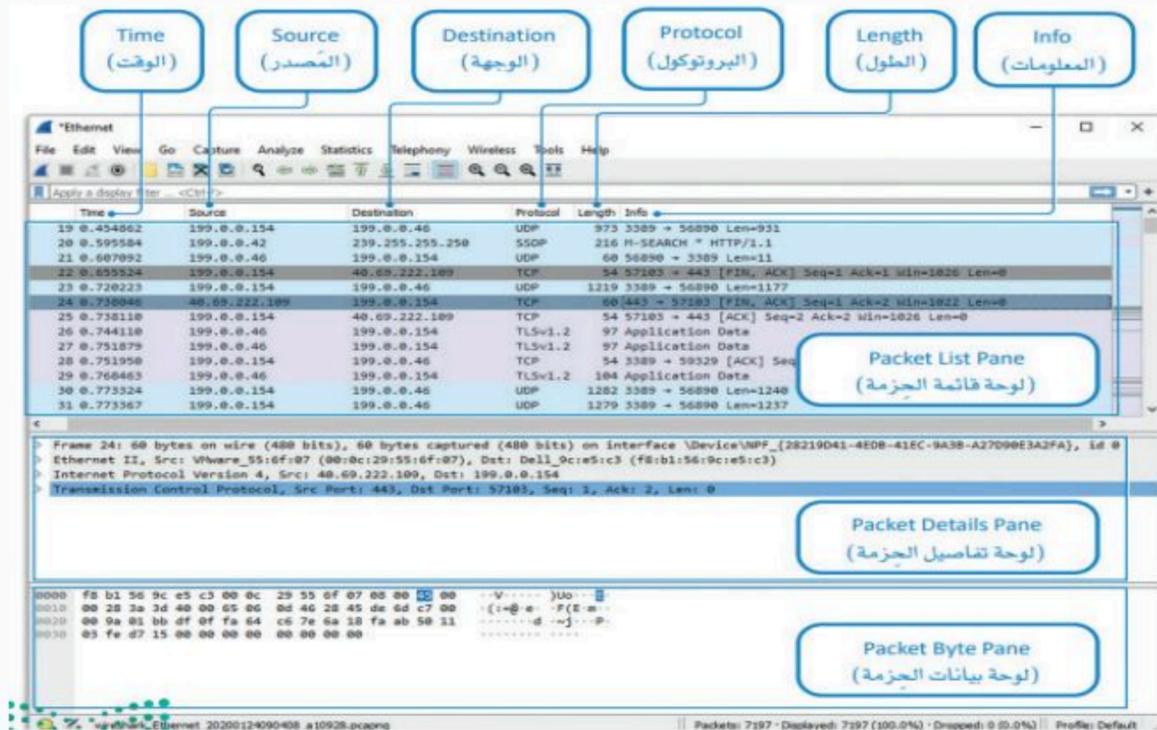
عزيزي المشارك، أمامك خريطة الفقاعة المزدوجة للمقارنة بين نظام كشف التسلل المستند إلى الشبكة ونظام كشف التسلل المستند إلى المضيف، تعاون مع مجموعتك لاستكمال هذه الخريطة .



لوحة قائمة الحزمة و لوحة تفاصيل الحزمة و لوحة بيانات الحزمة

عزيزي المشارك أمامك صور لوحة قائمة الحزمة و لوحة تفاصيل الحزمة و لوحة بيانات الحزمة و يطلب من المشاركين التعاون معًا لوصف كل صورة وتحديد عناصرها الأساسية

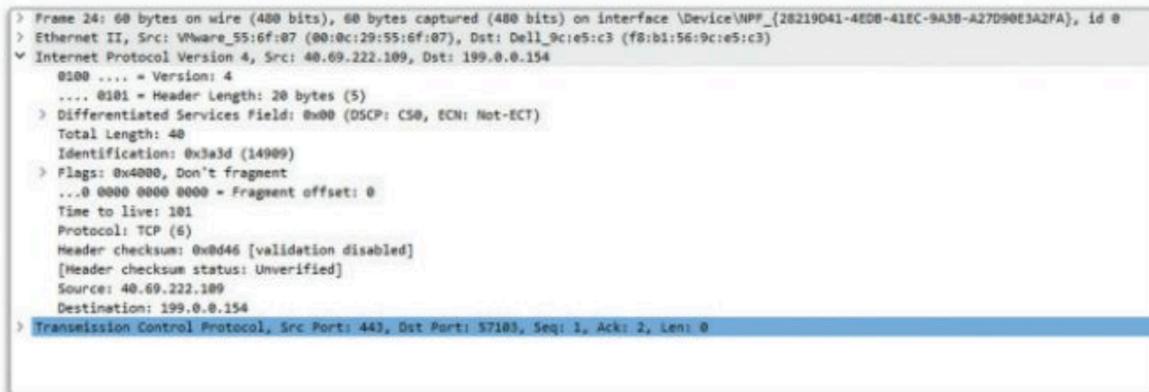
أولاً . لوحة قائمة الحزمة



The screenshot displays the Wireshark interface with three main panes highlighted by callouts:

