الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

academy.ncsa.gov.qa

مرحباً بكم

في عالم إلكتروني
أكثر أماناً ..

كيفية استخدام هذا الكتيّب؟

تم تصميم هذا الكتيب **لصالح الوكالة الوطنية للأمن السيبراني في قطر** لإلهام الشباب وزيادة اهتمامهم في مجال الأمن السيبراني.

تم استخراج محتويات هذا الكتيب من موقع **Tryhackme.com** وتتضمن حقائق ممتعة من وقت لآخر. يمتلئ الكتيب بالعديد من الأنشطة الممتعة التي ستساعد المشارك في فهم المفاهيم الأكثر تعقيدًا بسهولة.

يُستخدم هذا الكتاب كدليلٍ تكميلي للمخيمات التدريبية الحضورية المقامة في الدوحة، قطر، وليس مخصصًا للتعلّم الذاتي.

لنبدأ
الرحلة

مقدمة في الأمن السيبراني

تخيّل عالماً تكون فيه أنت حارس الكنز السري، تدافع عنه من لصوص مخادعين. هذا هو الأمن السيبراني، هو مغامرة ممتعة في حماية الحواسيب والشبكات والبيانات من المخترقين والأشرار الرقميين. ستتعلم تقنيات رائعة لاكتشاف التهديدات وكيفية الحفاظ على أمان معلوماتك وحتى كيفية التفوق على المجرمين السيبرانيين.

فاستعد للغوص في عالم مثير حيث ستصبح بطلاً للإنترنت.

هل تعلم؟

أن **أكتوبر** هو شهر التوعية الوطنية بالأمن السيبراني و يخصَّص لإعلان التوعية عن أهمية الأمن السيبراني

أكمل لعبة الكلمات المتقاطعة التالية (الإجابات باللغة الانجليزية)

الأفقي

2. النظام الأمني الذي يتحكم في حركة المرور الواردة و الصادرة عبر الشبكة استنادا إلى قواعد الأمن المحددة مسبقاً.

5. البرمجية الخبيثة التي تكرر نفسها و تنتشر لتلحق ضرراً بالأنظمة و البيانات.

6. الاستغلال المُتعمد لأنظمة الحاسوب و الشبكات و الأجهزة.

8. عملية تشفير البيانات لمنع الوصول غير المصرح به، مما يضمن الخصوصية والأمان.

9. تحديث لإصلاح الثغرات الأمنية أو تحسين الأداء الوظيفي في البرمجيات أو الأنظمة.

10. الوصول غير المصرح به إلى أنظمة الحاسوب أو الشبكات أو التلاعب بها.

الرأسي

1. برمجيات خبيثة مُصممة لتعطيل أو إتلاف أو الوصول غير المصرح به إلى الأنظمة أو البيانات.

3. البرمجية الخبيثة التي تقوم بتشفير الملفات وتطالب بالدفع مقابل فك التشفير.

4. حماية البيانات الشخصية من الوصول غير المصرح به او الكشف عنها.

7. المحاولات الخادعة للحصول على معلومات حساسة، غالباً من خلال الاتصالات الاحتيالية.

حماية
قلعتنا الرقمية

نحتاج دعمك لحماية قلعتنا!

اكتب قائمة بكل ما تراه في هذه الصورة

لنتخيل الآن هذه الصورة كعالم الإنترنت الرقمي الذي تعيش فيه...

عالمنا الرقمي مليء **بالأجهزة والمخازن**

تعتبر قلعة القرون الوسطى ذات الأبراج والجدران **حصناً لعالمنا الرقمي**

فرسان الفريق الأحمر
هم "الأعداء الودودون" وهم المخترقون الأخلاقيون الذين يطلقون هجمات محاكاة.

الشخصيات الغامضة
الكامنة خارج أسوار القلعة
هم "مجرمو الإنترنت"

فرسان الفريق الأزرق
هم "حراس الجدار" وهم محترفون في مجال الأمن السيبراني يدافعون عن القلعة

هل تعلم؟

أن المخترقين ليسوا جميعاً سيئين؟

هناك المخترقون الأخلاقيون والمعروفون أيضاً بـ**"المخترقين البيض"**

الذين يساعدون المؤسسات في العثور على الثغرات الأمنية وإصلاحها

مسارات وظيفية
في الأمن السيبراني

ملاءمة الوظائف السيبرانية

أي من الوظائف التالية تود أن تعمل بها يومًا ما؟

ظلل النجوم على الوظائف التي تهمك

المحلل الأمني

محلل الأمان هو المتخصص الذي يراقب الشبكات والأنظمة لاكتشاف محاولات الاختراق والأنشطة المشبوهة، ويحلل التهديدات والثغرات الأمنية، ويستجيب للحوادث الأمنية.

المهندس الأمني

يصمم ويبني مهندسو الأمن السيبراني جدرانًا وأبوابًا قوية لعالمنا الرقمي لمنع الأشرار من الدخول إليه. كما يستخدمون أدوات خاصة وخططًا ذكية للحفاظ على أمان الأنظمة الالكترونية.

مستجيب الحوادث

عندما تقع الهجمة السيبرانية، هؤلاء رجال الإطفاء الرقميون الذين ينطلقون إلى العمل و يحددون بسرعة ما حدث، كما يوقفون انتشار الأضرار، ويساعدون في إصلاح كل شيء بسرعة. إنهم كمن يلعبون لعبة سريعة حيث يحتاجون سرعة في التفكير واتخاذ القرار للحفاظ على الأمان.

محقق الأدلة الرقمية

هل تحب حل الألغاز والكشف عن الأسرار؟ تتعلق علوم الأدلة الجنائية الرقمية باستخدام أدوات خاصة لتتبع الأدلة والإمساك بمجرمي الإنترنت. يشبه هذا الدور أن تكون محققًا رقميًا في مهمة للحفاظ على أمان العالم عبر الإنترنت!

مختبر الاختراق (المخترق الأخلاقي)

المخترقون الأخلاقيون هم خبراء في الحاسوب يستخدمون مهاراتهم في الاختراق لأغراض الخير. إنهم كمحققين رقميين، يكتشفون الضعف في الأنظمة للحفاظ على سلامة معلومات الجميع من الأشرار.

محلل البرمجيات الضارة

تعرّف على محققي البرمجة في عالم الأمن السيبراني: محللو البرمجيات الضارة! هم يدرسون البرامج الحاسوبية الخبيثة، يحددون كيفية عملها وما تخطط لفعله. إنهم كمن يكشف لغزًا للقبض على المخربين الرقميين وللحفاظ على أمان أجهزتنا الحاسوبية.

رئيس أمن المعلومات (CISO)

يتولى رئيس أمن المعلومات (CISO) وضع الخطط لحماية أجهزة وأنظمة وبيانات المؤسسة، ويقود فريق الأمن السيبراني للحفاظ على سلامة المؤسسة. يشبه مدرب الفريق الرياضي؛ فهو يضع خطة الفوز ويقود الفريق لتحقيق النجاح.

أساسيات اللينيكس

أهلاً ! لينيكس هو مثل ساحة ألعاب رائعة للحواسيب. إنه نظام تشغيل خاص يمنح حاسوبك القدرة على تشغيل العديد من أنواع البرامج والألعاب المذهلة.

مثل صندوق أدوات سحري، يتيح لينيكس لك تخصيص حاسوبك وتعديله بطرق مذهلة. إنه كمن يحمل رمزًا سريًا لفتح مجالات لا حصر لها لحاسوبك.

لذا، إذا كنت تحب اكتشاف أشياء جديدة، فلينيكس هو أرض مغامراتك الرقمية الخاصة!

لينيكس هو نظام تشغيل رائع جداً، تماماً مثل ويندوز أو ماك او إس، لكنه مجاني ومفتوح المصدر! هذا يعني أنه يمكنك تحميله، استخدامه، وحتى وحتى القيام بتعديله إذا كنت تمتلك المعرفة اللازمة لذلك.

العديد من الخوادم وأجهزة الحواسيب الضخمة، وحتى هاتفك الذكي بنظام أندرويد، جميعهم يعملون بنظام لينكس. انتشرت شهرته لأنه آمن جداً ويمكن تخصيصه بشكل كبير.

إذا كنت تحب التلاعب بالتكنولوجيا وترغب في تعلم كيفية عمل الحواسيب بشكل حقيقي، لينكس يشبه ساحة ألعاب يمكنك فيها الاستكشاف والإبداع.

مهمّة

اختر كلمتين رائعتين عن لينيكس لفتتا انتباهك واكتبهما

تعرّف على
أبطال لينيكس

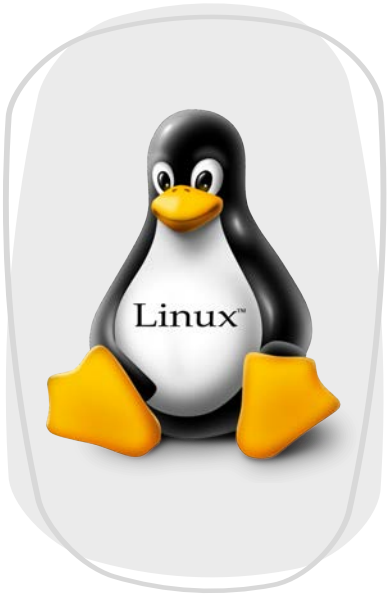
أوبونتو هو نظام تشغيل سهل الاستخدام من لينيكس ورائع للمبتدئين.
يشتهر بعملية التثبيت السهلة والدعم الكبير من المجتمع.
يمكنك استخدامه في كل شيء من تصفح الإنترنت إلى البرمجة وتشغيل الخوادم.

فيدورا هو نظام تشغيل متطور من لينيكس يوفر أحدث الميزات والتقنيات.
إنه رائع للمطورين وهواة التكنولوجيا الذين يرغبون في تجربة أحدث البرامج.
يشتهر فيدورا أيضاً بميزاته الأمنية القوية.

ديبيان هو نظام تشغيل مستقر وموثوق من لينيكس، ويعتبر الأساس للعديد من التوزيعات الأخرى، بما في ذلك أوبونتو.
يشتهر بقوته ويستخدم غالباً للخوادم.
إنه أكثر تقنية ولكنه قابل للتخصيص بشكل كبير.

سينت أو إس هو نظام تشغيل لينيكس من فئة المؤسسات وهو مجاني، يُستخدم غالباً للخوادم.
يشتهر باستقراره ودعمه طويل الأمد، مما يجعله خياراً شائعًا للشركات وخوادم استضافة الويب.
يعتمد على نظام ريد هات إنتربرايز لينيكس.

أوامر
لينيكس



أوامر لينيكس هي تعليمات بسيطة تعطيها لحاسوبك لجعله ينفذ بعض المهام. تمامًا مثل استخدام الاختصارات على لوحة المفاتيح، تتيح لك هذه الأوامر العثور على الملفات، والتنقل في المجلدات، وتشغيل البرامج.

إنها تشبه قليلاً التحدث بلغة سرية تجعل حاسوبك يستمع ويستجيب. تعلم هذه الأوامر سيساعدك على أن تصبح محترفًافي التنقل داخل نظام لينكس واستخدامه.

دعنا نبدأ ونرى مدى قوة هذه الكلمات الصغيرة!

هل تعلم؟

العديد من أوامر لينيكس تعود أصولها إلى نظام التشغيل يونيكس الذي تم تطويره في السبعينيات.

لقد تطورت بمرور الوقت لكنها لا تزال تحتفظ بوظائفها الأساسية.

الأصداء والهويات

اكتشف أساسيات أوامر لينيكس

باستخدام **echo** لإرسال الرسائل وَ **whoami** لمعرفة الهوية على حاسوبك.

هذه هي خطواتك الأولى في عالم الأوامر الأساسية.

whoami

هذا الأمر يساعدك في اكتشاف
من هو المستخدم الحالي للنظام
كأنك تنظر في المرآة

Echo

ببساطة يكرر كل ما تكتبه بعده.
إنه مثل أن تصرخ في الوادي
فتسمع صداك يرجع إليك.

```
tryhackme@linux1:~$ whoami
tryhackme
```

```
tryhackme@linux1:~$ echo "Hello World!"
"Hello World!"
```

مهمّة

إذا أردنا أن نرى النص"LinuxIsFun" فماذا سيكون الأمر؟

ماذا يوجد
في نظام الملفات؟

الآن لنغص في كيفية اكتشاف و إدارة مجلدات
حاسوبك و ملفاته باستخدام الأوامر السهلة.
كن مستعداً لإدارة محيطك الرقمي كمحترف.

ls (listing)

يستخدم هذا الأمر لعرض محتويات المجلد الحالي
والذي قد يتضمن عددا من الملفات والمجلدات بداخله

```
tryhackme@linux1:~$ ls
access.log  folder1  folder2  folder3  folder4
```

cd (تغيير المجلد)

هذا الأمر يتيح لك التنقل بين المجلدات المختلفة.
إنه مثل الانتقال الفوري إلى مواقع مختلفة في لعبة فيديو !!!

```
tryhackme@linux1:~$ cd folder4
tryhackme@linux1:~/folder4$ ls
note.txt
```

ماذا يوجد في نظام الملفات؟

cat (الدمج و عرض محتويات الملف)

هذا الأمر يعرض محتويات الملف. مثل فتح كتاب وقراءة المكتوب داخله

```
tryhackme@linux1:~/folder4$ ls
note.txt
tryhackme@linux1:~/folder4$ cat note.txt
Hello World!
```

pwd (طباعة المجلد الحالي)

هذا الأمر يخبرك بالمسار الكامل لموقعك الحالي في نظام الملفات.
إنه مثل استخدام نظام تحديد المواقع العالمي للعثور على طريقك !!!

```
tryhackme@linux1:~/folder4$ pwd
/home/tryhackme/folder4
tryhackme@linux1:~/folder4$
```

أسرار مخفيّة

بعض أوامر لينيكس تحتوي على أسرار مخفية
أو استجابات غريبة بغض النظر عن المدخلات التي تقوم بإدخالها.
جرب الأمر `apt-get moo` فستفاجأ!

البحث
عن الملفات

اكتشف كيفية البحث عن عناصر معينة واكتشافها
في الكنز الرقمي لجهاز الكمبيوتر الخاص بك.

Find

يتيح لك العثور على الملفات بأسمائها أو أنواعها أو معايير أخرى.
إنه مثل امتلاك كلب بحث يعثر على الملف الذي تريده

```
tryhackme@linux1:~$ find -name note.txt
./folder4/note.txt
tryhackme@linux1:~$
```

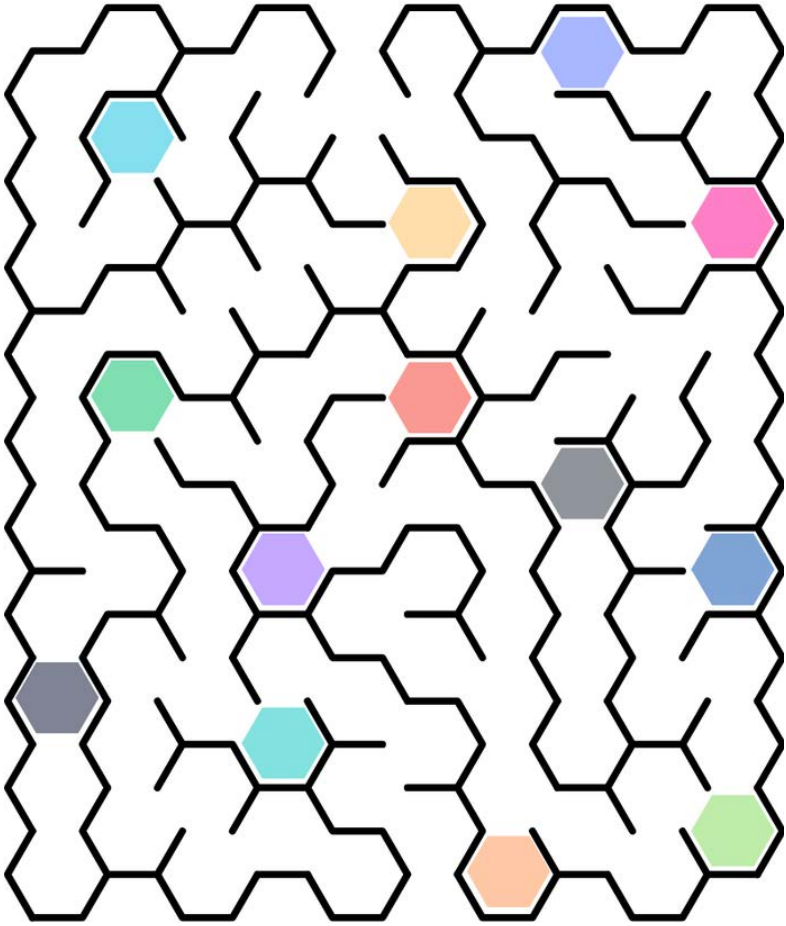
Grep

هذا الأمر يتيح لك البحث عن كلمات محددة داخل الملفات.
إنه مثل استخدام كاشف المعادن للعثور على الكنوز المخفية في الرمال!

```
tryhackme@linux1:~$ grep "81.143.211.90" access.log
81.143.211.90 - - [25/Mar/2021:11:17 + 0000] "GET / HTTP/1.1" 200 417
"-" "Mozilla/5.0 (Linux; Android 7.0; Moto G(4))"
tryhackme@linux1:~$
```

متاهة الاكتشاف

أنت في عالم رقمي غامض حيث تكون الملفات والمجلدات مخفية! تنقل عبر المتاهة للعثور على جميع الملفات والمجلدات المخفية في طريقك .



مهمَّة

على كم عثرت؟

مساعدة:

السداسيات الملونة على المسار الصحيح هي فقط الملفات والمجلدات المخفية. أما البقية فهي مجرد سداسيات!

أوامر
العميل السريّ

تعلم كيفية استخدام الأدوات المتخصصة لتنفيذ الأوامر بشكل سري وإدارة البيانات بفعالية في عملياتك الرقمية! اغمر نفسك في عالم واجهة الأوامر حيث لكل رمز غرض فريد، **مما يعزز تحكمك في المهام الحاسوبية.**

& (الخلفية)

هذا الرمز يتيح لك تشغيل الأوامر في الخلفية، بحيث يمكنك الاستمرار في استخدام سطر الأوامر لأداء مهام أخرى. إنه يشـــبه الحصول على قوة خارقة لتنفيذ المهام المتعددة!

```
tryhackme@linux1:~$ sleep 20 &
[1] 3124
tryhackme@linux1:~$
[1]+ Done sleep 20
```

المشغل "&&" (و)

هذا المشغل يتيح لك ربط عدة أوامر معًا، ولكن فقط إذا نجح الأمر الأول.
إنه يشـــبه الأمر يشبه صفّ قطع الدومينو - حيث يؤدي أمر واحد إلى تشغيل الأمر التالي!

```
tryhackme@linux1:~$ echo "Peter" && “James”
“Peter”
“James”
```

أوامر العميل السريّ

المشغل ">" (إعادة توجيه المخرجات)

يتيح لك هذا الرمز إعادة توجيه نتيجة الأمر داخل ملف بدل طباعة النتيجة على الشاشة

إنه يشبه تحويل النهر إلى مجرى جديد!

```
tryhackme@linux1:~$ echo hey > welcome
tryhackme@linux1:~$ cat welcome
hey
```

المشغل ">>" (إضافة)

هذا المشغل مشابه لـ >، لكنه يضيف النتيجة إلى نهاية الملف بدلا من الكتابة فوقه.