- Time (الوقت)**: Points to the 'Time' column in the Packet List Pane.
- Source (المصدر)**: Points to the 'Source' column in the Packet List Pane.
- Destination (الوجهة)**: Points to the 'Destination' column in the Packet List Pane.
- Protocol (البروتوكول)**: Points to the 'Protocol' column in the Packet List Pane.
- Length (المطول)**: Points to the 'Length' column in the Packet List Pane.
- Info (المعلومات)**: Points to the 'Info' column in the Packet List Pane.
- Packet List Pane (لوحة قائمة الحزمة)**: Points to the table of captured packets.
- Packet Details Pane (لوحة تفاصيل الحزمة)**: Points to the hierarchical view of the selected packet's structure.
- Packet Byte Pane (لوحة بيانات الحزمة)**: Points to the raw byte representation of the packet.

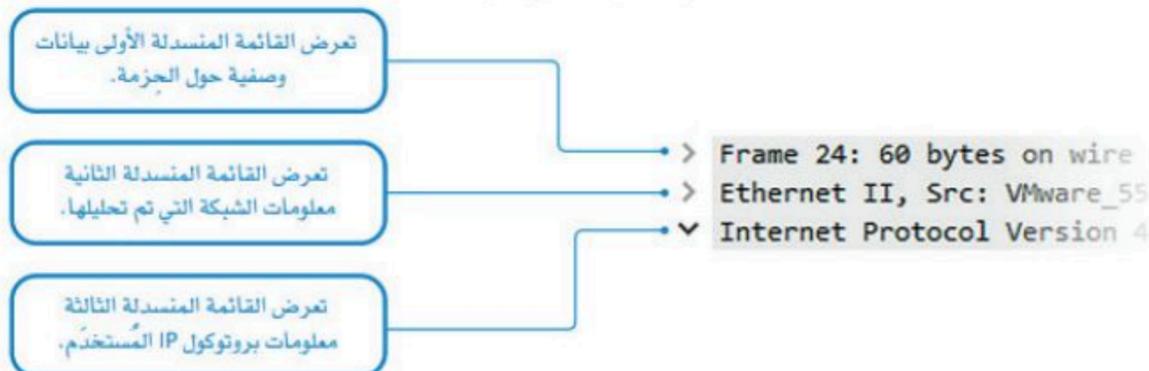
ثانيًا لوحة تفاصيل الحزمة



The screenshot shows the expanded details of Frame 24, highlighting the IP header fields:

- Frame 24: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{28219D41-4E0B-41EC-9A3B-A27D90E3A2FA}, id 0
- Ethernet II, Src: VMware_55:6f:07 (00:0c:29:55:6f:07), Dst: Dell_9c:e5:c3 (f8:b1:56:9c:e5:c3)
- Internet Protocol Version 4, Src: 40.69.222.109, Dst: 199.0.0.154
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 40
 - Identification: 0x3a3d (14989)
 - Flags: 0x4000, Don't fragment
 - ...0 0000 0000 0000 = Fragment offset: 0
 - Time to live: 101
 - Protocol: TCP (6)
 - Header checksum: 0x0d46 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 40.69.222.109
 - Destination: 199.0.0.154
- Transmission Control Protocol, Src Port: 443, Dst Port: 57103, Seq: 1, Ack: 2, Len: 0

شكل 2.11: لوحة تفاصيل الحزمة



The diagram illustrates the relationship between the callout boxes and the Packet Details Pane:

- عرض القائمة المنسدلة الأولى بيانات وصفية حول الحزمة.** (Display the first expanded list data descriptive about the packet.) - Points to the IP header.
- عرض القائمة المنسدلة الثانية معلومات الشبكة التي تم تحليلها.** (Display the second expanded list network information that has been analyzed.) - Points to the Ethernet II header.
- عرض القائمة المنسدلة الثالثة معلومات بروتوكول IP المستخدم.** (Display the third expanded list IP protocol information used.) - Points to the TCP header.

ثالثًا: لوحة بيانات الحزمة



The screenshot shows the raw byte representation of the packet:

```

0000 f8 b1 56 9c e5 c3 00 0c 29 55 6f 07 08 00 45 00  ..V...Uo...E
0010 00 28 3a 3d 40 00 65 06 0d 46 28 45 de 6d c7 00  .(:@e.F(E.m.
0020 00 9a 01 bb df 0f fa 64 c6 7e 6a 18 fa ab 50 11  .....d~j...P
0030 03 fe d7 15 00 00 00 00 00 00 00 00
    
```

مرفق (٢-٤-٢-٣): كشف نشاط مريب على الشبكة

لكشف طلبات بروتوكول اقتران العناوين (ARP)

< من علامة تبويب Edit (تحرير)، اضغط على 1
Preferences (التفضيلات). 2

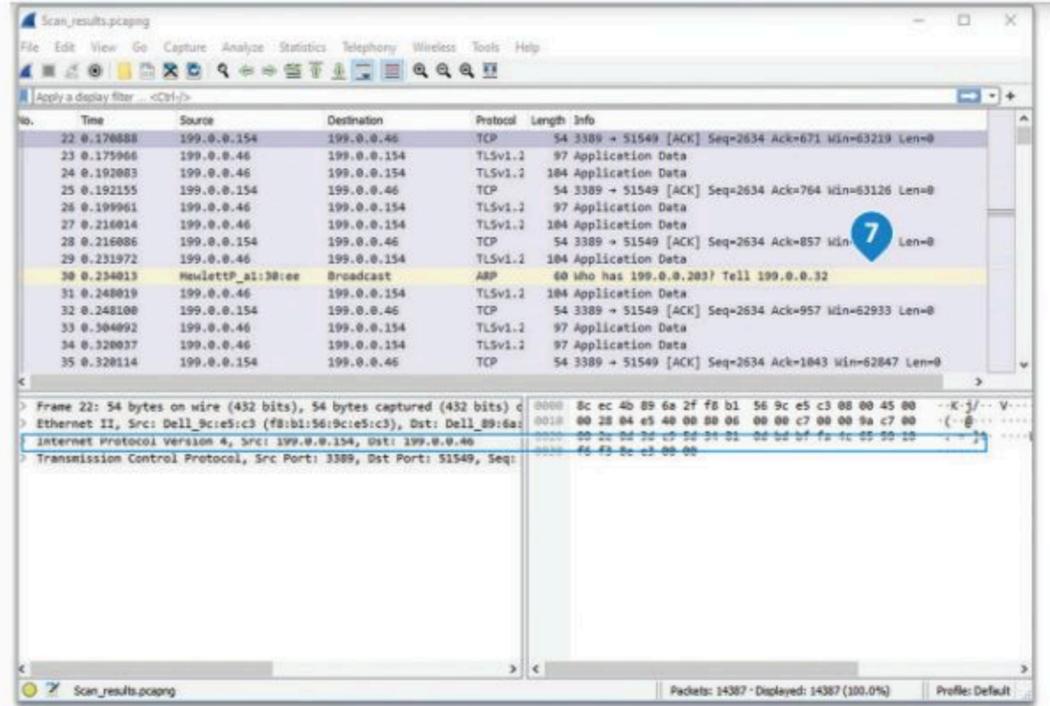
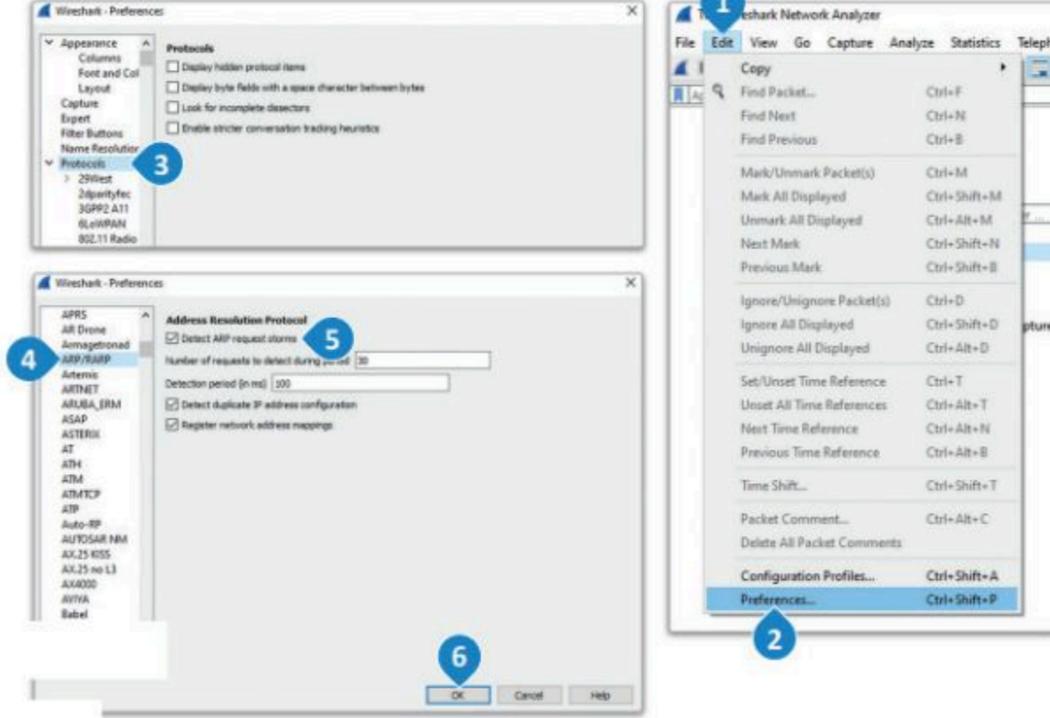
< من نافذة Preferences (التفضيلات)، اختر خيار 3
Protocols (البروتوكولات).