إنه مثل إضافة فصل جديد إلى كتاب!

```
tryhackme@linux1:~$ echo hello >> welcome
tryhackme@linux1:~$ cat welcome
hey
hello
```

أسرار مخفيّة

يمكنك استخدام أمر '**history**' لعرض قائمة بالأوامر التي تم تنفيذها سابقًا، مما يسهل تكرار أو استدعاء الإجراءات.

أمن الويب

مرحباً بكم في عالم الويب المثير! الإنترنت يشبه مكتبة ضخمة حيث يمكنك العثور على أي شيء تقريبًا، بدءًا من الألعاب ومقاطع الفيديو وحتى المعلومات حول موضوعاتك المفضلة. تشبه مواقع الويب الكتب الموجودة في هذه المكتبة، ومتصفحات الويب مثل Chrome أو Firefox هي الأدوات التي تستخدمها لقراءتها. إن فهم كيفية عمل هذه الأمور يساعدك على التنقل في العالم الرقمي بشكل أكثر أمانًا وكفاءة!

في حين أن شبكة الإنترنت مليئة بالأشياء الممتعة والمفيدة، إلا أن هناك أيضًا مخاطر كامنة. تمامًا كما هو الحال في ألعاب الفيديو، هناك "أشرار" يحاولون خداعك أو سرقة معلوماتك أو العبث بأجهزتك. يمكن أن تأتي هذه التهديدات في شكل فيروسات أو حيل تصيد أو قرصنة. إن معرفة هذه التهديدات هي الخطوة الأولى للبقاء آمنًا على الإنترنت!

لحماية نفسك على الإنترنت، تحتاج إلى بعض الحركات الدفاعية الهامة! فكر في الأمر مثل وجود درع رادع في اللعبة. يعد استخدام كلمات مرور قوية وتحديث برامجك والحرص على الروابط التي تنقر عليها من الطرق الهامة للحفاظ على أمان عالمك الرقمي. تعلم هذه المهارات سيجعلك بطلاً في مجال الأمن السيبراني!

تصفح بأمان مثل بطل الأمن السيبراني

أساسيات
بناء الويب

دعونا نتعرف على أساسيات الويب..

الإنترنت

هو رمثل خريطة الكنز المليئة بجميع أنواع الأماكن المذهلة التي يمكنك استكشافها. إنه المكان الذي يمكنك من خلاله العثور على مواقع ويب ملونة وألعاب ممتعة ومقاطع فيديو رائعة كلها جاهزة للاكتشاف. يمكنك العثور على معلومات حول الحيوانات والفضاء الخارجي وحتى الأبطال الخارقين المفضلين لديك.

شبكة الويب العالمية

هى شبكة سحرية تربط الناس في جميع أنحاء العالم مثل شبكة العنكبوت التي تنسج من خلال أجهزة الكمبيوتر والأدوات الذكية. تنتشر الرسائل ومقاطع الفيديو في جميع أنحاء العالم، مما يوفر ترفيهًا لا نهاية له. اكتشف عالمًا من المعرفة في هذه الشبكة الواسعة من الإمكانيات المثيرة!

كيف تظهر مواقع الويب على الشاشة؟

هل فكرت كيف تظهر ألعابك المفضلة و الفيديوهات بسرعة؟ كل ذلك بفضل نموذج العميل والخادم، حيث يتواصل متصفح الويب الخاص بك مع أجهزة الحواسيب القوية حول العالم (الخوادم) لجلب صفحات الويب و عرضها. تخيل متصفحك كبطل خارق يتجول على الإنترنت ليحضر لك أشياء مدهشة بمجرد النقر عليها.

URL

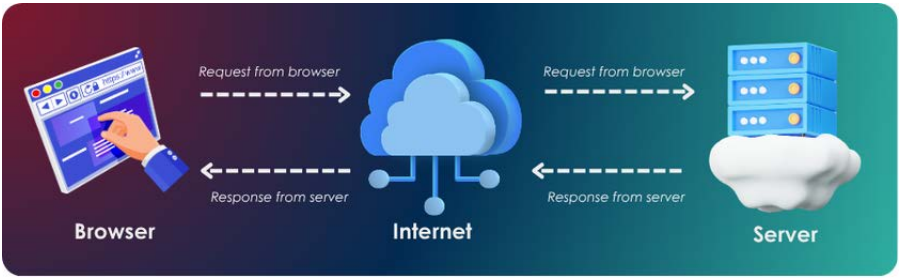
عنوان URL (محدد موقع الموارد الموحد) يشبه عنوانًا لمواقع الويب. فهو يخبر متصفح الويب الخاص بك أين يبحث عن صفحة أو ملف محدد على الإنترنت.

على سبيل المثال:

"www.example.com" هو عنوان URL يوجهك إلى موقع اسمه "example"

هل تعلم؟

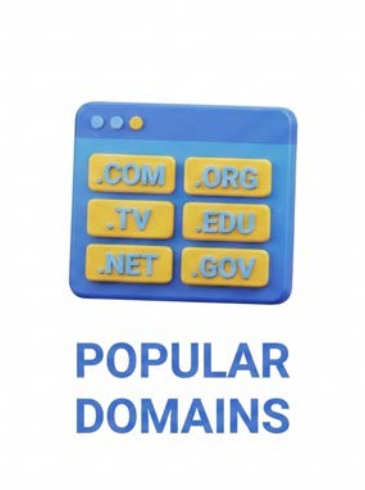
أن أول موقع للويب، أنشأه تيم بيرنرز-لي في عام 1991، ولا يزال متاحًا على الإنترنت! إنه صفحة بسيطة تشرح مشروع الشبكة العنكبوتية العالمية.



الفرق بين
الواجهة الأمامية و الواجهة الخلفية

وجه الاختلاف	الواجهة الخلفية (جانب الخادم)	الواجهة الأمامية (جانب العميل)
الغرض	يدير عمليات جانب الخادم ومهام قاعدة البيانات	يتعامل مع ما يراه المستخدمون ويتفاعلون معه
اللغات	Python، PHP، Ruby، Java	HTML، CSS، JavaScript
المسؤوليات	التعامل مع طلبات الخادم، تخزين البيانات، واسترجاعها	تصميم واجهات المستخدم، التخطيطات، التصفح
التنفيذ	يتم تنفيذه على الخادم	يتم تنفيذه على متصفح المستخدم
يركز على	أداء الخادم وإدارة البيانات	تجربة المستخدم (UX)
الأدوات	الخوادم، قواعد البيانات، بيئات التطوير المتكاملة (IDEs)	متصفحات الويب، محررات النصوص، أدوات التصميم
المهارات	البرمجة، إدارة قواعد البيانات، الأمان	تصميم، مبادئ واجهة المستخدم (UI/UX)، تجربة المستخدم
الأمثلة	برمجيات الخادم، استعلامات قواعد البيانات، مهام برمجة التطبيقات (APIs)	الأزرار، القوائم، النماذج، الرسوم المتحركة

حلقة فك الشفرة السرية
لموقعك على الويب



اسم النطاق

اسم النطاق، مثل "google.com" أو "amazon.com"، هو اسم سهل التذكر يحدد موقعًا على الويب بشكل فريد. إنه مشابه لاستخدام عنوان صديق للعثور على منزله بدلاً من تذكر الأرقام. يتم تسجيل كل اسم نطاق من خلال منظمات خاصة لضمان أنه فريد. بهذه الطريقة، يمكنك بسهولة زيارة مواقعك المفضلة دون الحاجة إلى تذكر أرقام معقدة.

عنوان بروتوكول الإنترنت

عنوان بروتوكول الإنترنت (IP address) هو مجموعة فريدة من الأرقام التي تُخصص لكل جهاز متصل بالإنترنت. إنه يشبه رقم الهاتف لجهاز الحاسوب أو الجهاز اللوحي أو الهاتف الذكي الخاص بك، مما يساعده على التواصل مع الأجهزة الأخرى. عندما تزور موقعًا على الويب، يستخدم جهازك عنوان IP الخاص به للعثور على خادم الموقع والاتصال به، والذي لديه أيضًا عنوان IP الخاص به. تضمن هذه العناوين وصول البيانات إلى الوجهة الصحيحة، تمامًا مثل إرسال رسالة إلى عنوان محدد.

حلقة فك الشيفرة السرية
لموقعك على الويب

نظام أسماء النطاقات

نظام أسماء النطاقات (DNS) يشبه دفتر الهاتف للإنترنت. يقوم بترجمة أسماء النطاقات التي يفهمها البشر، مثل www.example.com، إلى عناوين IP التي يفهمها الحاسوب، مثل 192.0.2.1، حتى يتمكن جهازك من العثور على الخادم الصحيح والاتصال به. عندما تكتب عنوان موقع ويب في متصفحك، يقوم خادم DNS بالبحث بسرعة عن عنوان IP المرتبط بذلك الاسم ويوجه متصفحك إليه. تحدث هذه العملية في الخلفية خلال جزء من الثانية، مما يجعل من السهل علينا تصفح الويب دون الحاجة إلى تذكر سلاسل معقدة من الأرقام.

مهمّة

تخيل أنك تنشئ موقع الويب الرائع الخاص بك!
ما هو اسم النطاق الرائع الذي ستختاره؟
على سبيل المثال: "SuperCoder.com".
اكتب الاسم الذي ستختاره. كن مبدعًا!

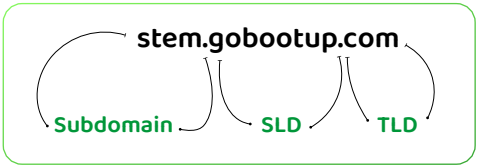
التسلسل الهرمي للنطاق

TLD (نطاق المستوى الأعلى)

هو الجزء الأخير من اسم النطاق، مثل .com في tryhackme.com. هناك نوعان من TLDs:

gTLDs (نطاق المستوى الأعلى العام) تخبرك غرض الموقع الإلكتروني.

على سبيل المثال:



.com للمواقع التجارية

.org للمنظمات

.edu للتعليم

.gov للحكومة

ccTLDs (نطاق المستوى الأعلى للرمز الوطني)

تشير إلى بلد الموقع على سبيل المثال:

.qa لدولة قطر

.ae لدولة الإمارات

في الوقت الحاضر، هناك العديد من gTLDs الجديدة، مثل .biz .website .club .onlin.

SLD (نطاق المستوى الثاني)

في tryhackme.com:

"tryhackme" هو نطاق المستوى الثاني (SLD) و".com" هو نطاق المستوى الأعلى (TLD).

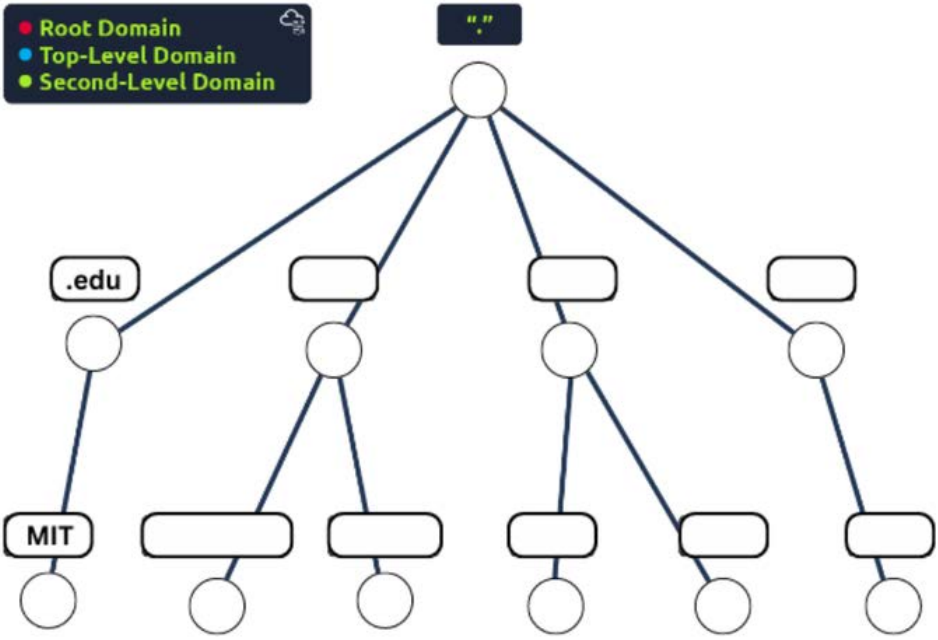
نطاق المستوى الثاني هو ما تختاره لتسمية موقعك على الويب، ويمكن أن يتكون من ما يصل إلى 63 حرفًا. يمكن أن يشمل حروفًا (a-z)، وأرقامًا (0-9)، وواصلات (-)، لكنه لا يمكن أن يبدأ أو ينتهي بواصلات، ولا يحتوي على واصلات متتالية. يساعد هذا الاسم الفريد، بالاقتران مع نطاق المستوى الأعلى، في تحديد موقعك على الإنترنت.

النطاقات الفرعية

يظهر النطاق الفرعي قبل نطاق المستوى الثاني (SLD) ويتم فصله بنقطة. على سبيل المثال، في "admin.tryhackme.com، "admin هو النطاق الفرعي. تخضع النطاقات الفرعية لنفس قواعد نطاقات المستوى الثاني: يمكن أن يصل طولها إلى 63 حرفًا ويمكن أن تشمل حروفًا (a-z)، وأرقامًا (0-9)، وواصلات(لكن لا يمكن أن تبدأ أو تنتهي بواصلات أو تحتوي على واصلات متتالية). يمكن أن يكون لديك نطاقات فرعية متعددة، مثل jupiter.servers.tryhackme.com، طالما أن الطول الإجمالي 253 حرفًا أو أقل. لا يوجد حد لعدد النطاقات الفرعية التي يمكنك إنشاؤها.

هل يمكنك حلها ؟

باستخدام الرسم التخطيطي ووسيلة الإيضاح الموضحة أدناه، ابحث عن أمثلة واكتب TLDs (نطاقات المستوى الأعلى) وSLDs ذات الصلة (نطاقات المستوى الثاني) لكل منها. لقد تم عمل مثال واحد لك. قم بتلوين كل مستوى مجال وفقًا لوسيلة الإيضاح.



ماذا يحدث
عند طلب DNS؟

1. التحقق من الذاكرة المحلية

عندما تكتب عنوان موقع ويب (مثل www.example.com) في متصفحك، يتحقق الكمبيوتر أولاً من ذاكرته المحلية (ذاكرة التخزين المؤقت) لمعرفة ما إذا كان عنوان الـIP المقابل موجودًا.

2. طلب خادم DNS المتكرر

إذا لم يتم العثور على العنوان محليًا، يرسل الكمبيوتر الطلب إلى خادم DNS المتكرر، عادةً ما يوفره مزود خدمة الإنترنت (ISP) أو يمكن إدخاله يدويًا.

3. البحث في الذاكرة

يمتلك خادم DNS المتكرر ذاكرة مؤقتة خاصة به. إذا وجد العنوان هناك، يعيده مباشرة إلى جهازك.

4. خوادم DNS المتتالية

إذا لم يتم العثور على العنوان في ذاكرة التخزين المؤقت، يبدأ خادم DNS المتكرر في البحث ضمن خوادم DNS المتتالية، وهي خوادم تحتوي على معلومات عن النطاقات العليا.

5. خوادم نطاق المستوى الأعلى (TLD)

في النهاية، يصل خادم DNS المتكرر إلى خوادم نطاق المستوى الأعلى مثل com.، ويحصل منها على عنوان الـIP المطلوب ويرسله إليك.

ماذا يحدث
عند طلب DNS؟

6. خادم DNS المخوّل

خادم TLD لا يعرف عنوان الموقع بنفسه، لكنه يقوم بتوجيه جهازك إلى الخادم المخول المسؤول عن النطاق والذي يحتوي سجلات DNS الخاصة بذلك النطاق.

7. استرداد سجلات DNS

يستعلم خادم DNS المتكرر من الخادم المخوّل عن سجلات DNS المتعلقة بالنطاق المطلوب.

8. الرد على العميل

يرسل الخادم المخوّل سجلات DNS (مثل عناوين IP) إلى خادم DNS المتكرر.

9. تحديث الذاكرة المحلية

يحفظ خادم DNS المتكرر هذه السجلات في ذاكرته المحلية للاستخدام المستقبلي. ووفقًا لقيمة مدة البقاء (TTL)، يتم تخزين السجل حتى يحين وقت التحقق منه مرة أخرى.

10. الرد النهائي على العميل

يرسل خادم DNS المتكرر سجلات DNS من ذاكرته إلى جهاز العميل الذي طلبها، ليتمكن بعدها من الاتصال بخادم موقع الويب وتحميل الصفحة.

الفرق بين
HTTP و HTTPS

ما هو HTTP

(بروتوكول نقل النص الفائق) يشبه مجموعة من القواعد التي تساعد جهاز الكمبيوتر الخاص بك على التحدث إلى مواقع الويب. تم إنشاؤه بواسطة تيم بيرنرز-لي (Tim Berners-Lee) وفريقه في أواخر الثمانينيات وأوائل التسعينيات. إنه الطريقة التي يطلب بها جهاز الكمبيوتر الخاص بك ويحصل على كل المحتويات على صفحات الويب، مثل الصور، ومقاطع الفيديو، والكلمات.

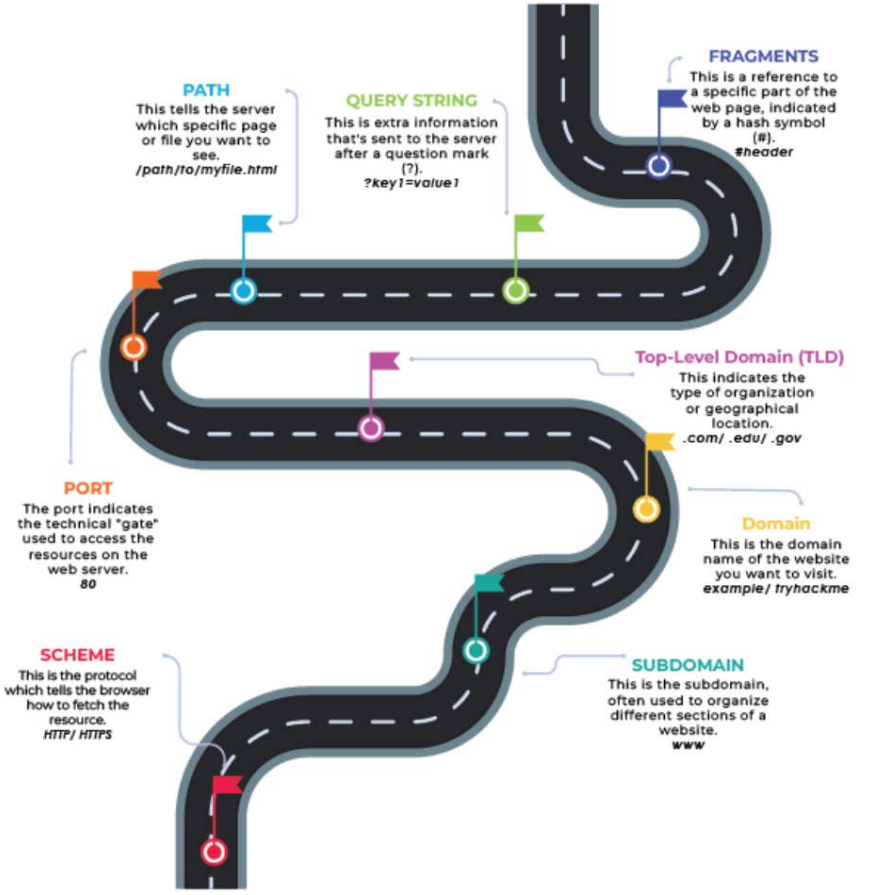
ما هو HTTPS

هو نسخة أكثر أمانًا من HTTP. يحافظ على خصوصية بياناتك عن طريق تشفيرها، مما يعني أنه يشبه وضع معلوماتك في رمز سري لا يمكن فك شفرته إلا بواسطة الموقع الصحيح. هذا يساعد على التأكد من أنك تتواصل مع الموقع الحقيقي وليس مع شخص يتظاهر بأنه هو.

التنقل خلال URL

فكر في عنوان URL كعنوان سحري للإنترنت! تماماً كما أن عنوان منزلك يوجه ساعي البريد إلى أين يرسل الرسائل، فإن عنوان URL يخبر متصفح الويب الخاص بك أين يجد المواقع الإلكترونية. إنه رمز خاص مكون من كلمات ورموز يوجه متصفحك عبر متاهة الإنترنت الواسعة.

https://www.example.com:80/path/to/myfile.html?key1=value1#header



طرق HTTP

طرق HTTP تخبر خادم الويب بالإجراء الذي ترغب في اتخاذه عندما تقوم بتقديم طلب.

POST

يُستخدم لإرسال بيانات إلى خادم الويب وربما إنشاء سجلات جديدة.

GET

يُستخدم للحصول على معلومات من خادم الويب.

Delete

يُستخدم لحذف المعلومات/السجلات من خادم الويب.

PUT

يُستخدم لإرسال بيانات إلى خادم الويب لتحديث المعلومات.

هل تعلم؟

أن HTTPS يساعد في منع هجمات "man-in-the-middle" من خلال تشفير البيانات بين العميل (متصفحك) والخادم، مما يضمن اتصالات آمنة.

رموز حالة HTTP

رموز حالة HTTP هي رسائل من الخادم تخبرك بكيفية التعامل مع طلبك. يمكن أن تشير إلى النجاح (مثل "OK 200")، الأخطاء (مثل "Not Found 404")، أو معلومات مهمة أخرى حول ما حدث عندما حاولت الوصول إلى صفحة ويب.

199–100 **استجابة المعلومات**	تُرسل هذه الرموز لتخبر العميل أن الجزء الأول من طلبه قد تم قبوله ويجب عليه متابعة إرسال باقي طلبه. هذه الرموز لم تعد شائعة جدًا.
299–200 **النجاح**	يُستخدم هذا النطاق من رموز الحالة لإخبار العميل أن طلبه كان ناجحًا.
399–300 **إعادة التوجيه**	تُستخدم هذه الرموز لتوجيه طلب العميل إلى مورد آخر. قد يكون ذلك إلى وصف صفحة مختلفة أو موقع مختلف تمامًا.
499–400 **أخطاء العميل**	يُخصص هذا النطاق للأخطاء التي تحدث على جانب العميل وعادة ما تشير إلى مشكلة في طريقة تعامل العميل مع الطلب.
599–500 **أخطاء الخادم**	يُخصص هذا النطاق للأخطاء التي تحدث على جانب الخادم وعادة ما تشير إلى مشكلة كبيرة في تعامل الخادم مع الطلب.

رموز حالة HTTP العامة

200 **تمام**	تم إكمال الطلب بنجاح.
201 **تم الإنشاء**	تم إنشاء مورد ما (مثل مستخدم جديد أو مقالة جديدة).
301 **تم التحويل** **بشكل دائم**	يقوم هذا بإعادة توجيه متصفح العميل إلى صفحة ويب جديدة أو يخبر محركات البحث أن الصفحة انتقلت إلى مكان آخر ويجب أن تبحث هناك بدلاً من ذلك.
302 **تم العثور**	مماثل للتوجيه الدائم أعلاه، ولكن كما يوحي الاسم، هذا تغيير مؤقت فقط وقد يتغير مرة أخرى في المستقبل القريب.
400 **طلب خاطئ**	يخبر المتصفح أن هناك شيء خاطئ أو مفقود في الطلب. يمكن استخدام هذا أحيانًا إذا كان مورد خادم الويب الذي يتم طلبه يتوقع معلومة معينة لم يرسلها العميل.
401 **غير مصرح**	ليس لديك حالياً الإذن لعرض هذا المورد حتى تكون قد قمت بتسجيل الدخول إلى تطبيق الويب، وعادة ما يكون ذلك بواسطة اسم مستخدم وكلمة مرور.

رموز حالة
HTTP العامة

هناك العديد من رموز حالة HTTP المختلفة، وحتى التطبيقات يمكن أن تعرف رموز خاصة بها.
دعنا نلقي نظرة على الأكثر شيوعاً التي من المحتمل أن تصادفها:

403 **ممنوع**	ليس لديك الإذن لعرض هذا المورد سواء قمت بتسجيل الدخول أم لا.
404 **لم يتم العثور على الصفحة**	الصفحة أو المورد الذي طلبته غير موجود.
405 **الطريقة غير مسموح بها**	لا يسمح المورد بطلب بهذه الطريقة. مثال: إرسال طلب GET إلى //create-account بينما كان يتوقع طلب POST.
500 **خطأ داخلي في الخدمة**	واجه الخادم خطأ ما مع الطلب ولا يعرف كيفية التعامل معه بشكل صحيح.
503 **الخدمة غير متاحة**	لا يمكن للخادم التعامل مع الطلب لأنه يواجه ضغطا كبيرا أو أن الخادم تحت الصيانة

رتب الحروف لتجد المصطلحات ذات المعنى أدناه

NPGI 

ATCH 

GERAN 

TENLIC 

DAIMON 

ORPT 

NIRGTS 

DOFERA 

TODHEM 

ERQYU 

RMNIFOU 

IKSD 

ما رمز حالة HTTP الذي وجدته؟

خلف كواليس
مغامرات الويب الخاصة بك

العناوين (Headers)

العناوين (Headers) هي بيانات إضافية يمكنك إرسالها إلى خادم الويب عند تقديم الطلبات. على الرغم من أن العناوين ليست ضرورية بشكل صارم عند تقديم طلب HTTP، إلا أنك ستجد صعوبة في عرض الموقع بشكل صحيح ما لم تقم بإضافتها.

ملفات تعريف الارتباط (Cookies)

ملفات تعريف الارتباط هي ملفات صغيرة يتم تخزينها على جهاز الكمبيوتر الخاص بك عن طريق مواقع الويب. وهي تتذكر تفضيلاتك ومعلومات تسجيل الدخول، مما يجعل تجربة الويب الخاصة بك أكثر سلاسة وأكثر تخصيصًا.

ملفات تعريف الارتباط
(Cookies)

هل تعلم؟

أنه تم استخدام ملفات تعريف الارتباط الأولى على الويب بواسطة Netscape في عام 1994 لتخزين معلومات المستخدم على مواقع التجارة الإلكترونية، مثل محتويات سلة المشتريات الخاصة بالمستخدم.

تقنيات وإطارات الويب

عندما تزور موقعًا على الويب، يقوم متصفحك (مثل سفاري أو جوجل كروم) بإرسال طلب إلى خادم الويب لطلب معلومات حول الصفحة التي تزورها.

سيستجيب الخادم ببيانات يستخدمها متصفحك لعرض الصفحة لك؛ خادم الويب هو مجرد كمبيوتر مخصص في مكان ما في العالم يتعامل مع طلباتك.

يتم إنشاء مواقع الويب في المقام الأول باستخدام

HTML

لبناء مواقع الويب وتحديد بنيتها (صور، نصوص، روابط)

CSS

لإنشاء مواقع ويب جميلة من خلال إضافة خيارات التصميم

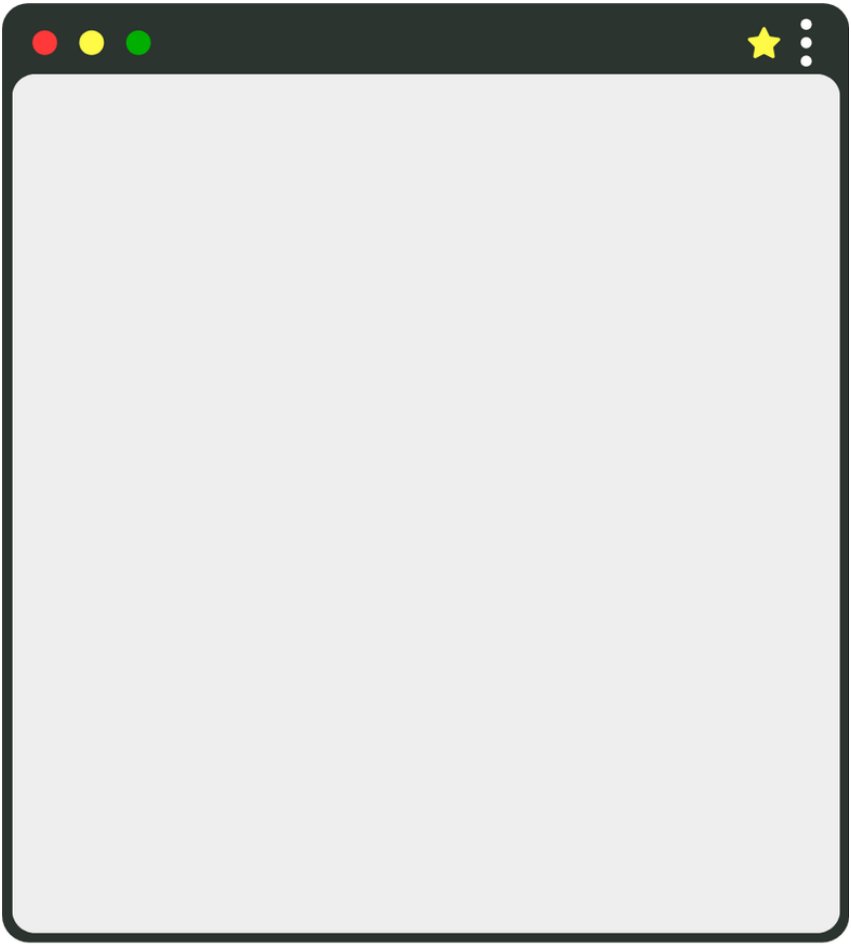
JS

تستخدم لإضافة التفاعل والحركة إلى صفحات الويب

صمم موقع الويب
الذي تحلم به

ارسم مخططًا لموقع الويب الذي تحلم به.

كن مبدعًا في التصميم والتخطيط والألوان والمحتوى. استخدم عناصر مثل شريط التنقل، الصور، النصوص، وأي ميزات تفاعلية تتخيلها. فكر في ما يمكن أن يجعل موقعك فريدًا وممتعًا للاستخدام.



HTML
(HyperText Markup Language)

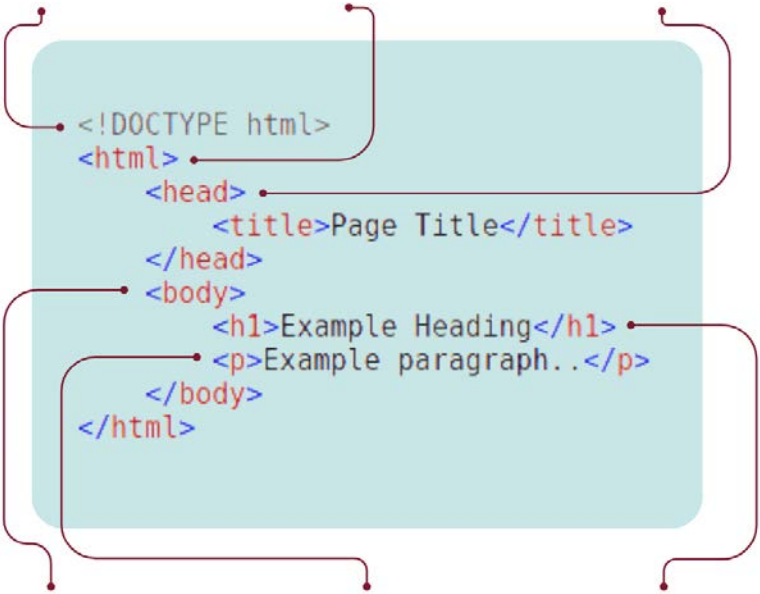
لغة الترميز النصي الفائق (HTML) هي اللغة التي تُكتب بها المواقع على الويب.
العناصر (المعروفة أيضًا بالوسوم) هي لبنات بناء صفحات HTML وتحدد كيفية عرض المحتوى في المتصفح.

يُظهر المثال أدناه ملف HTML بسيط، ورغم اختلاف تصميم مواقع الويب ومحتواها، فإن معظمها يعتمد على هذا الهيكل الأساسي.

يحدد أن الصفحة هي مستند HTML5

إنه العنصر الجذر لصفحة HTML

يحتوي على معلومات حول الصفحة



يحدد نص مستند HTML

يحدد الفقرة

يحدد عنوان كبير

وسوم HTML

هي الأجزاء الأساسية لصفحة الويب التي تخبر المتصفح بكيفية عرض المحتوى.

على سبيل المثال:

<h1> هذا الوسم ينشئ عنوانًا رئيسيًا (أكبر عنوان في الصفحة).

<p> هذا الوسم ينشئ فقرة من النص.

<img> هذا الوسم يُدرج صورة.

<a> هذا الوسم ينشئ رابطًا لصفحة ويب أخرى.

سمات HTML

الوسوم يمكن أن تحتوي على سمات، وهي مثل معلومات إضافية توفر سياقاً إضافياً حول العنصر. على سبيل المثال:

class

```
<div class="container">Content</div>
```

تُستخدم السمة "class" لتجميع عناصر متعددة معًا وتطبيق نفس الأنماط عليها. تحدد "class" اسم فئة لتصميم CSS.

src & alt

```
<img src="image.jpg" alt="A description">
```

تُستخدم السمة "src" لتحديد مصدر الصورة
بينما "alt" توفر وصفًا بديلًا في حالة عدم تحميل الصورة أو لقراءات الشاشـــة.

id

```
<p id="intro">Hello, welcome to my website!</p>
```

تُستخدم السمة "id" لتحديد عنصر معين بشكل فريد.
ويمكن استخدامها للوصول إلى هذا العنصر وتنسيقه باستخدام CSS أو التفاعل معه باستخدام JavaScript.

CSS Cascading Style Sheets

Inline CSS (المضمّن)

```
<p style="color: blue;">This text is blue.</p>
```

يتم تطبيق الأنماط مباشرة داخل وسم HTML باستخدام style

Internal CSS (الأنماط الداخلية)

```
<head>
  <style>
    p { color: blue; }
  </style>
</head>
```

تُكتب الأنماط داخل علامة <style> ضمن قسم <head> في ملف HTML

External CSS (الأنماط الخارجية)

```
<head>
  <link rel="stylesheet" href="styles.css">
</head>
```

تُكتب الأنماط في ملف CSS منفصل، ويتم ربطه بملف HTML باستخدام وسم <link>

JavaScript

هي لغة برمجة تُستخدم لجعل المواقع الإلكترونية تفاعلية. تتيح لك إنشاء محتوى ديناميكي مثل الرسوم المتحركة، والتحقق من صحة النماذج، والخرائط التفاعلية.

عندما ترى صفحة ويب تقوم بشيء أكثر من مجرد عرض معلومات ثابتة، مثل تحديث المحتوى دون الحاجة إلى تحديث الصفحة، فإن ذلك يكون بفضل جافا سكريبت.

المفاهيم الأساسية في جافا سكريبت

المتغيرات- Variables : هذه هي حاويات لتخزين البيانات، مثل الأرقام والنصوص أو حتى الكائنات الكاملة.

الدوال - Functions : هي مجموعة من الأوامر تُكتب مرة واحدة لتنفيذ مهمة محددة، ويمكن استدعاؤها كلما احتجت إليها دون إعادة كتابة الأوامر. يساعد ذلك على تنظيم الشيفرة البرمجية وتسهيل قراءتها وإعادة استخدامها.

الأحداث - Events : هذه هي الإجراءات التي تحدث على صفحة الويب، مثل النقر على زر أو مرور الفأرة فوق عنصر. يمكن لـ JavaScript الاستماع لهذه الأحداث والتفاعل معها وفقًا لذلك.

ثلاث طرق
لإضافة جافا سكريبت

Inline JavaScript (مضمن)

يتم كتابة JavaScript المضمن مباشرة داخل عنصر HTML باستخدام سمات onclick أو onload أو غيرها من سمات الأحداث. ينصح بتجنب هذه الطريقة لكونها تؤدي إلى ثغرات أمنية، كما تزيد من صعوبة قراءة الكود البرمجي وإصلاحه.

```
<button onclick="alert('Hello!')">Click Me</button>
```

Internal JavaScript (داخلي)

يتم وضع JavaScript الداخلي داخل وسم <script> في قسم <head> أو <body> لملف HTML. يفضل استخدام هذه الطريقة إذا كان التطبيق الذي تقوم بإنشائه مكوناً من صفحة واحدة فقط.

```
<!DOCTYPE html>
<html>
<head>
  <script>
    function sayHello() {
      alert('Hello from Internal JavaScript!');
    }
  </script>
</head>
<body>
  <button onclick="sayHello()">Click Me</button>
</body>
</html>
```

```
<!DOCTYPE html>
<html>
<head>
  <script src="script.js"></script>
</head>
<body>
  <button onclick="sayHello()">Click Me</button>
</body>
</html>
```

External JavaScript (خارجي)

يتم تخزين JavaScript الخارجي في ملفات js. منفصلة ويتم ربطها بملف HTML باستخدام وسم <script> مع سمة src. هذا يكون أفضل للنصوص البرمجية الكبيرة وإعادة استخدام الكود عبر صفحات متعددة.