< اختر بروتوكول ARP/RARP (بروتوكول اقتران العناوين/
بروتوكول اقتران العناوين العكسي). 4

< حدد صندوق Detect ARP request storms (اكتشاف
طلبات بروتوكول اقتران العناوين). 5

< اضغط على OK (موافق). 6

< يمكنك من لوحة Packet List (قائمة الحزمة) التحقق من
وجود نشاط مريب. 7



No.	Time	Source	Destination	Protocol	Length	Info
22	0.176888	199.0.0.154	199.0.0.46	TCP	54	3389 → 51549 [ACK] Seq=2634 Ack=671 Win=63219 Len=0
23	0.175966	199.0.0.46	199.0.0.154	TLSv1.2	97	Application Data
24	0.192083	199.0.0.46	199.0.0.154	TLSv1.2	104	Application Data
25	0.192155	199.0.0.154	199.0.0.46	TCP	54	3389 → 51549 [ACK] Seq=2634 Ack=764 Win=63126 Len=0
26	0.199961	199.0.0.46	199.0.0.154	TLSv1.2	97	Application Data
27	0.216014	199.0.0.46	199.0.0.154	TLSv1.2	104	Application Data
28	0.216006	199.0.0.154	199.0.0.46	TCP	54	3389 → 51549 [ACK] Seq=2634 Ack=857 Win=0 Len=0
29	0.231972	199.0.0.46	199.0.0.154	TLSv1.2	104	Application Data
30	0.234013	HewlettP_a1:30:ee	Broadcast	ARP	60	who has 199.0.0.203? Tell 199.0.0.32
31	0.248019	199.0.0.46	199.0.0.154	TLSv1.2	104	Application Data
32	0.248100	199.0.0.154	199.0.0.46	TCP	54	3389 → 51549 [ACK] Seq=2634 Ack=957 Win=62933 Len=0
33	0.304092	199.0.0.46	199.0.0.154	TLSv1.2	97	Application Data
34	0.320037	199.0.0.46	199.0.0.154	TLSv1.2	97	Application Data
35	0.320114	199.0.0.154	199.0.0.46	TCP	54	3389 → 51549 [ACK] Seq=2634 Ack=1043 Win=62647 Len=0



قد يحاول شخص اكتشاف ما إذا كان عنوان بروتوكول الإنترنت 199.0.0.203 قيد الاستخدام.

ورقة العمل (٣-٢-٦-١)

توظيف التقنيات التعليمية الحديثة

من خلال دراستك للشكل الذي أمامك اكتب كيف يمكنك توظيفها من خلال مقرر التصميم

الهندسي:



ورقة العمل (٤-١-١-١)

خطوات عملية التحليل الجنائي الرقمي

عزيزي المشارك في ضوء دراستك للنشرة السابقة تعاون مع مجموعتك لاستكمال المنظم تخطيطي لخطوات عملية التحليل الجنائي الرقمي،

.....

.....

.....