Javascript

```
function sayHello() {
  alert('Hello from External JavaScript!');
}
```

متصفح الويب

متصفح الويب هو تطبيق برمجي يُستخدم للوصول إلى مواقع الويب وعرضها على الإنترنت. يقوم بجلب المعلومات من الويب وعرضها على جهازك. تشمل متصفحات الويب الشائعة مثل Google Chrome وMozilla Firefox وMicrosoft Edge وSafari. يتيح لك المتصفح التنقل بين صفحات الويب، ووضع علامات على مواقعك المفضلة، واستخدام تطبيقات الويب المختلفة. إنه أداة أساسية لتصفح الإنترنت، مما يضمن لك العثور على المحتوى والتمتع به بسهولة.

ميزات الأمان في متصفحك:

رسائل التحذير

يقوم المتصفح بتحذيرك إذا كان الموقع خطيرًا أو يحاول تثبيت برامج مشبوهة، مثل مراقب حي ودود يحافظ على سلامتك.

مانعات النوافذ المنبثقة (Pop-up Blockers)

تمنع هذه الميزات ظهور النوافذ المنبثقة المزعجة والمحتملة الخطورة، مثل الحارس الذي يمنع الضيوف غير المرغوب فيهم.

العزل (Sandboxing)

هو أسلوب أمان يجعل كل صفحة ويب تعمل داخل "صندوق" منفصل، بحيث لا تستطيع التأثير في بقية أجزاء المتصفح أو الوصول إلى ملفات جهازك دون صلاحية

مهمّة

أي من هذه الشعارات للمتصفحات تعرفها؟
ارسم دائرة حول الشعارات التي رأيتها أو استخدمتها من قبل!

الخوادم

نموذج الخادم والعميل

نموذج الخادم والعميل يشبه محادثة بين صديقين. العميل، كمثال : أنت تستخدم متصفح الويب، تطلب شيئًا (مثل صفحة ويب) من الخادم، الذي يشبه الصديق المساعد الذي يقدم ما طلبته. إنه وسيلة للتواصل بين الحواسيب عبر الشبكة، حيث يقوم العملاء بإرسال طلبات ويستجيب الخوادم بإرسال البيانات المطلوبة.

ماذا يفعل خادم العميل

طلبات المتصفح - Browser Requests

عندما تكتب عنوان موقع ويب في متصفحك، يرسل المتصفح طلبًا إلى الخادم يطلب فيه ملفات الصفحة.

استجابة الخادم - Server Responds

يستقبل الخادم الطلب، ويجد الملفات المطلوبة (مثل HTML والصور)، ثم يرسلها مرة أخرى إلى متصفحك.

عرض المتصفح - Browser Renders

بمجرد أن يحصل متصفحك على الملفات، يجمع كل شيء معًا ويعرض صفحة الويب على شاشتك، بما في ذلك النصوص والصور والأزرار التي يمكنك التفاعل معها.

خادم الويب

خادم الويب هو جهاز كومبيوتر قوي يخزن ويوصل محتوى المواقع الإلكترونية إلى متصفحك. عندما تكتب عنوان موقع ويب في متصفحك، يقوم خادم الويب بإرسال صفحات الموقع والصور والملفات الأخرى إلى جهازك، مما يتيح لك رؤية الموقع والتفاعل معه. فكر في الأمر كمكتبة تقدم لك الكتاب الذي ترغب في قراءته!

ماذا يفعل خادم الويب

تخزين ملفات الموقع الإلكتروني Stores Website Files

يخزن جميع أجزاء الموقع في مكان آمن.

معالجة الطلبات-Handles Requests

عندما يرغب شخص ما في عرض موقع إلكتروني، يطلب من خادم الويب الحصول على ملفات الموقع.

توصيل المحتوى-Delivers Content

يستجيب بإرسال الملفات المطلوبة إلى متصفح المستخدم، الذي يعرض بعد ذلك الموقع الإلكتروني.

إدارة البيانات - Manages Data

بالنسبة للمواقع الإلكترونية التي تتغير أو تحتوي على محتوى ديناميكي (مثل تحديثات الأخبار أو عناصر التسوق)، يتفاعل خادم الويب مع قواعد البيانات لتخزين واسترجاع وتحديث المعلومات حسب الحاجة.

قواعد البيانات
Databases

قواعد البيانات تشبه خزائن الملفات الرقمية المنظمة حيث تقوم الحواسيب بتخزين وإدارة المعلومات.

تم تصميمها لتخزين كميات كبيرة من البيانات بطريقة منظمة، مما يسهل العثور على المعلومات وتحديثها واسترجاعها عند الحاجة. تُستخدم قواعد البيانات في المواقع الإلكترونية والتطبيقات والعديد من الأنظمة الحاسوبية الأخرى لتخزين كل شيء من حسابات المستخدمين والمعلومات إلى البيانات العلمية والسجلات المالية.

NoSQL Databases
قواعد بيانات NoSQL

تخزن قواعد بيانات NoSQL البيانات بتنسيقات مرنة مثل الوثائق أو أزواج المفتاح-القيمة. تعتبر الخيار الأنسب للتعامل مع كميات كبيرة من البيانات غير المنظمة، كما في تطبيقات الويب وتحليلات البيانات الكبيرة.

Relational Databases
قواعد البيانات العلائقية

تخزن قواعد البيانات العلائقية البيانات في جداول تحتوي على صفوف وأعمدة، باستخدام SQL (لغة الاستعلامات الهيكلية) لإدارتها. وتعتبر الخيار الأنسب للتعامل مع البيانات المنظمة مثل السجلات المالية وتطبيقات الأعمال.

قواعد البيانات هي العنصر السري الذي يجعل المواقع الإلكترونية ديناميكية.

فهي تتيح للمواقع الإلكترونية أن:

- تخصص المحتوى: تعرض لك توصيات بناءً على عمليات الشراء أو تاريخ التصفح السابق الخاص بك.
- تتعامل مع تفاعلات المستخدم: تخزن تعليقاتك، وإعجاباتك، ومشاركاتك، وتفاعلاتك الأخرى مع الموقع.
- تدير المعاملات: تعالج طلباتك ومدفوعاتك والمعلومات الحساسة الأخرى بأمان. يمكن تشبيه الأمر بخزنة مصرفية موثوقة تحافظ على أموالك بأمان.

صندوق أدوات
تطوير الويب

إطارات الويب

الأدوات التي توفر للمطورين تعليمات برمجية ومكتبات مكتوبة مسبقًا لتبسيط عملية إنشاء تطبيقات الويب. توفر هذه الإطارات طريقة منظمة لإنشاء صفحات الويب وتنظيمها وإدارة قواعد البيانات والتعامل مع تفاعلات المستخدم والمزيد.

بعض إطارات تطوير الويب الشائعة:

Bootstrap

هو إطار عمل للواجهة الأمامية يسهل تصميم مواقع الويب المتجاوبة والأنيقة لعرض المواقع بشكل مناسب عبر الهواتف المحمولة، باستخدام HTML وCSS وJavaScript.

React

هي مكتبة JavaScript لبناء واجهات المستخدم، وغالباً ما تُستخدم لإنشاء تطبيقات الصفحة الواحدة حيث يتم تحديث المحتوى دون الحاجة إلى تحديث الصفحة.

Angular

هو إطار عمل للواجهة الأمامية مبني على TypeScript، تم تطويره بواسطة جوجل. يُستخدم لبناء تطبيقات الويب الديناميكية مع ميزات مثل الربط ثنائي الاتجاه للبيانات وحقن الاعتمادات.

Vue.js

هو إطار عمل JavaScript تم تصميمه لبناء واجهات ويب تفاعلية. يُعرف ببساطته ومرونته، مما يجعله سهل الدمج في مشاريع أخرى.

Django

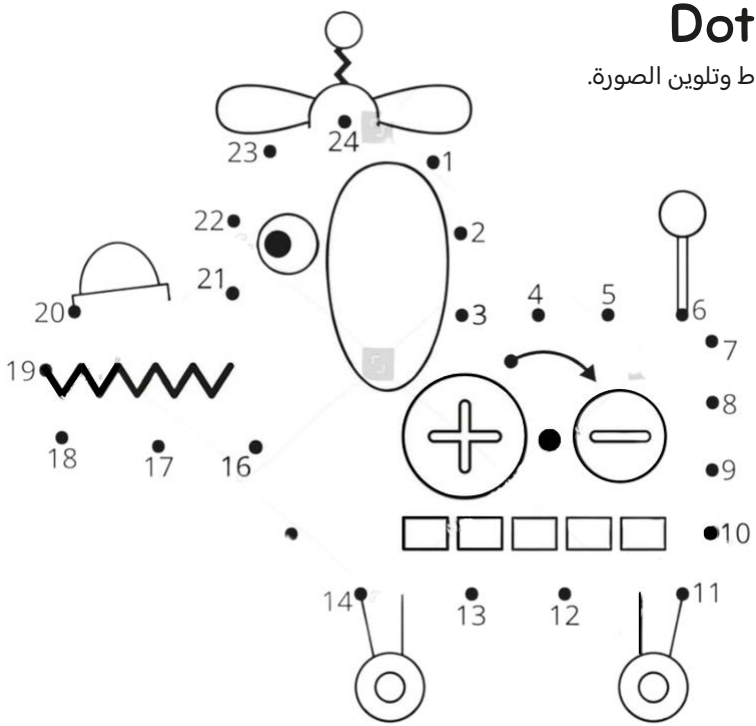
هو إطار عمل ويب عالي المستوى بلغة Python يشجع على التطوير السريع والتصميم النظيف والعملي. يتبع نمط التصميم MVC (النموذج-العرض-التحكم).

Ruby on Rails

يُشار إليه غالباً باسم Rails، هو إطار عمل لتطبيقات الويب مكتوب بلغة Ruby. يركز على القواعد بدلاً من التكوين ويهدف إلى تبسيط تطوير تطبيقات الويب.

Dot to Dot

قم بتوصيل النقاط وتلوين الصورة.

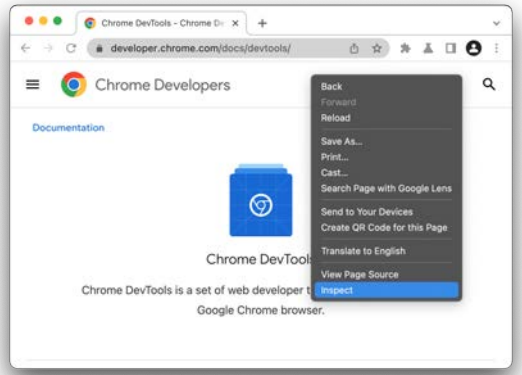


جدار الحماية لتطبيقات الويب

WAF (Web Application Firewall)

جدار الحماية الخاص بتطبيقات الويب (WAF) يجلس بين طلبات الويب والخادم لحمايته من الاختراقات وهجمات حجب الخدمة (DOS). يقوم بفحص طلبات الويب بحثًا عن أساليب الهجوم الشائعة، ويتحقق مما إذا كان الطلب من متصفح حقيقي، ويحدد عدد الطلبات في الثانية من عنوان IP. إذا اكتشف هجومًا محتملاً، فإنه يحظر الطلب قبل أن يصل إلى الخادم.

تفتيش الويب



أدوات المطور - المفتش

يعد "Browser Inspector" أداة مدمجة في متصفحات الويب تتيح للمطورين والمستخدمين عرض التعليمات البرمجية الأساسية وبنية صفحة الويب والتفاعل معها.

تُعرف أيضًا باسم "أدوات المطور" أو "DevTools" في العديد من المتصفحات مثل Google Chrome وMozilla Firefox وMicrosoft Edge وSafari.

هل تعلم؟

يقوم Browser Inspector بتحسين مواقع الويب، مما يضمن القيام بوظيفة بشكل صحيح وتوفير تجربة مستخدم سلسة.

إليك ما يسمح لك بفعله:

1. تفقد العناصر
2. إجراء تعديلات مباشرة على كود HTML وCSS
3. تصحيح كود جافا سكريبت
4. مراقبة نشاط الشبكة
5. قياس أوقات تحميل الصفحة وتحليل الأداء
6. وحدة تحكم لتنفيذ أوامر JavaScript بشكل تفاعلي

كشف التعليقات والعناصر المخفية

أحيانًا يترك مطورو الويب تعليقات أو عناصر مخفية في التعليمات البرمجية. يمكن أن تكون هذه ملاحظات لأنفسهم، أو تذكيرات للمطورين الآخرين، أو حتى رسائل سرية! يمكن لمفتش المتصفح اكتشاف هذه الجواهر المخفية ومعرفة المزيد حول أمان موقع الويب أو وظائفه.

أدوات المطور Developer Tools

مصحح الأخطاء Debugger

تهدف هذه اللوحة الموجودة في أدوات المطورين إلى تصحيح أخطاء JavaScript، وهي ميزة ممتازة لمطوري الويب الراغبين في معرفة سبب عدم عمل شيء ما. ولكن باعتبارنا مختبري اختراق، فهو يمنحنا خيار التعمق في كود JavaScript. في Firefox وSafari، تسمى هذه الميزة Debugger، ولكن في Google Chrome، تسمى Sources.

إليك ما تسمح لك بفعله:

1. **إيقاف تنفيذ التعليمات البرمجية مؤقتًا عن طريق تعيين نقاط توقف في التعليمات البرمجية مما يسمح لك بفحص التعليمات البرمجية.**
2. **فحص المتغيرات لتحديد الأخطاء أو فهم الكود في أي مرحلة من تنفيذ الكود.**
3. **بتعديل كود JavaScript في الوقت الفعلي لمعرفة مدى تأثيره على سلوك موقع الويب.**

الشبكة Network

يمكن استخدام علامة تبويب الشبكة الموجودة في أدوات المطور لتتبع كل طلب خارجي تقدمه صفحة الويب.

تحليل حركة الشبكة يتيح لك :

عرض قائمة بكل الطلبات أو الاستجابات في صفحة الويب

بإمكانك النقر على كل طلب أو استجابة لعرض التفاصيل الخاصة به، وتتضمن هذه التفاصيل:

URL : عنوان المورد المطلوب.

Method : طريقة HTTP المستخدمة للطلب (على سبيل المثال، GET، POST).

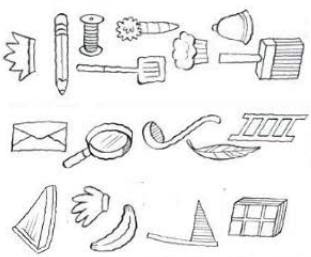
Status : رمز حالة HTTP للاستجابة (على سبيل المثال، 200 OK، 404 Not Found).

Type : نوع المورد المطلوب (على سبيل المثال، مستند، برنامج نصي، صورة).

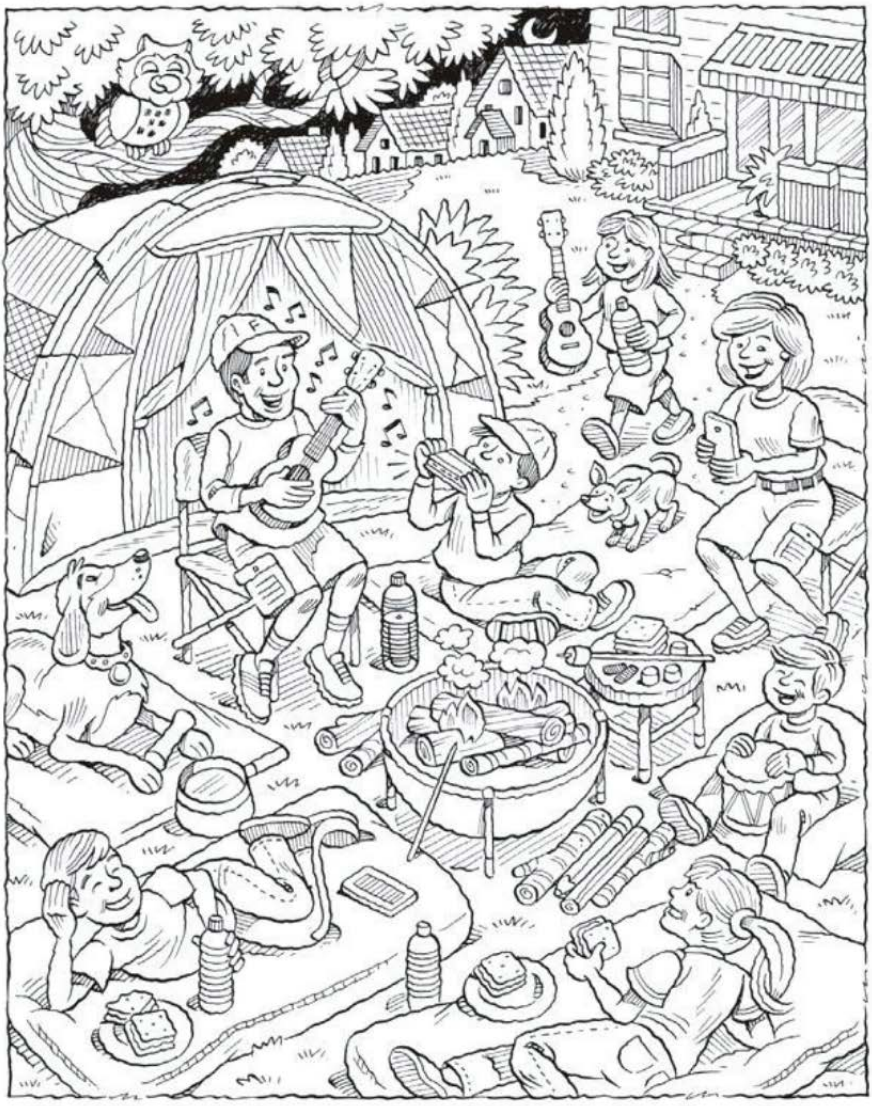
Size : حجم المورد المطلوب.

Time : الوقت الذي استغرقه إكمال الطلب.

العثور على الأشياء المخفية



تقضي هذه العائلة وقتاً معاً في التخييم في الفناء الخلفي لمنزلهم. **هل يمكنك العثور على هذه الأشياء المخفية؟**



التصيّد الاحتيالي

هجوم التصيد الاحتيالي

هو نوع من الهجمات السيبرانية حيث تحاول الجهات الفاعلة الخبيثة خداع الأفراد للكشف عن معلومات حساسة مثل أسماء المستخدمين أو كلمات المرور أو أرقام بطاقات الائتمان أو البيانات الشخصية الأخرى.

غالبًا ما تعتمد على أساليب الهندسة الاجتماعية لاستغلال ثقة الإنسان وفضوله، مما يجعل من المهم للمستخدمين توخي الحذر والتحقق من صحة أي طلبات للحصول على معلومات شخصية يتلقونها عبر الإنترنت

أساليب التصيد الشائعة

المواقع الخادعة | المرفقات الضارة | هندسة اجتماعية | انتحال البريد

كيفية التعرف على هجمات Phishing

التحقق من عنوان البريد الإلكتروني للمرسل غالبًا ما تستخدم رسائل البريد الإلكتروني التصيدية عناوين تحاكي العناوين الشرعية ولكن قد تحتوي على اختلافات طفيفة أو أخطاء إملائية.

ابحث عن تحيات عامة مثل "عزيزي المستخدم" بدلاً من مخاطبتك باسمك.

احذر من الاستعجال أو التهديدات مثل المطالبة بإغلاق حسابك إذا لم تستجب بسرعة.

التحقق من الروابط قبل النقر قم بتمرير مؤشر الماوس فوق الروابط في رسائل البريد الإلكتروني (دون النقر) لرؤية عنوان URL الفعلي الذي قد يكون موقع ويب مزيفا تم تصميمه لسرقة معلوماتك.

التحقق من الأخطاء الإملائية والنحوية

تجنب تقديم معلومات شـخصية مثل كلمات المرور أو أرقام الضمان الاجتماعي أو تفاصيل الحساب.

تحقق من طلبات الدفع أو تغييرات الحساب قبل اتخاذ أي إجراء.

نقاط ضعف الويب الشائعة
(OWASP Top 10)

هجمات الحقن Injection Attacks

الهجوم الحقني هو نوع من الهجمات السيبرانية حيث يتم حقن تعليمات برمجية أو أوامر ضارة في نظام أو تطبيق ضعيف. تستغل هذه الهجمات نقاط الضعف التي تسمح للمهاجم بإدخال أوامر أو بيانات غير مصرح بها في النظام، والتي يمكن بعد ذلك تنفيذها بواسطة النظام.

أنواع هجمات الحقن

حقن الأوامر Command Injection

يستهدف هذا الهجوم المواقع التي تسمح للمستخدمين بتنفيذ أوامر على الخادم. من خلال حقن أوامر ضارة في حقول الإدخال لموقع ويب، يمكن للمهاجمين خداع الخادم لتنفيذ أوامرهم، مما قد يعطيهم السيطرة على الخادم أو الوصول إلى الملفات الحساسة.

حقن SQL SQL Injection (SQLi)

يستهدف هجوم المواقع التي تستخدم قواعد بيانات SQL. من خلال حقن كود SQL ضار في حقول الإدخال لموقع ويب، يمكن للمهاجمين خداع قاعدة البيانات لكشف معلومات حساسة أو حتى تعديل أو حذف البيانات.

البرمجة النصية عبر المواقع Cross-Site Scripting (XSS)

يستهدف هجوم مواقع الويب التي تسمح للمستخدمين بإدخال البيانات التي يتم عرضها بعد ذلك للمستخدمين الآخرين. من خلال إدخال نصوص برمجية ضارة في حقول إدخال موقع الويب، يمكن للمهاجمين خداع موقع الويب لتنفيذ نصوصهم البرمجية في متصفحات المستخدمين الآخرين، مما قد يؤدي إلى سرقة ملفات تعريف الارتباط الخاصة بهم أو الرموز المميزة للجلسة أو غيرها من المعلومات الحساسة.

1 حقن SQL Injection

هجوم حقن SQLi هو نوع من الهجمات السيبرانية التي تستغل الثغرات الأمنية في تطبيقات الويب التي تتفاعل مع قواعد البيانات. وإليك كيف يعمل:

تحديد الثغرات الأمنية

بناء استعلامات SQL بناءً على هذه المدخلات دون التحقق من الصحة أو التصحيح المناسب.

المدخلات الضارة

إدخال تعليمات SQL ضارة: يُدخل المهاجم تعليمات SQL ضارة ضمن استعلام يبدو شرعيًا، ثم يرسلها إلى خادم قاعدة البيانات.

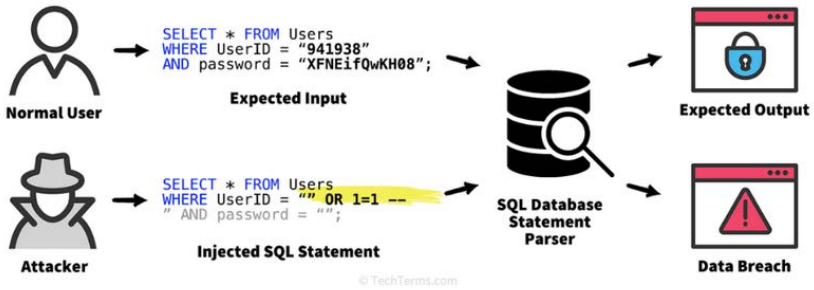
تنفيذ تعليمات SQL الضارة: ينفّذ خادم قاعدة البيانات هذه التعليمات على أنها جزء من استعلام SQL شرعي، مما قد يسمح للمهاجم بالوصول إلى البيانات أو تعديلها.

الإجراءات غير المصرح بها

اعتمادًا على طبيعة كود SQL الذي تم إدخاله، يمكن للمهاجمين:

- **استرجاع البيانات الحساسة من قاعدة البيانات**
- **تعديل أو حذف البيانات المخزنة في قاعدة البيانات**
- **تنفيذ الأوامر الإدارية والسيطرة على نظام قاعدة البيانات بأكمله**

مثال: لنفترض أن تطبيق ويب يستخدم إدخال المستخدم لإنشاء استعلام SQL لمصادقة المستخدمين أثناء تسجيل الدخول:



في هذه الحالة: تكون قيمة 'OR 1=1' صحيحة دائمًا، مما يؤدي إلى تجاوز التحقق من كلمة المرور. يعلق '--' على بقية الاستعلام، متجاهلاً شرط كلمة المرور.

ونتيجة لذلك، يمكن للمهاجم تسجيل الدخول كمسؤول دون معرفة كلمة المرور، مستغلًا ثغرة حقن SQL في التطبيق.

2 حقن الأوامر Command Injection

هجوم حقن الأوامر هو نوع من الثغرات الأمنية حيث يمكن للمهاجم تنفيذ أوامر خبيثة على نظام التشغيل المضيف من خلال تطبيق يعاني من ثغرات. يحدث هذا عادةً عندما يقوم التطبيق بتمرير مدخلات المستخدم غير الآمنة إلى واجهة الأوامر أو مفسر الأوامر النظامية.

كيف تعمل؟

إدخال المستخدم

يقبل التطبيق الإدخال من المستخدم.

تنفيذ الأمر

يتضمن التطبيق هذا الإدخال في أمر النظام دون التحقق من الصحة أو التعقيم المناسب.

الأوامر الضارة

يقوم المهاجم بصياغة الإدخال ليشمل أوامر ضارة، والتي ينفذها التطبيق بامتيازاته الخاصة.

كيفية عمل المواقع الإلكترونية
مركـز القيـادة

لغات البرمجة

تستخدم خوادم الويب لغات خاصة (مثل PHP أو Python أو NodeJS) لفهم هذه الطلبات ومعالجتها.

مكالمات النظام System Calls

في بعض الأحيان، تحتاج هذه اللغات إلى التحدث إلى نظام تشغيل الخادم للقيام بأشياء مثل قراءة الملفات أو تنفيذ الأوامر.

خدعة الهاكر: حقن الأوامر

يمكن للمتسللين استغلال هذا الاتصال عن طريق إدخال أوامرهم الخاصة في حقول الإدخال الخاصة بموقع الويب.

على سبيل المثال

قد يتوقع منك شريط البحث أن تكتب كلمة رئيسية،

ولكن يمكن للمتسلل أن يكتب:

```
Bash
whoami;
```

يخبر هذا الأمر الخادم بالكشف عن اسم المستخدم الذي يعمل تحته، مما يمنح المتسلل معلومات قيمة.

اكتشاف العلامات:

حقن الأوامر الأعمى:

لا يعرض موقع الويب ناتج الأمر الذي تم تنفيذه. لذلك يعتمد المهاجم على مؤشرات غير مباشرة، مثل ملاحظة التأخير في الاستجابة أو التحقق من حدوث تغييرات في الملفات، لمعرفة ما إذا كان الهجوم قد نجح.

حقن الأوامر المرئي (Visible Command Injection)

يعرض موقع الويب ناتج الأمر الذي تم تنفيذه مباشرة على الصفحة، مما يسهّل على المهاجم معرفة نتيجة الأمر. وفي المقابل، يسهّل ذلك أيضًا على مطوري الموقع اكتشاف المشكلة وإصلاحها.

مجموعة أدوات القراصنة: أوامر مفيدة Useful Payloads

Windows

whoami - يكشف اسم مستخدم الخادم
dir - يسرد الملفات والمجلدات
ping - يخلق تأخيرًا زمنيًا (يستخدم في حقن الأوامر الأعمى)
timeout - طريقة أخرى لإنشاء تأخير الوقت

Linux

whoami - يكشف عن اسم مستخدم الخادم
ls -يسرد الملفات والمجلدات
ping - يخلق تأخيرًا زمنيًا (يستخدم في حقن الأوامر الأعمى)
sleep - طريقة أخرى لإنشاء تأخير الوقت
nc - يمكن استخدامها لإنشاء باب خلفي في الخادم

كسر المصادقة
Broken Authentication

ثغرات أمنية في عملية المصادقة تسمح للمهاجمين باختراق حسابات المستخدمين. يمكن أن يحدث هذا بسبب ضعف كلمات المرور أو سوء إدارة الجلسة أو عيوب أخرى في الطريقة التي يتعامل بها موقع الويب مع مصادقة المستخدم

تشمل هجمات كسر المصادقة الشائعة

حشو بيانات الاعتماد
Credential stuffing
استخدام أسماء المستخدمين وكلمات المرور المسروقة للوصول إلى حسابات أخرى

هجمات القوة الغاشمة
Brute force attacks
تخمين كلمة مرور المستخدم من خلال تجربة العديد من المجموعات المختلفة

اختطاف الجلسة
Session hijacking
سرقة ملف تعريف ارتباط جلسة المستخدم، مما يسمح للمهاجم بانتحال شخصية المستخدم والوصول إلى حسابه.

كيف يحدث ذلك؟

قد تحدث المصادقة المعطّلة عندما:
-يسمح الموقع باستخدام كلمات مرور ضعيفة أو سهلة التخمين.
-لا يفرض الموقع حدًا لعدد محاولات تسجيل الدخول الفاشلة.
- يستخدم آليات غير آمنة لإدارة الجلسات.
-لا يوفّر وسائل مصادقة قوية، مثل المصادقة متعددة العوامل (MFA).
- يحتوي على آليات غير آمنة لإعادة تعيين كلمة المرور أو استعادة الحساب.

في بعض الأحيان، يترك المطورون عن غير قصد معلومات حساسة في هذا الرمز، مثل:
- بيانات اعتماد تسجيل الدخول (Login credentials)
- الروابط المخفية
- بيانات حساسة أخرى مفاتيح واجهة برمجة التطبيقات API Keys ، والتعليقات التي تحتوي على ملاحظات داخلية، وما إلى ذلك

ما الذي يمكن أن يؤدي إليه؟

- سرقة الهوية سرقة معلوماتك الشخصية وانتحال شخصيتك
- الاحتيال المالي استخدم معلومات بطاقة الائتمان لإجراء عمليات شراء غير مصرح بها
- الابتزاز التهديد بكشف معلومات حساسة ما لم يتم دفع فدية للمهاجم.

كيفية اكتشاف ذلك؟

- التحقق مما إذا كان الموقع يقبل كلمات مرور ضعيفة.
- اختبار ما إذا كان الموقع يقيّد محاولات تسجيل الدخول المتكررة والفاشلة.
- التأكد من تغيّر معرّف الجلسة (Session ID) بعد تسجيل الدخول.
- التحقق من استخدام الموقع لاتصال آمن (HTTPS) وتوفيره للمصادقة متعددة العوامل (MFA).

البحث عن الكلمات

ضع دائرة حول الكلمات أدناه ذات الصلة ب"هجمات الويب"

SOCIAL	SCRIPTING	MALICIOUS
URGENCY	REQUESTS	ENGINEERING
SPOOFING	GENERIC	AUTHORIZATION
WEBSITES	INJECTION	AUTHENTICATION
PAYMENT	PHISHING	VULNERABILITIES

T	R	A	U	T	H	E	N	T	I	C	A	T	I	O	N	R	P	E	C
O	G	M	U	N	I	C	A	T	I	O	N	O	X	Y	H	A	E	O	R
Y	E	I	P	I	B	W	T	A	P	M	O	C	R	E	Y	T	I	N	E
A	N	E	T	H	A	E	I	H	S	D	N	E	I	M	F	U	O	V	Q
V	E	R	P	M	I	B	I	O	A	T	N	I	E	A	T	R	E	S	U
U	R	Y	T	S	E	S	C	H	R	D	L	N	E	L	N	G	M	M	E
L	I	E	S	C	S	I	H	P	P	O	T	T	E	I	E	E	R	F	S
N	C	P	I	Y	A	T	M	I	R	E	V	O	L	C	A	N	T	P	T
E	L	R	F	L	S	E	F	S	N	F	E	F	F	I	N	C	O	C	S
R	P	A	R	T	N	S	R	R	E	G	O	T	P	O	T	Y	M	P	S
A	U	T	H	O	R	I	Z	A	T	I	O	N	I	U	R	A	O	I	M
B	E	C	R	E	P	S	E	R	D	N	E	I	R	S	S	O	O	R	P
I	T	E	N	G	I	N	E	E	R	I	N	G	C	N	F	T	A	M	U
T	E	I	T	N	E	M	M	I	T	M	O	C	I	I	M	A	T	N	I
I	E	R	T	I	I	N	J	E	C	T	I	O	N	O	C	M	M	U	N
E	M	S	C	S	S	E	N	O	H	Y	T	G	L	A	P	O	R	T	P
S	S	S	C	A	R	T	S	C	R	I	P	T	I	N	G	I	L	I	A

مختبرو الاختراق
Penertation Testers

مختبرو الاختراق، يُطلق عليهم غالباً "Pen testers" أو المتسللون الأخلاقيون "Ethical hackers"، هم متخصصون في مجال الأمن السيبراني يقومون بمحاكاة الهجمات الإلكترونية على نظام أو شبكة أو تطبيق لتحديد الثغرات الأمنية. هدفهم هو العثور على نقاط الضعف وإصلاحها قبل أن يتمكن المتسللون الخبيثون من استغلالها

ماذا يعملون؟

1. محاكاة الهجمات

يستخدم مختبرو الاختراق تقنيات مشابهة لتلك التي يستخدمها المهاجمون الحقيقيون لاختبار أمان النظام

2. تحديد نقاط الضعف

يبحثون عن نقاط الضعف مثل الأخطاء أو التعليمات الخاطئة أو البرامج القديمة

3. نتائج التقرير

بعد الاختبار، يقدمون تقريرًا تفصيليًا بالنتائج والتوصيات لإصلاح المشكلات

4. تعزيز الأمان

يعزز مختبرو الاختراق أمن المؤسسة من خلال اكتشاف نقاط الضعف والمساعدة في معالجتها قبل أن يستغلها المهاجمون

أفضل ممارسات
تطبيقات الويب

تأمين تطبيقات الويب

ممارسات الترميز coding الآمن :

التحقق من صحة المدخلات – تحقّق دائمًا من مدخلات المستخدم في موقع الويب للتأكد من أنها تتوافق مع نوع البيانات المطلوب، مثل الاسم أو عنوان البريد الإلكتروني، وأنها لا تحتوي على تعليمات برمجية ضارة.

ترميز المخرجات – هو أسلوب أمني يحوّل البيانات قبل عرضها في صفحة الويب إلى صيغة آمنة، بحيث يتعامل معها المتصفح كنص عادي بدل تنفيذها كتعليمات برمجية. يساعد ذلك على حماية المستخدمين من الهجمات مثل XSS.

الاستعلامات ذات المعلمات(Parameterized Queries for SQLi) – درع قاعدة البيانات لمواقع الويب التي تستخدم قواعد البيانات، تشبه الاستعلامات ذات المعلمات درعًا خاصًا يحمي من هجمات حقن SQL. حيث يتم فصل البيانات التي يقدمها المستخدم عن الأوامر الفعلية التي تتحدث إلى قاعدة البيانات

إفلات الأحرف الخاصة – قبل تنفيذ أي أمر، يتأكد التطبيق من التعامل مع الأحرف الخاصة التي يُدخلها المستخدم على أنها جزء من النص فقط، وليس كأوامر يمكن تنفيذها. يساعد ذلك على منع المهاجمين من استغلال هذه الأحرف لتنفيذ أوامر ضارة.

معالجة الأخطاء – تخيّل أنك لا تكشف أوراقك أثناء اللعب. بالطريقة نفسها، لا ينبغي أن تكشف رسائل الخطأ تفاصيل النظام للمهاجمين، بل تعرض رسالة عامة فقط.

تقليل الامتيازات – أساس الحاجة إلى المعرفة هو تصور كل جزء من تطبيق الويب الخاص بك كحارس مختلف. يجب أن يكون لدى كل حارس فقط المفاتيح التي يحتاجها للقيام بعمله المحدد، وليس الوصول إلى القلعة بأكملها

التحديثات المنتظمة وإدارة التصحيحات
Regular Updates and Patch Management

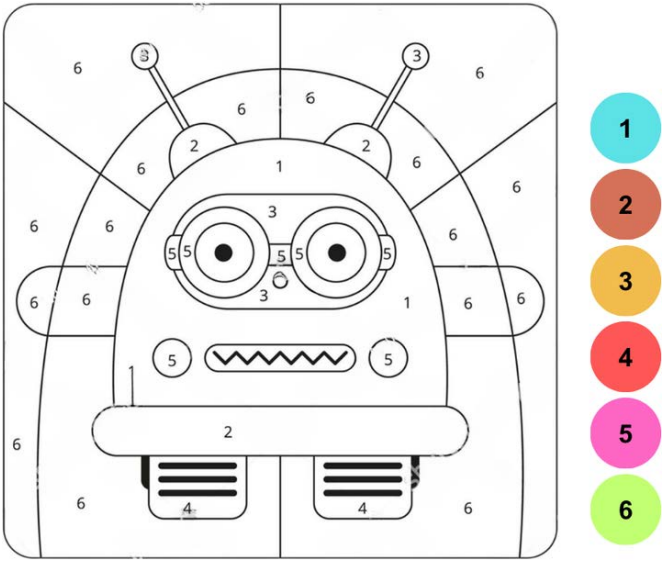
الممارسات الحاسمة في أمن الويب التي تتضمن التحديث المستمر للبرامج والأنظمة للحماية من نقاط الضعف والتهديدات.