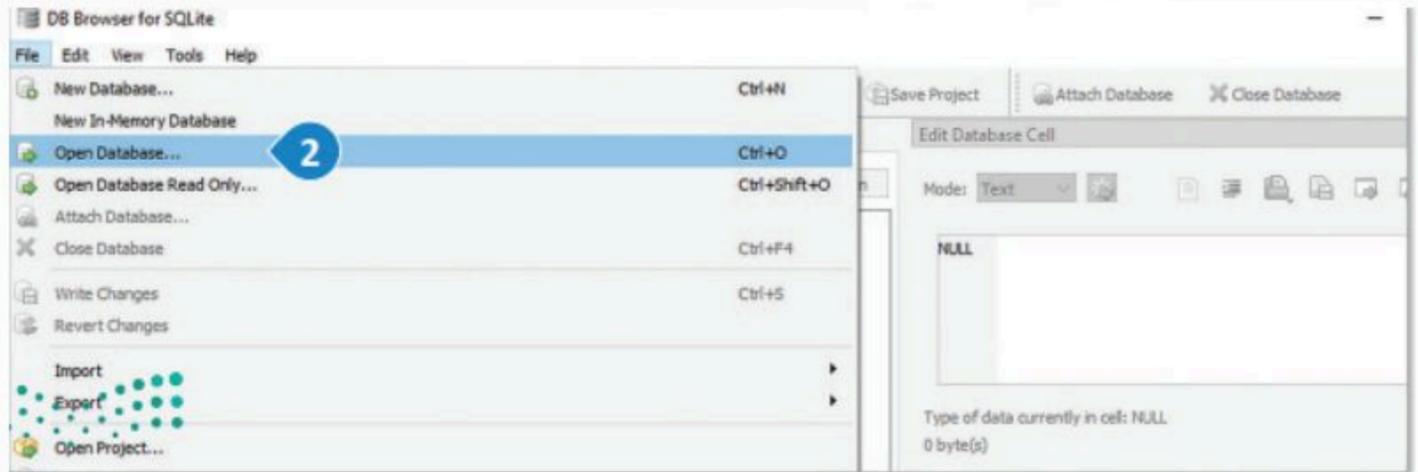
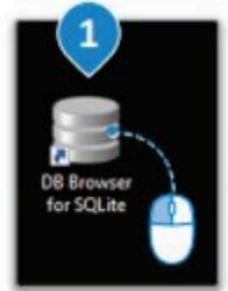
.....