سبب أهميتها:

1. **إصلاح نقاط الضعف**
2. **ثغرات البرمجيات :** تعمل التحديثات المنتظمة على إصلاح العيوب الأمنية.
3. **التصحيحات الأمنية:** يؤدي تطبيق التصحيحات إلى سد الثغرات الأمنية
4. **تحسين الميزات والأداء**
5. **ميزات جديدة:** جعل الأنظمة أكثر كفاءة وأمانًا
6. **إصلاحات الأخطاء:** تعمل التحديثات على حل الأخطاء التي يحتمل استغلالها
7. **البقاء متقدما على التهديدات**
8. **التهديدات المتطورة:** التهديدات السيبرانية تتطور باستمرار
9. **الامتثال للقوانين والمعايير العالمية:** تتطلب العديد من اللوائح أنظمة مُحدثة

قم بتلوين الصورة

استخدم رمز اللون لإكمال الصورة



المصادقة والتفويض
Authentication and Authorization

الحماية ضد كسر المصادقة
Protecting Against Broken Authentication

استخدم سياسات كلمة المرور القوية

التعقيد: تتطلب كلمات المرور أن تكون مزيجًا من الأحرف (الكبيرة والصغيرة) والأرقام والأحرف الخاصة.

الطول: فرض حد أدنى للطول (على سبيل المثال، 12 حرفًا على الأقل).

انتهاء الصلاحية: تنفيذ تغييرات دورية لكلمة المرور.

حظر إعادة الاستخدام: منع المستخدمين من إعادة استخدام كلمات المرور القديمة.

تخزين كلمات المرور بشكل آمن

التجزئة: استخدم خوارزميات التجزئة القوية والمملحة salted hashing algorithms (على سبيل المثال، Argon2، bcrypt) لتخزين كلمات المرور.

تجنب النص العادي: لا تقم مطلقًا بتخزين كلمات المرور في نص عادي أو باستخدام تشفير قابل للعكس.

الحد من محاولات تسجيل الدخول

تحديد المعدل: تطبيق سياسة العدد المحدود لعملية تسجيل الدخول من عنوان IP واحد.

تأمين الحساب: قفل الحسابات مؤقتًا بعد عدد معين من محاولات تسجيل الدخول الفاشلة.

المصادقة المتقدمة
Advanced Authentication

تنفيذ المصادقة متعددة العوامل Multi-Factor Authentication (MFA)

يتطلب MFA من المستخدمين توفير عاملي تحقق أو أكثر للوصول. يضيف طبقة إضافية من الأمان تتجاوز مجرد كلمة المرور، مما يجعل من الصعب على المهاجمين الوصول إليها.

استخدم إدارة الجلسة الآمنة:

معرفات الجلسة Session IDs: إنشاء معرفات جلسة فريدة لكل تسجيل دخول.

المهلات Timeouts: تسجيل الخروج تلقائيًا بعد فترة من عدم النشاط.

ملفات تعريف الارتباط الآمنة Secure Cookies: استخدام ملفات تعريف الارتباط الآمنة (HTTPS) وHttpOnly لتخزين معلومات الجلسة

حماية البيانات

التشفير Encryption

هي طريقة لتحويل البيانات القابلة للقراءة (نص عادي) إلى تنسيق غير قابل للقراءة (نص مشفر) لحمايتها من الوصول غير المصرح به. تضمن هذه العملية أن الأطراف المصرح لها فقط هي التي يمكنها قراءة المعلومات الأصلية باستخدام مفتاح خاص.

فيما يلي تفصيل بسيط لكيفية عمل التشفير:

نص عادي Plaintext: البيانات أو الرسالة الأصلية القابلة للقراءة والتي تحتاج إلى الحماية.

خوارزمية التشفير Encryption Algorithm: مجموعة من القواعد الرياضية المستخدمة لتحويل النص العادي إلى نص مشفر.

المفتاح Key: قيمة سرية تستخدمها خوارزمية التشفير لإجراء التحويل. فقط أولئك الذين لديهم المفتاح الصحيح يمكنهم فك تشفير النص المشفر مرة أخرى إلى نص عادي.

النص المشفر Ciphertext: البيانات الناتجة المشوشة وغير القابلة للقراءة بعد التشفير.

فوائد التشفير:

السرية: يضمن أن تظل المعلومات الحساسة خاصة ولا يمكن الوصول إليها إلا للأفراد المصرح لهم بذلك.

سلامة البيانات: تساعد على التحقق من عدم تغيير البيانات أثناء الإرسال.

المصادقة: التأكد من هوية الأطراف المشاركة في الاتصال.

عدم الرفض: يضمن أن المرسل لا يستطيع إنكار أنه أرسل الرسالة، وذلك باستخدام وسائل تحقق مثل التوقيع الرقمي.

مهمّة

اختر كلمة المرور الأقوى.

تذكر أن كلمة المرور القوية
تحافظ على أمان حساباتك!

- [ ] sunshine123
- [ ] P@ssw0rd!2024
- [ ] aB1!z9X2?mY7!L3

حماية البيانات

استخدم مفتاح الإزاحة 2+ لتشفير الجملة التالية
SECURITY FIRST

فك تشفير الجملة التالية باستخدام مفتاح الإزاحة 2-
JGNNQ YQTNF

تخزين آمن

يشير التخزين الآمن إلى الأساليب والممارسات المستخدمة لحماية البيانات الحساسة من الوصول غير المصرح به والتلاعب والفقدان. يتضمن ذلك استخدام تقنيات وبروتوكولات مختلفة لضمان بقاء البيانات سرية وسليمة سواء تم تخزينها على أجهزة مادية أو بتنسيقات رقمية.

المكونات الرئيسية للتخزين الآمن:

التشفير Encryption: يتم تشفير البيانات قبل تخزينها باستخدام خوارزميات تشفير قوية. يمكن تطبيق التشفير على كل من البيانات غير النشطة (البيانات المخزنة) والبيانات المنقولة (البيانات التي يتم نقلها).

ضوابط الوصول Access Controls : يضمن تنفيذ ضوابط الوصول الصارمة أن المستخدمين والأنظمة المصرح لهم فقط هم من يمكنهم الوصول إلى البيانات المخزنة. يمكن التحكم في الوصول من خلال مصادقة المستخدم والصلاحيات والأدوار.

النسخ الاحتياطية Backups: يتم إجراء نسخ احتياطية منتظمة للبيانات لمنع فقدان البيانات في حالة فشل الأجهزة، أو الحذف العرضي، أو غيرها من الكوارث. يجب أيضًا تخزين النسخ الاحتياطية بشكل آمن، وغالبًا ما يكون ذلك في موقع مختلف عن البيانات الأصلية.

سلامة البيانات

تشير سلامة البيانات إلى دقة البيانات واتساقها وموثوقيتها طوال دورة حياتها. ويعني ضمان سلامة البيانات أن البيانات دقيقة وتبقى دون تغيير ما لم يتم تغييرها من خلال العمليات المعتمدة. إنه جانب حاسم لإدارة البيانات والأمن السيبراني وتصميم قواعد البيانات.

التجزئة Hashing هي تقنية تشفير تستخدم لضمان سلامة البيانات عن طريق إنشاء سلسلة ذات حجم ثابت من الأحرف (تسمى قيمة التجزئة أو رمز التجزئة) من بيانات الإدخال بأي حجم. تمثل قيمة التجزئة هذه بصمة فريدة للبيانات الأصلية.

عمليات تدقيق أمنية منتظمة واختبارات الاختراق

اختبارات الاختراق
Penetration Testing

اختبار الاختراق، والذي يُختصر غالبًا باسم "pentesting"، هو عبارة عن محاكاة استباقية ومصرح بها لهجوم إلكتروني على نظام كمبيوتر أو شبكة أو تطبيق ويب لتقييم أمانه. الهدف من اختبار الاختراق هو تحديد نقاط الضعف التي يمكن استغلالها من قبل المهاجمين الضارين.

أنواع اختبارات الاختراق

اختبار الصندوق الأسود

Black Box Testing

ليس لدى المخترقين الأخلاقيين أي معرفة بالبنية الداخلية لتطبيق الويب الخاص بك. ويشبه ذلك اختبار سيارة بقيادتها فقط دون فتح غطاء المحرك لمعرفة كيفية عملها.

اختبار الصندوق الأبيض

White Box Testing

يتمتع المخترقون الأخلاقيون بالمعرفة الكاملة بالنص البرمجي لتطبيق الويب الخاص بك وبنيته. ويشبه ذلك فحص سيارة بعد فتح غطاء المحرك، حيث يمكن رؤية جميع الأجزاء واكتشاف الأعطال بدقة.

عمليات التدقيق الأمني
Security Audit

هو عملية مراجعة وفحص الأنظمة والسياسات والإجراءات الأمنية للتأكد من أنها تحمي المعلومات والأنظمة بشكل صحيح، وللكشف عن أي نقاط ضعف تحتاج إلى تحسين.

الجوانب الرئيسية لعمليات التدقيق الأمني

تقييم الضوابط الأمنية

يتضمن ذلك فحص جدران الحماية، وأنظمة كشف التسلل، وضوابط الوصول، وآليات التشفير، وغيرها.

تحديد نقاط الضعف

فحص الثغرات الأمنية واختبار الاختراق ومراجعة التعليمات البرمجية للكشف عن نقاط الضعف في تطبيق الويب أو موقع الويب.

التحقق من الامتثال

التزام عمليات التدقيق بمعايير الأمان واللوائح وأفضل الممارسات ذات الصلة

تقييم المخاطر

تحديد أولويات المخاطر بناءً على تأثيرها المحتمل واحتمال استغلالها.

أمن الويب

الشـبكات هي ببسـاطة الأشـياء المتصـلة.
الشبكة هي ارتباط بين جهازين أو أكثر يمكنهما نقل واستقبال البيانات والمعلومات.
يمكن أن يكون الاتصـال سـلكياً (مثل الكابلات أو أسلاك الهاتف)
أو لاسـلكياً (مثل الموجات الراديوية أو الموجات الميكروية).
تتيح الشـبكة لنا مشـاركة الموارد، وتبادل الملفات، والتواصل.

الشبكات مدمجة في حياتنا اليومية. سـواء كان ذلك لجمع البيانات عن الطقس، أو توصيل الكهرباء إلى المنازل، أو حتى تحديد من له حق المرور على الطريق. نظراً لأن الشبكات مدمجة بشـكل كبير في العصر الحديث، فإن الشـبكات هي مفهوم أساسي يجب فهمه في الأمن السـيبراني.

يمكن العثور على الشبكات في جميع جوانب الحيـاة:

- نظام النقل العام في المدينة
- البنية التحتية مثل الشبكة الوطنية للطاقة الكهربائية
- الاجتماع والتواصل مع لجيرانك.

ماهو
الإنترنت؟

الإنترنت هو شبكة عملاقة تتكون من العديد من الشبكات الصغيرة داخلها.

تاريخ الإنترنت

كانت النسخة الأولى من الإنترنت ضمن مشروع ARPANET في أواخر الستينيات. كان هذا المشروع ممولًا من قبل وزارة الدفاع الأمريكية وكان أول شبكة موثقة تعمل.

ومع ذلك، لم يُخترع الإنترنت كما نعرفه إلا في عام 1989 عندما ابتكر تيم برنرز-لي Tim Berners-Lee الشبكة العالمية (WWW).

الشبكة العامة

الشبكة العامة هي نوع من الشبكات التي يمكن لأي شخص، أي العامة، الوصول إليها ومن خلالها يمكن الاتصال بشبكات أخرى أو بالإنترنت. وهذا على عكس الشبكة الخاصة، حيث يتم وضع قيود وقواعد وصول لتقييد الوصول إلى عدد قليل فقط.

الشبكة الخاصة

الشبكات الخاصة هي شبكات أصغر تُستخدم عادةً في المنازل والشركات والمنظمات لتوفير التواصل الآمن وتبادل البيانات.
تقتصر على مجموعة محددة من المستخدمين أو الأجهزة.

بروتوكولات
الشـــبكة

هو مجموعة من القواعد التي تحدد كيفية نقل البيانات بين أجهزة مختلفة في شبكة بغض النظر عن أي اختلافات في عملياتها الداخلية أو هيكلها أو تصميمها.

لكي تتواصل الأجهزة معًا، يجب أن يدعم كلا الجهازين نفس البروتوكول أو سيتعين استخدام بوابة لترجمة التواصل.

ثلاثة انواع من بروتوكولات الشبكة

أمان الشبكة

بروتوكولات الأمان هي بروتوكولات تستخدم تدابير الأمان مثل التشفير والترميز لحماية البيانات. من أمثلتها: SFTP وSSL وHTTPS.

الاتصال بالشبكة

مجموعة من البروتوكولات المستخدمة لوضع قواعد وتنسيقات (مثل البنية والتزامن والدلالات) لتبادل البيانات عبر الشبكة.
تشمل أنواع بروتوكولات الاتصال بالشبكة: TCP وUDP و IP وHTTP وIRC وBGP وARP.

إدارة الشبكة

تحدد هذه البروتوكولات السياسات المصممة لمراقبة وإدارة وصيانة الشبكة. من أمثلتها:
Syslog
NETCONF
ICMP

عنوان IP

عنوان IP (أو بروتوكول الإنترنت) هو عنوان فريد يستخدم لتحديد جهاز حاسوب عند الاتصال بالإنترنت. يمكن استخدام عنوان IP كطريقة لتحديد مضيف على الشبكة لفترة من الزمن، حيث يمكن بعد ذلك ربط هذا العنوان بجهاز آخر دون تغيير عنوان IP.

يمكن أن تتغير عناوين IP من جهاز إلى جهاز ولكن لا يمكن لجهازين امتلاك نفس العنوان في نفس الوقت ضمن الشبكة نفسها

أنواع عنوان IP

1. عنوان IP الخاص

عنوان IP الخاص هو العنوان الذي يُعطى للأجهزة المتصلة بشبكة خاصة مثل الشبكة المنزلية أو شبكة العمل. لا يمكن الوصول إلى هذا العنوان من خارج هذه الشبكة الخاصة.

2. عنوان IP العام

هو العنوان الذي يُعطى لشبكة خاصة عند الاتصال بالإنترنت وهو فريد لجميع المستخدمين. تُقدم عناوين IP العامة من قبل مزود خدمة الإنترنت (ISP) مقابل رسوم شهرية.

3. عناوين IP الثابتة والديناميكية

العنوان الثابت (Static IP) هو عنوان لا يتغير، ويُعيَّن يدويًا أو يُخصص دائمًا لجهاز معين، لذلك يُستخدم غالبًا مع الخوادم والطابعات وأجهزة الشبكة التي يجب الوصول إليها باستخدام العنوان نفسه باستمرار.

أما العنوان الديناميكي (Dynamic IP) فيُعيَّن تلقائيًا للجهاز عند اتصاله بالشبكة بواسطة بروتوكول التهيئة الآلية للمضيفين (DHCP)، وقد يتغير عند إعادة تشغيل الجهاز أو إعادة الاتصال بالشبكة. ويُستخدم هذا النوع في معظم المنازل والمدارس لأنه يسهّل إدارة الشبكة ويوزع عناوين IP على الأجهزة تلقائيًا.

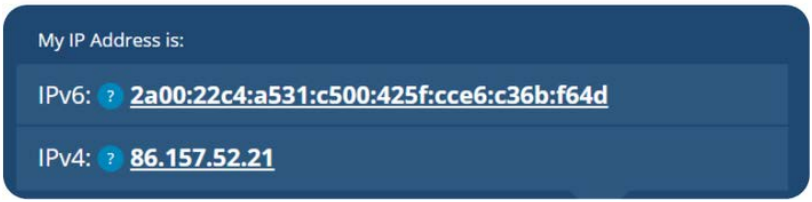
بروتوكول IPv4

بروتوكول IPv4 هو عنوان فريد على الشبكة يتكون من 32 binary bits. يُعد IPv4 نسخة قديمة تستخدم ما يصل إلى 4 مليارات عنوان IP فقط، لكنه لا يزال قيد الاستخدام. يتم التعبير عن IPv4 بأربع مجموعات من الأرقام، كل مجموعة مفصولة بنقطة. كل مجموعة هي تمثيل عشري لرقم ثنائي مكون من ثمانية أرقام، ويُطلق عليه أيضًا اسم "أوكتت". يتم حساب هذا الرقم من خلال تقنية تعرف بـ "توجيه IP وتقسيم الشبكة".

يمكن أن يتراوح كل أوكتت بين 00000000 و 11111111 بالثنائي و بين 0 و 255 بالعشري. بعض الأرقام في النطاقات المذكورة أعلاه محجوزة لأغراض محددة على الشبكات التي تستخدم بروتوكول TCP/IP.

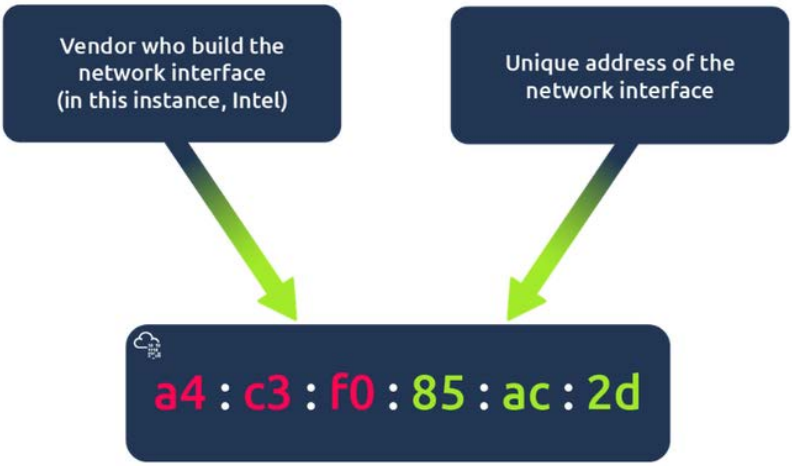
بروتوكول IPv6

هو الجيل التالي للبنية التحتية القديمة للعناوين،تم تصميم ipv6 لتجاوز القيود المتعلقة ب ipv4.
هو عنوان فريد يتكون من 128 binary bits. يتم التعبير عنه في ثماني مجموعات من الارقام ذات نظام العد الست عشري و كل مجموعة مفصولة بنقطتين.



عناوين MAC

تحتوي الأجهزة الموجودة على شبكة على واجهة شبكة مادية، وهي لوحة ميكروشيب توجد على لوحة الأم للجهاز. يتم تعيين عنوان فريد لهذه الواجهة في المصنع الذي تم بناؤها فيه، يُعرف بعنوان Media Access Control (MAC).



عنوان MAC هو رقم سداسي عشري مكون من اثني عشر حرفًا (نظام عد أساسي ستة عشر يُستخدم في الحوسبة لتمثيل الأرقام) مقسم إلى مجموعات من اثنين ومفصول بنقطتين. تُعتبر هذه النقط نقط فصل. على سبيل المثال، a4:c3:f0:85:ac:2d. تمثل الأحرف الستة الأولى الشركة التي صنعت واجهة الشبكة، والستة الأخيرة هي رقم فريد.

يمكن تزوير عنوان MAC في عملية تُعرف باسم انتحال عنوان MAC Spoofing (MAC). في هذه العملية، يستخدم جهاز عنوان MAC الخاص بجهاز آخر ليظهر على الشبكة وكأنه ذلك الجهاز. وقد يؤدي ذلك إلى تجاوز بعض وسائل الحماية التي تعتمد فقط على عنوان MAC للتحقق من هوية الأجهزة.

Ping (ICMP)

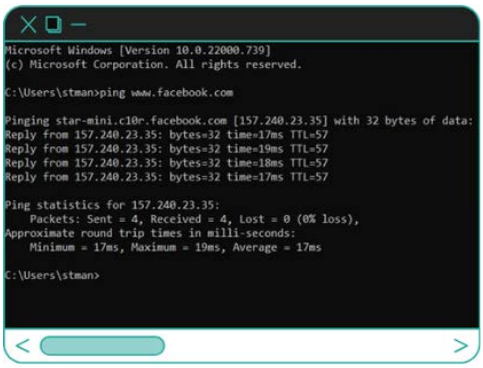
Ping هو أحد أكثر أدوات الشبكة الأساسية المتاحة لنا، يستخدم Ping حزم ICMP(بروتوكول رسائل التحكم بالإنترنت) لتحديد أداء الاتصال بين الأجهزة.

عند إصدار أمر Ping ، يتم إرسال حزمة طلب echo إلى العنوان المحدد. عندما يستلم المضيف البعيد طلب echo ، يستجيب بحزمة رد echo .

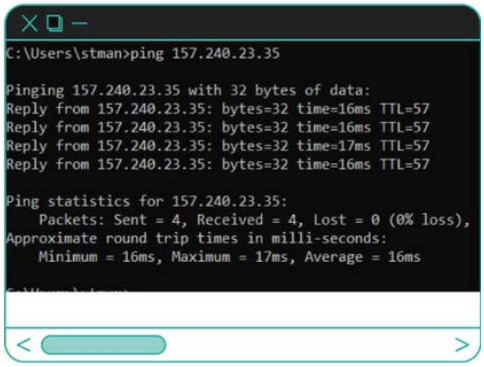
صيغة أمر Ping الأساسي متشابهة لكل من أنظمة ويندوز ولينيكس. يكفي كتابة "ping" متبوعًا بعنوان URL أو عنوان IP الوجهة.

بشكل افتراضي، يرسل أمر Ping عدة طلبات echo ، عادةً أربع أو خمس. يتم عرض نتيجة كل طلب echo ، موضحًا ما إذا كان الطلب قد تلقى استجابة ناجحة، وعدد البايتات التي تم تلقيها في الرد، ومدة بقاء الحزمة (TTL)، وكم من الوقت استغرقت الاستجابة للوصول، بالإضافة إلى إحصاءات حول فقدان الحزم وأوقات الرحلة ذهابًا وإيابًا.

1. Ping www.facebook.com



2. Ping 157.240.23.35



أنواع
الشـــبكات

هناك أنواع مختلفة من الشبكات بناءً على حجمها وكذلك الغرض منها. يعتمد حجم الشبكة على المنطقة الجغرافية وعدد أجهزة الحاسوب. يمكن أن تكون الأجهزة مترابطة داخل غرفة واحدة أو عبر العالم.

أنواع رئيسية

PAN
(شبكة المنطقة الشخصية)

هي أصغر نوع من الشبكات وتستخدم لربط الأجهزة الشخصية مثل الهواتف الذكية والأجهزة اللوحية وأجهزة الحواسيب الشخصية لإقامة الاتصال الرقمي والاتصال بالإنترنت.

LAN
(شبكة المنطقة المحلية)

هي اتصال مجموعة من أجهزة الحواسيب والأجهزة الطرفية داخل موقع واحد. يمكن إعداد شبكات لان كشبكات سلكية (LAN) أو لاسلكية (WLAN).

إنها شبكة بسيطة وشائعة الاستخدام لمشاركة الموارد مثل الطابعات والألعاب والتطبيقات الأخرى. بشكل عام، تعتبر شبكة LAN شبكة خاصة مملوكة أو مُتحكم بها من قبل منظمة واحدة.

WAN
(شبكة المنطقة الواسـعة)

هي شبكة أكبر تنتشر في منطقة جغرافية واسعة مثل بلد أو منطقة أو قارة. يمكن اعتبار هذه الشبكة كاتصال بين عدة شبكات LAN عبر وسيط سلكي أو لاسلكي. وهي محدودة لمنظمة واحدة.

طوبولوجيات شبكة المنطقة المحلية
LAN Topologies

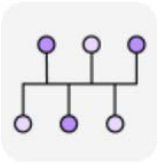
الطوبولوجيا الشبكية هي وصف تخطيطي لكيفية ترتيب الشبكة، بما في ذلك الوصفين المادي والمنطقي لكيفية إعداد الروابط والأجهزة والعقد لتتفاعل مع بعضها البعض.
الوصف المادي يوضح كيفية توصيل الأجهزة والكابلات معًا في الواقع.
الوصف المنطقي يوضح كيفية انتقال البيانات بين الأجهزة، بغض النظر عن طريقة توصيلها فعليًا

الطوبولوجيا النجمية

الفرضية الأساسية للطوبولوجيا النجمية هي أن الأجهزة متصلة بشكل فردي عبر جهاز شبكة مركزي مثل المبدل (switch) أو الموزع (hub). تعتبر هذه الطوبولوجيا الأكثر شيوعًا اليوم بسبب موثوقيتها وقابليتها للتوسع، على الرغم من تكلفتها.

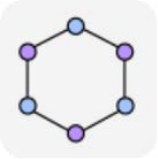
أي معلومات تُرسل إلى جهاز في هذه الطوبولوجيا يتم إرسالها عبر الجهاز المركزي الذي يتصل به.

الطوبولوجيا الخطية



هذا النوع من الاتصال يعتمد على اتصال واحد يُعرف بكابل العمود الفقري. نظرًا لأن كل شيء متصل بخط مستقيم من كابل مركزي واحد، فإنها طوبولوجيا فعّالة من حيث التكلفة، وسهلة الإعداد وإضافة العقد الجديدة.

طوبولوجيا الحلقة



وُصل الأجهزة على شكل حلقة، بحيث يتصل كل جهاز بجهازين فقط، أحدهما على يمينه والآخر على يساره. تنتقل البيانات من جهاز إلى آخر عبر الحلقة حتى تصل إلى وجهتها، وعادةً ما تتحرك في اتجاه واحد، مما يساعد على تنظيم حركة البيانات وتقليل حدوث التصادمات.

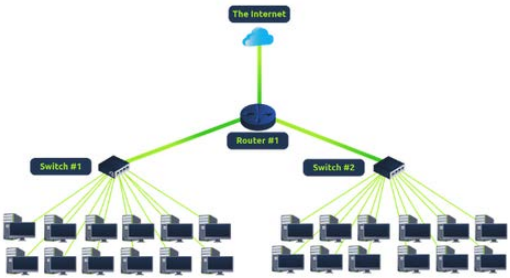
أجهزة
الشبكة

تساعد أجهزة الشبكة على نقل البيانات بشكل أسرع وآمن وفعّال عبر الشبكة.

غالبًا ما توجد المبدلات في الشبكات الكبيرة مثل الشركات والمدارس أو الشبكات ذات الحجم المماثل، حيث يوجد العديد من الأجهزة المتصلة بالشبكة. يمكن للمبدلات توصيل عدد كبير من الأجهزة من خلال توفر منافذ بعدد 4 أو 8 أو 16 أو 24 أو 32 أو 64 لجهاز التوصيل.

أجهزة الشبكة هي أجهزة مادية تساعد الأجهزة الأخرى مثل الكمبيوتر والطابعات وآلات الفاكس وغيرها من الأجهزة الإلكترونية على الاتصال بالشبكة.

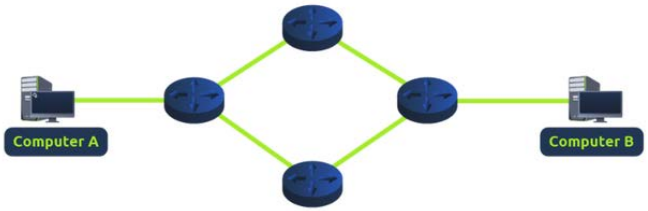
ما هو المبدل Switch ؟



المبدلات هي أجهزة مخصصة داخل الشبكة صممت لربط عدة أجهزة أخرى مثل أجهزة الحواسيب والطابعات أو أي جهاز آخر قابل للتوصيل بالشبكة عبر الإيثرنت. يتم توصيل هذه الأجهزة المختلفة بمنفذ على المبدل.

ما هو الموجه Router ؟

وظيفة الموجه هي ربط الشبكات وتمرير البيانات بينها. يقوم بذلك باستخدام التوجيه (ومن هنا جاء اسم "موجه"!). التوجيه هو المصطلح الذي يُطلق على عملية انتقال البيانات عبر الشبكات. يتضمن التوجيه إنشاء مسار بين الشبكات بحيث يمكن تسليم البيانات بنجاح.



التحزيم الفرعي
Subnetting

عندما يتم تقسيم شبكة كبيرة إلى شبكات أصغر للحفاظ على الأمان، يُعرف ذلك بالتحزيم الفرعي (Subnetting). وبالتالي، تصبح الصيانة أسهل بالنسبة للشبكات الأصغر.

يوفر التحزيم الفرعي مجموعة من الفوائد، بما في ذلك:
الكفاءة - الأمان - التحكم الكامل

كيف يعمل التحزيم الفرعي Subnetting ؟

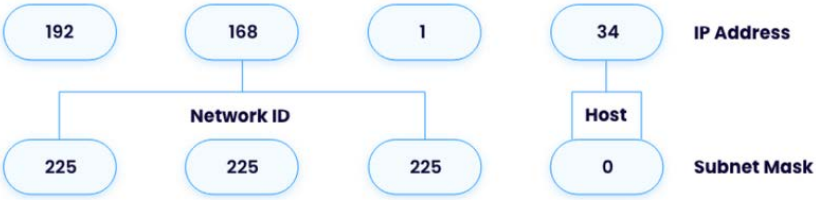
يبدأ عمل الشبكات الفرعية بحيث يتم أولاً تقسيم الشبكات الكبيرة إلى شبكات أصغر. للتواصل بين الشبكات الفرعية، يتم استخدام الموجهات. تسمح كل شبكة فرعية للأجهزة المتصلة بها بالتواصل مع بعضها البعض.

عند اتصال جهاز بالشبكة، يُخصَّص له عنوان IP لتمييزه عن بقية الأجهزة. ويتكوّن عنوان IP من جزأين: جزء الشبكة (Network ID) وجزء المضيف (Host ID). يحدد جزء الشبكة الشبكة التي ينتمي إليها الجهاز، بينما يحدد جزء المضيف الجهاز نفسه داخل تلك الشبكة.

ما هو قناع الشبكة الفرعية Subnet Mask ؟

قناع الشبكة الفرعية هو رقم يميز عنوان الشبكة وعنوان المضيف ضمن عنوان IP. الشبكة الفرعية هي شبكة أصغر ضمن شبكة أكبر تتطلب قناع شبكة فرعية.

لا يمكن معرفة أي جزء من عنوان IP يمثل الشبكة وأي جزء يمثل المضيف من خلال عنوان IP وحده. لذلك يُستخدم قناع الشبكة الفرعية لتحديد الحد الفاصل بينهما، مما يساعد الأجهزة على معرفة ما إذا كانت الوجهة ضمن الشبكة نفسها أم في شبكة أخرى.

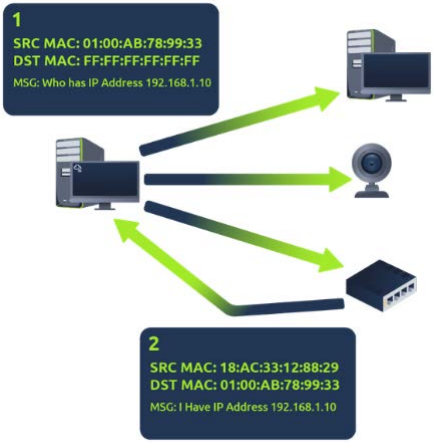


بروتوكول
ARP

يمكن أن تحتوي الأجهزة على معرّفين: عنوان MAC وعنوان IP. بروتوكول حل العناوين أو ARP باختصار هو التكنولوجيا المسؤولة عن تمكين الأجهزة من التعرف على نفسها في الشبكة.

ببساطة، يسمح بروتوكول ARP لجهاز ما بربط عنوان MAC الخاص به بعنوان IP على الشبكة. يحتفظ كل جهاز على الشبكة بسجل للعناوين MAC المرتبطة بالأجهزة الأخرى.

عندما ترغب الأجهزة في التواصل مع جهاز آخر، تقوم بإرسال بث إلى الشبكة بالكامل للبحث عن الجهاز المحدد. يمكن للأجهزة استخدام بروتوكول ARP للعثور على عنوان MAC (وبالتالي المعرف المادي) لجهاز ما من أجل التواصل.



كيف يعمل بروتوكول ARP؟

كل جهاز داخل الشبكة يمتلك سجلًا لتخزين المعلومات يُسمى الذاكرة المؤقتة (Cache). في سياق بروتوكول ARP، تقوم هذه الذاكرة المؤقتة بتخزين معرّفات الأجهزة الأخرى على الشبكة.

لربط هذين المعرفين معًا (عنوان IP وعنوان MAC)، يرسل بروتوكول ARP نوعين من الرسائل:

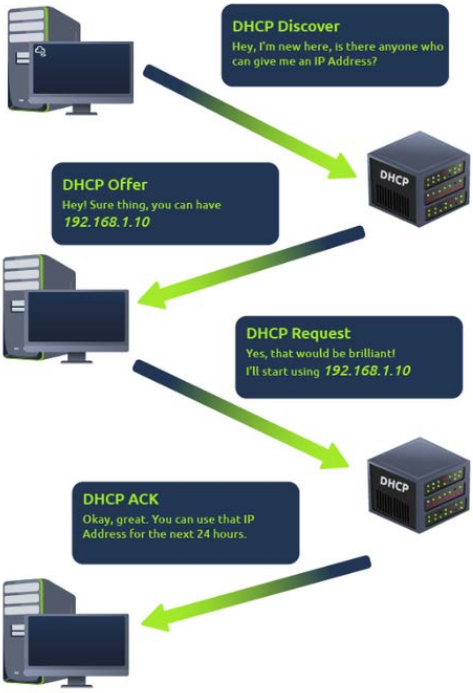
1. طلب ARP: يرسل الجهاز طلب ARP (ARP Request) إلى جميع الأجهزة في الشبكة المحلية، يسأل فيه: "من يملك عنوان IP هذا؟"

2. إجابة ARP: يرد الجهاز الذي يملك عنوان IP المطلوب برسالة ARP Reply تحتوي على عنوان MAC الخاص به.

بروتوكول
DHCP

يمكن تعيين عناوين IP إما يدويًا، عن طريق إدخالها فعليًا في الجهاز، أو تلقائيًا وغالبًا باستخدام خادم DHCP (بروتوكول التهيئة الديناميكية للمضيف).

كيف يعمل بروتوكول DHCP؟



1. البحث عن خادم DHCP Discover (DHCP)

عند اتصال الجهاز بالشبكة، يرسل رسالة يسأل فيها: "هل يوجد خادم DHCP يمكنه إعطائي عنوان IP؟"

2. عرض عنوان DHCP Offer (IP)

يرد خادم DHCP بعرض يتضمن عنوان IP متاحًا، بالإضافة إلى معلومات أخرى مثل قناع الشبكة الفرعية والبوابة الافتراضية وخادم DNS.

3. طلب استخدام العنوان (DHCP Request)

يرسل الجهاز رسالة إلى خادم DHCP يخبره فيها بأنه يريد استخدام عنوان IP الذي عُرض عليه.

4. تأكيد تخصيص العنوان (DHCP ACK)

يرسل خادم DHCP رسالة تؤكد تخصيص عنوان IP للجهاز، وبذلك يصبح الجهاز جاهزًا للاتصال بالشبكة واستخدام الإنترنت.

جدران الحماية
Firewalls

جدار الحماية هو برنامج أو جهاز أمني يراقب حركة البيانات الداخلة إلى الشبكة والخارجة منها، ويقرر السماح بها أو حظرها وفقًا لقواعد يحددها مسؤول الشبكة. ويساعد ذلك على حماية الأجهزة والشبكة من الاتصالات غير المصرح بها.

الشبكة الخاصة الافتراضية
VPN

الشبكة الخاصة الافتراضية (أو VPN) هي تقنية تتيح للأجهزة على شبكات منفصلة التواصل بأمان عن طريق إنشاء مسار مخصص بين بعضها البعض عبر الإنترنت (يُعرف بالنفق). تشكل الأجهزة المتصلة داخل هذا النفق شبكتها الخاصة.

هل تعلم؟

أول هجوم إلكتروني معروف وقع في عام 1834، حيث قام بعض الفرنسيين بالعبث بنظام التلغراف لسرقة معلومات مالية.

أنظمة التشغيل

هو البرنامج الأساسي الذي يدير عمل الحاسوب. فهو يتحكم في مكونات الجهاز، مثل المعالج والذاكرة والتخزين، ويسمح للمستخدم بتشغيل البرامج والتفاعل مع الحاسوب بسهولة.

أنواع
أنظمة التشغيل

ويندوز	ماك أو أس	لينيكس
Windows	MacOS	Linux

الوظائف الأساسية لنظام التشغيل

إدارة الأجهزة

يتحكم في جميع الأجهزة في حاسوبك، مثل لوحة المفاتيح والفأرة والشاشة ومحركات التخزين. إنه مثل المسؤول الذي يدير جميع البنية التحتية للمدينة.

تشغيل التطبيقات

يشغل برامجك وتطبيقاتك، ويضمن أن لديها الموارد التي تحتاجها لتعمل بشكل صحيح. إنه يشبه المدير الذي يضمن أن الشركات لديها التصاريح والموارد اللازمة لتعمل.