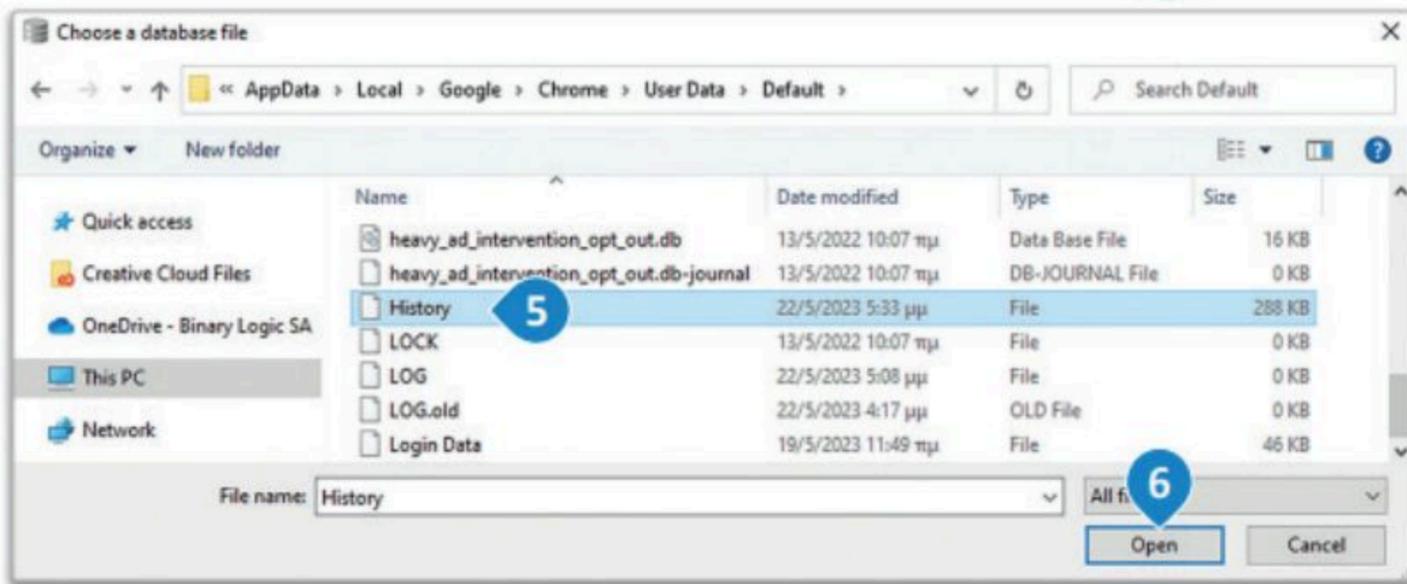
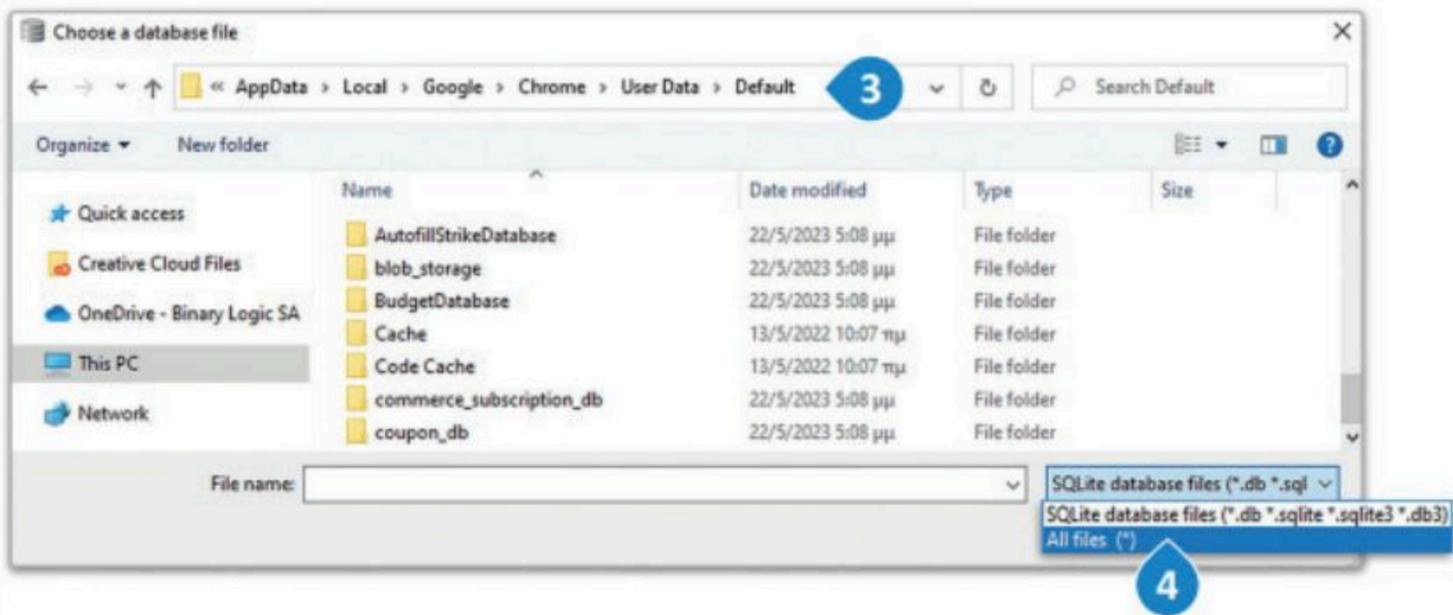
.....

.....

مرفق (٤-١-١-١): خطوات أنشطة الويب على الجهاز باستخدام برنامج متصفح دي بي إس كيو لايت DB Browser for SQLite

- افتح متصفح دي بي وتحميل ملف السجل،
- 1 < اضغط ضغطاً مزدوجاً على اختصار DB Browser (متصفح دي بي) من سطح المكتب.
 - 2 < اضغط على File (ملف) < Open Database... (فتح قاعدة بيانات...).
 - 3 < أدخل: "C:\Users\[username]\AppData\Local\Google\Chrome\User Data\Default" في مسار الموقع، وفي حقل [username] اسم المستخدم أدخل اسم مستخدم الحاسب.
 - 4 < اختر (*) All files (كافة الملفات) من القائمة المنسدلة.
 - 5 < اضغط على History (المحفوظات)، 5 لاختيار ملف سجل المحفوظات، ثم اضغط على Open (فتح).
 - 6

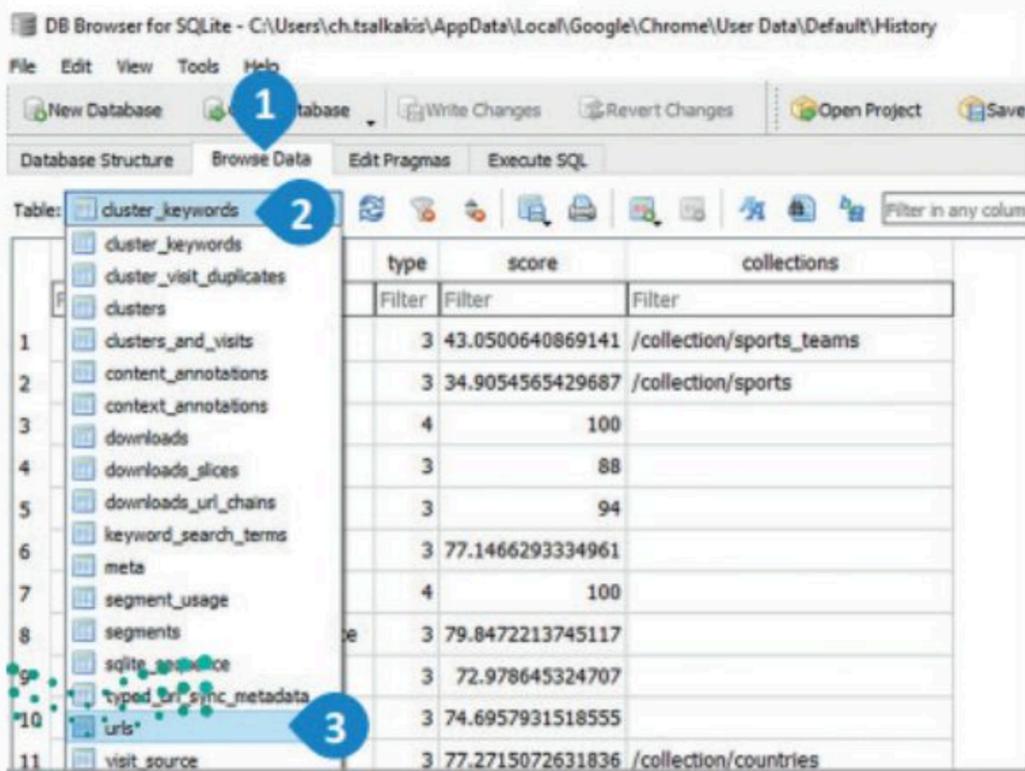




لعرض جدول:

1 < اضغط على علامة تبويب
Browse Data (تصفح
البيانات).

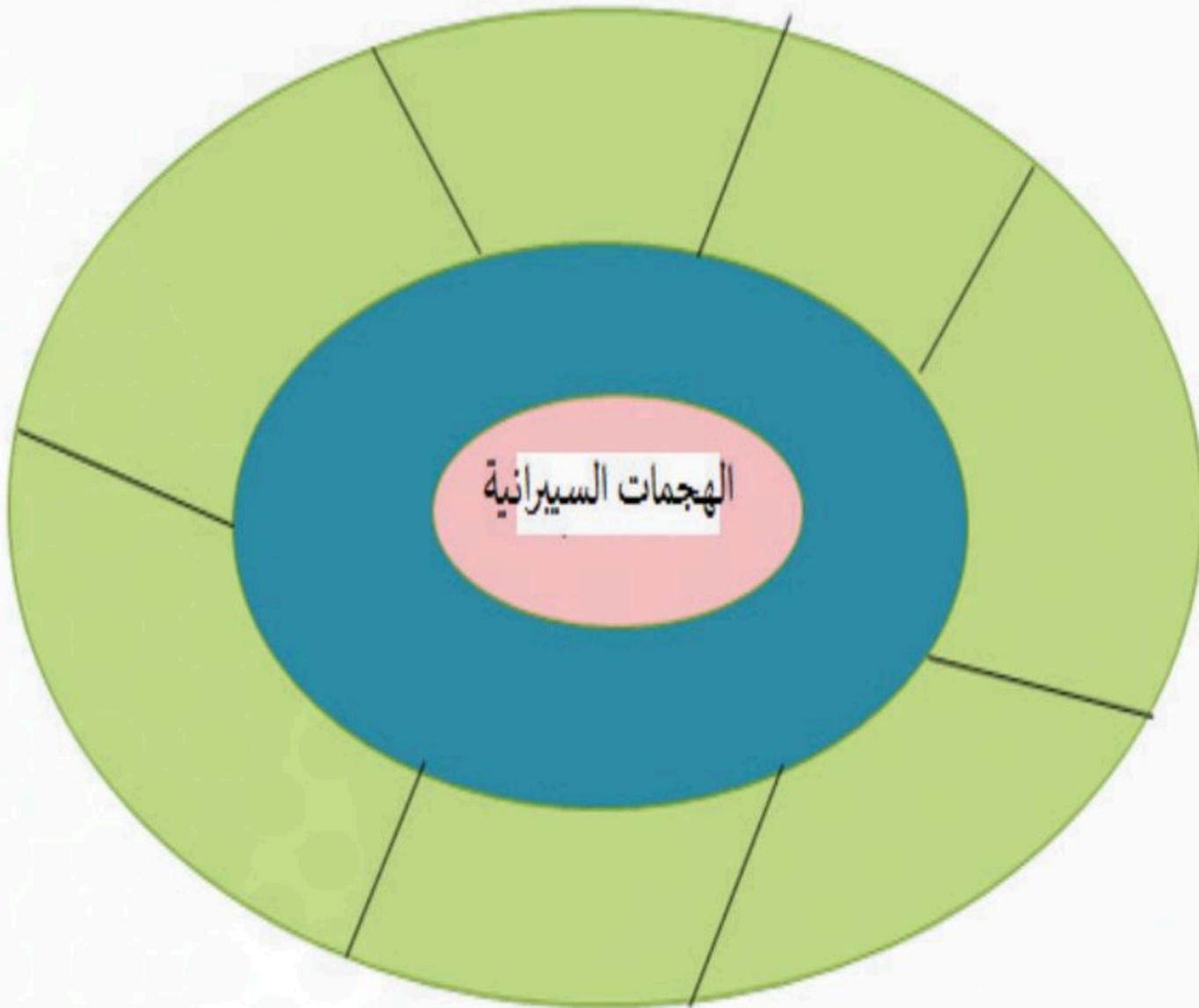
2 < اضغط على القائمة المنسدلة،
ثم اختر urls (مُحدّات موقع
الموارد المُوحّد) لعرض جدول
عناوين urls.



ورقة العمل (٤-١-٣-١)

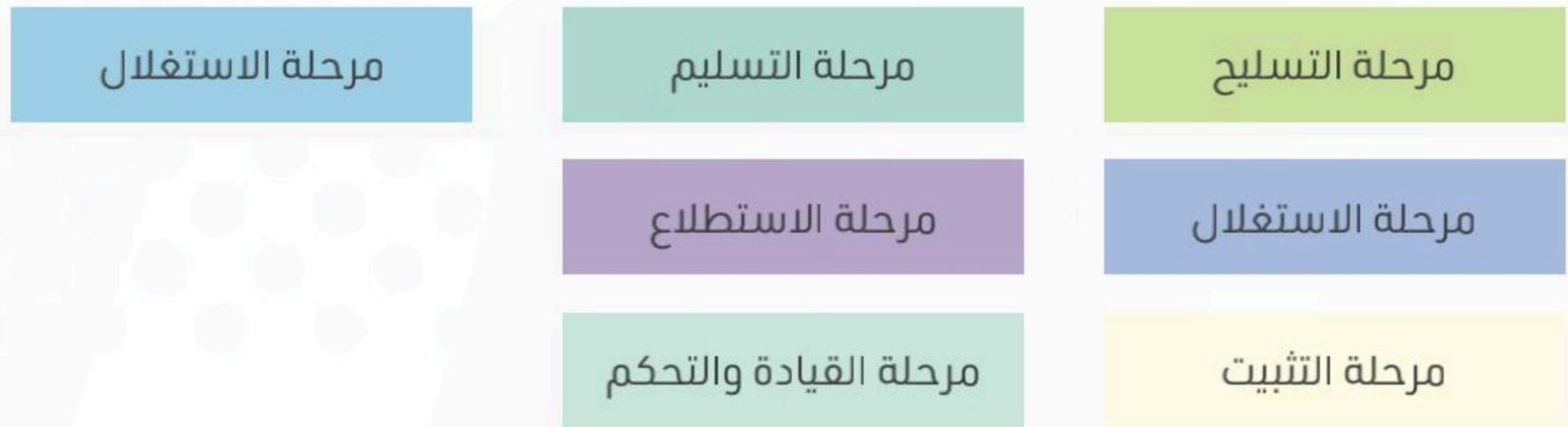
الهجمات السيبرانية

عزيزي المشارك أمامك مخطط البيت الدائري عن الهجمات السيبرانية، في ضوء ما تعلمته تعاون مع مجموعتك لاستكمال هذا المخطط.



مرفق (٤-١-٣-١): لعبة تعليمية عن مراحل سلسلة الهجوم السيبراني

عزيزي المشارك أمامك مجموعة من الكروت بها مراحل سلسلة الهجوم السيبراني، تعاون مع مجموعتك لترتيب هذه المراحل



الاستطلاع- التسليح- التسليم - الاستغلال- التثبيت- القيادة والتحكم - تحقيق الأهداف

ورقة العمل (٤-١-٤-١) 

القرصنة الأخلاقية

عزيزي المشارك أمامك مخطط تنظيمي عن أهم الجوانب الحاسمة للحفاظ على التوازن والموضوعية فيما يتعلق بالقرصنة الأخلاقية. تعاون مع مجموعتك لاستكمال هذا المخطط .

الإذن والتفويض

.....
.....
.....
.....

الامتثال القانوني والتنظيمي

.....
.....
.....
.....

الإفصاح والمعالجة

.....
.....
.....
.....

الاحترافية والمسؤولية

.....
.....
.....
.....

ورقة العمل (٤-٢-٥-١) 

علم التشفير وخصائصه

عزيزي المشارك أمامك نموذج فراير عن علم التشفير تعاون مع مجموعتك لاستكمال النموذج

عناصرها	التعريف
الخصائص	الأمثلة

علم التشفير

ورقة العمل (٤-٢-٥-١) علم التشفير وخصائصه

عزيزي المشارك في ضوء ما عرضه عليك مدربك عن أنواع التشفير، تعاون مع مجموعتك لاستكمال خريطة الفقاعة المزدوجة للمقارنة بين تشفير المفتاح المتماثل وتشفير المفتاح غير المتماثل