إدارة الملفات

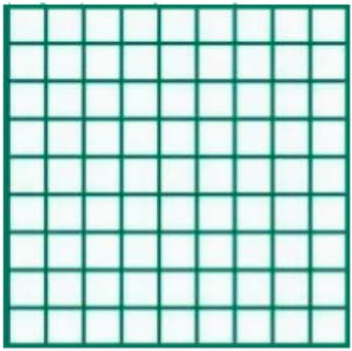
ينظم ملفاتك ومجلداتك، مما يسهل العثور على ما تحتاجه والوصول إليه. يشبه ذلك أمين المكتبة الذي يقوم بترتيب الكتب والوثائق في الرفوف لتسهيل الوصول إليها.

واجهة المستخدم

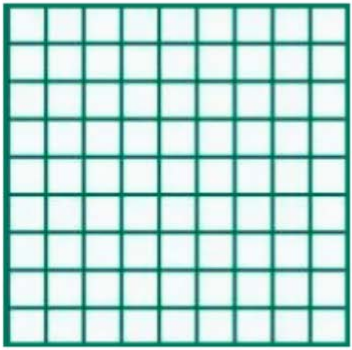
هي الجزء الذي يتيح لك التفاعل مع الحاسوب، مثل النوافذ والأيقونات والقوائم والأزرار التي تظهر على الشاشة. ومن خلالها يمكنك تشغيل البرامج وإدارة الملفات واستخدام الحاسوب بسهولة.

نشاط لغة الحاسوب

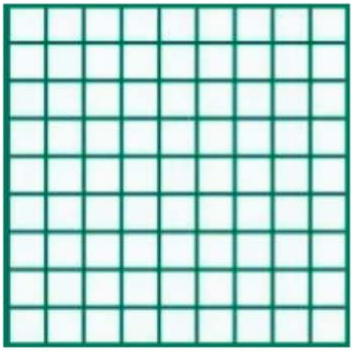
النظام الثنائي يستخدم الأرقام 1 و 0 فقط، والتي تمثل حالتين ممكنتين للإشارات الكهربائية داخل الحواسيب - مفتوح (1) ومغلق (0). للكشف عن الصور بالأسفل، استخدم اللون الأبيض لتمثيل 0 والأخضر لتمثيل 1."



1. 000000000
2. 000101000
3. 000101000
4. 000000000
5. 011000110
6. 001000100
7. 000111000
8. 000000000
9. 000000000



1. 000010000
2. 000111000
3. 001111100
4. 011111110
5. 001111100
6. 001101100
7. 001101100
8. 001101100
9. 000000000



1. 000000000
2. 001101100
3. 011111110
4. 011111110
5. 011111110
6. 001111100
7. 000111000
8. 000010000
9. 000000000

اختراق
كلمات المرور

مقدمة

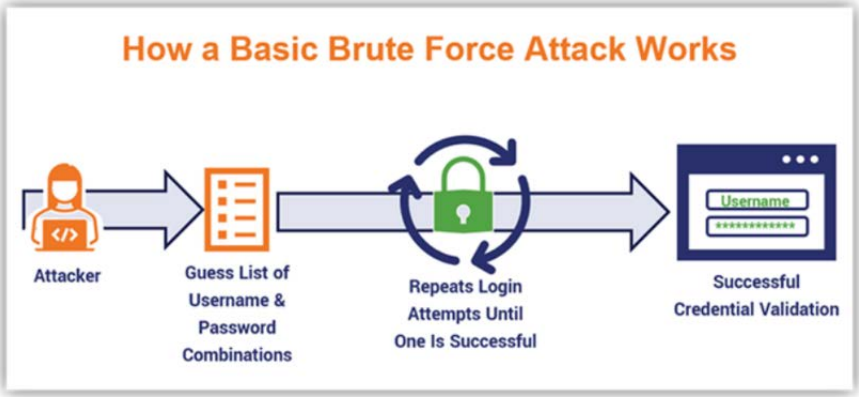
في اختراق كلمات المرور

اختراق كلمات المرور هو طريقة تخمين أو كشف كلمة مرور شخص ما. يستخدم المخترقون طرقًا متنوعة لمحاولة اختراق حساباتك، ومن الضروري فهم حيلهم لتتمكن من حماية نفسك

التقنيات العامة في كسر كلمة المرور

1. هجمات القوة الغاشمة
brute-force attacks

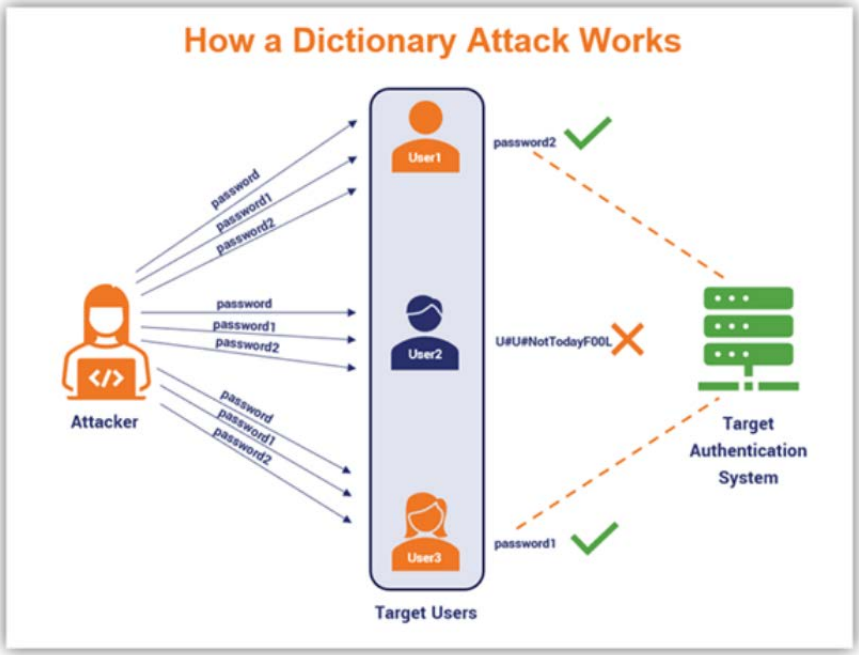
يستخدم المخترقون حواسيب قوية لتجربة كل مجموعة ممكنة من الأحرف حتى يجدوا كلمة المرور الصحيحة.



التقنيات العامة في كسر كلمة المرور

2. هجمات القاموس
Dictionary Attacks

يستخدم المخترقون قوائم تحتوي على كلمات وعبارات وأنماط شائعة لتخمين كلمات المرور.



نشاط
اخترق كلمة المرور

استخدم الكود أدناه لاختراق الـ 3 كلمات مرور!

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
7	1	8	2	10	11	3	5	26	9	21	19	15	4	18	25

Q	R	S	T	U	V	W	X	Y	Z
6	12	23	16	17	13	20	14	22	24

تصعيد
الامتيازات

تصعيد الامتيازات هو عندما يحصل المهاجم على صلاحيات أعلى في النظام، مما يمنحه مزيدًا من الوصول والتحكم

هناك نوعان

- **تصعيد الامتيازات العمودي**

الانتقال من مستخدم بمستوى أقل إلى مستخدم بمستوى أعلى (مثل الانتقال من ضيف إلى مسؤول).

- **تصعيد الامتيازات الأفقي**

الحصول على الوصول إلى الموارد ضمن نفس مستوى الامتيازات ولكن تخص مستخدمًا آخر (مثل الوصول إلى ملفات مستخدم آخر).

تصعيد الامتيازات في ويندوز

تحتوي أنظمة ويندوز بشكل أساسي على نوعين من المستخدمين:

المسؤولون: هؤلاء المستخدمون لديهم أعلى الامتيازات و يمتلكون صلاحيات المسؤول أو المدير. لديهم القدرة على إجراء أي تعديلات على إعدادات النظام والوصول إلى جميع الملفات الموجودة فيه دون قيود.

المستخدمون العاديون: يمكن لهؤلاء المستخدمين الوصول إلى الحاسوب ولكن يمكنهم أداء مهام محدودة فقط. وعادةً، لا يمكن لهؤلاء المستخدمين إجراء تغييرات دائمة أو أساسية على النظام وتقتصر صلاحياتهم على ملفاتهم.

الأساليب العامة لتصعيد الامتيازات في ويندوز

1 استغلال الخدمات المعرضة للخطر

Exploiting Vulnerable Services

غالبًا ما تعمل خدمات ويندوز بامتيازات مرتفعة (مثل SYSTEM). إذا كانت الخدمة تحتوي على ثغرة، يمكن للقراصنة استغلالها للحصول على تلك الامتيازات.

2 سوء التكوين

Misconfigurations

يرتكب مسؤولو النظام أحياناً أخطاء عند تكوين إعدادات ويندوز أو الصلاحيات. يمكن للقراصنة استغلال هذه الأخطاء للحصول على امتيازات مرتفعة.

3 استغلال ثغرات يوم-الصفر

Zero-Day Exploits

هذه هي الثغرات التي تكون غير معروفة لمورّد البرمجيات أو للمجتمع. يمكن للمخترقين الذين يكتشفون هذه الثغرات استغلالها قبل توفر التصحيح.

تصعيد الامتيازات في لينيكس

الأساليب العامة لتصعيد الامتيازات في لينكس

1 الثنائيات SUID (تعيين معرف المستخدم)

هي برامج تعمل بصلاحيات مالك الملف، وليس بصلاحيات المستخدم الذي يشغّلها. وإذا احتوى أحد هذه البرامج على ثغرة أمنية، فقد يتمكن المهاجم من استغلالها للحصول على صلاحيات مالك الملف، والتي قد تكون صلاحيات مرتفعة مثل صلاحيات المستخدم الجذر (root).

2 الأخطاء في الإعدادات Misconfigurations

يرتكب مسؤولو النظام احيانا أخطاء عند ضبط إعدادات ويندوز أو الصلاحيات. يمكن للمخترقين استغلال هذه الأخطاء للحصول على امتيازات مرتفعة.

3 استغلال الخدمات Exploiting Services

إذا كانت إحدى الخدمات التي تعمل على النظام تمتلك صلاحيات مرتفعة ولم تُؤمَّن بشكل صحيح، فقد يتمكن المهاجم من استغلالها للحصول على صلاحيات أعلى أو تنفيذ أوامر غير مصرح بها. ويحدث ذلك عادةً عندما تكون الخدمة تحتوي على ثغرة أمنية، أو تستخدم إصدارًا قديمًا، أو تكون إعداداتها غير آمنة.

استغلال الثغرات في الخدمات

الخدمات هي برامج تعمل في خلفية جهاز الكمبيوتر الخاص بك.

كيف تعمل؟

تحديد خدمة معرضة لثغرات أمنية: يبحث القراصنة عن الخدمات التي تعمل بامتيازات مرتفعة (مثل الجذر) وتحتوي على ثغرات معروفة.

استغلال الثغرة: يستخدم القراصنة استغلالاً مصمماً بعناية للاستفادة من الثغرة، وغالباً ما يؤدي ذلك للحصول على امتيازات الخدمة التي تم استهدافها.

الحصول على الوصول: بامتيازات مرتفعة، يمكن للقراصنة الآن القيام بأشياء لم يتمكنوا من القيام بها من قبل، مثل تثبيت البرامج الضارة، سرقة البيانات، أو السيطرة على النظام.

برمجيات
الفدية

تعمل برمجيات الفدية عن طريق تشفير ملفاتك وتحويلها إلى رموز غير قابلة للقراءة. الطريقة الوحيدة لفك تشفيرها هي باستخدام مفتاح خاص يحتفظ به المخترقون للحصول على فدية.

كيف تقع برمجيات الفدية؟

وسائل التصيد الإلكتروني Phishing Emails: هذه الرسائل الخادعة تبدو غالبًا كأنها من مصدر موثوق، مثل مصرفك أو صديق. قد تحتوي على مرفق ضار أو رابط يؤدي عند النقر عليه إلى تحميل برمجيات الفدية على جهاز الحاسوب الخاص بك.

أنواع الملفات الضارة Malicious File Types: قد يقوم المهاجمون بإرسال ملفات تبدو آمنة لخداع المستخدم، مثل ملفات PDF ومستندات Word وExcel وملفات ZIP. وقد تحتوي هذه الملفات على روابط أو تعليمات تؤدي إلى تنزيل أو تشغيل برمجيات خبيثة، مثل برمجيات الفدية. كما قد تكون البرمجيات الخبيثة نفسها على هيئة ملفات تنفيذية (.exe) أو سكربتات مثل .ps1 (PowerShell) و.bat (Batch) و.js (JavaScript).

التحميلات العابرة Drive-by Downloads: ببساطة زيارة موقع ويب مخترق يمكن أن يؤدي إلى تنزيل عشوائي، حيث يتم تثبيت برمجيات الفدية بصمت دون علمك.

التدابير الأمنية ضد برمجيات الفدية

- حافظ على تحديث برامجك
- كن حذرًا من الرسائل الإلكترونية والروابط
- استخدم برنامج مكافحة فيروسات موثوق وفعال
- قم بعمل نسخ احتياطية لبياناتك بانتظام

المصادقة القوية
وَ مديرو كلمات المرور

كلمة المرور القوية

- استخدم 12 حرفًا على الأقل.
- امزجها بحروف كبيرة وصغيرة وأرقام ورموز (مثل @، #، $، %).
- لا تُعِد استخدام نفس كلمة المرور لحسابات مختلفة.

المصادقة متعددة العوامل (MFA)

أشهر وسائل المصادقة متعددة العوامل (MFA):

الرموز لمرة واحدة - (One-Time Passwords - OTP)

رموز مؤقتة تُرسل إلى هاتفك أو تُولَّد بواسطة تطبيق مصادقة، وتُستخدم مرة واحدة فقط.

الإشعارات الفورية - (Push Notifications)

يرسل التطبيق إشعارًا إلى هاتفك، ويمكنك الموافقة على محاولة تسجيل الدخول أو رفضها.

القياسات الحيوية - (Biometrics)

مثل بصمة الإصبع أو التعرف على الوجه أو بصمة العين لإثبات هويتك.

مديرو كلمات المرور

مديرو كلمات المرور هي أدوات تخزن وتنظم كلمات مرورك بشكل آمن. تساعدك هذه الأدوات على إنشاء كلمات مرور قوية وفريدة لكل حساباتك وتملؤها تلقائيًا عندما تحتاج إلى تسجيل الدخول. بهذه الطريقة، لا تحتاج إلى تذكر كلمات مرور متعددة، وتصبح حساباتك أكثر أمانًا.

أشهر أدوات إدارة كلمات المرور

1Password

KeePass

Bitwarden

LastPass

نشاط - فك التشفير

فكك الكلمات المخفية

Letter 1 - • ↓ ↓ →

Letter 2 - • ← ↑ ↑ → →

Letter 3 - • ↑ ← ←

Letter 4 - • ← ← ↓ ↓ →

Letter 5 - • → → ↑ ↑ ← ←

Letter 6 - • ↑ → →

Letter 7 - • ↑ ↑ ← ← ↓

Letter 8- • ← ↑ ↑ ←

Letter 9 - • ↓ ← ↑ ←

Letter 10 - • ↓ → ↓

Letter 11 - • ↓ ← ← ↑ ↑

Letter 12 - • → ↑ ↑ ← ← ←

Letter 13 - • ↑ → ↓ →

Letter 14 - • ↑ → ↑ → ↓

I	Y	E	U	L
T	Z	D	C	N
C	J	●	R	O
K	S	P	B	F
G	H	R	A	M

سلامة الشبكات العامة

مخاطر الواي فاي العام Public Wi-Fi

- **هجمات Man-in-the-middle:** يمكن للمخترقين اعتراض حركة المرور الخاصة بك وسرقة بيانات تسجيل الدخول، أرقام بطاقات الائتمان، وبيانات حساسة أخرى.

- **التجسس:** يمكن للمخترقين الاستماع إلى محادثاتك ورؤية المواقع التي تزورها.

- **توزيع البرمجيات الخبيثة:** يمكن للمخترقين نشر البرمجيات الخبيثة عبر شبكات الواي فاي العامة، مما يؤدي إلى إصابة جهازك دون علمك.

البقـاء آمنـاً على الواي فاي العام

- يمكنك **استخدام شبكة خاصة افتراضية (VPN)** موثوقة لتشفير حركة المرور الخاصة بك، مما يجعلها غير قابلة للقراءة بالنسبة للمخترقين

- **تجنب استخدام الخدمات المصرفية** عبر الإنترنت أو التسوق الإلكتروني أو تسجيل الدخول إلى الحسابات الحساسة عند الاتصال بشبكة Wi-Fi عامة، خاصة إذا كانت غير محمية أو غير موثوقة.

- **تصفح مواقع الويب الآمنة فقط** وابحث عن HTTPS.

- حافظ على **تحديث برامجك.**

النسخ الاحتياطي

النسخ الاحتياطي هو نسخ من بياناتك المهمة، مثل الملفات والصور والمستندات، تُخزن بشكل منفصل للحفاظ على أمانها. إذا فقدت بياناتك الأصلية أو تعرضت للتلف، يمكنك استخدام النسخ الاحتياطية لاستعادتها.

انواع النسخ الاحتياطية

الكاملة

النسخة الاحتياطية الكاملة: هذه النسخة تنشئ نسخة كاملة من جميع ملفاتك وبياناتك. يستغرق إنشاؤها وقتًا طويلا لكنها الخيار الأكثر شمولاً للنسخ الاحتياطي.

التزايدية

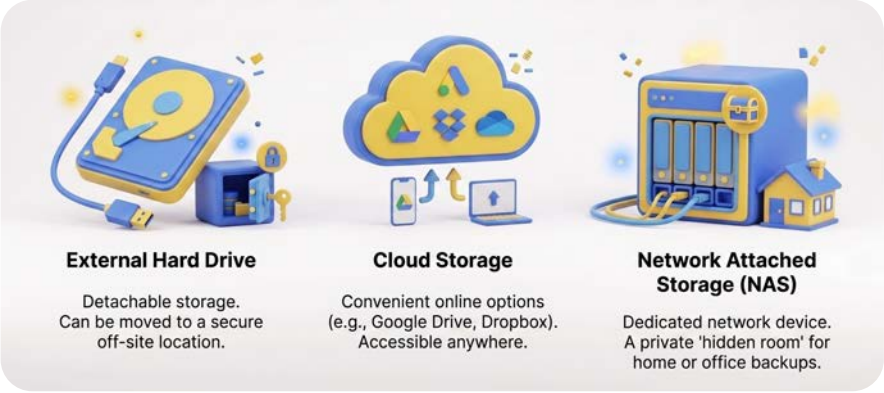
النسخة الاحتياطية التزايدية: هذه النسخة تنسخ فقط الملفات التي تغيرت منذ آخر نسخة احتياطية. هي أسرع من النسخة الاحتياطية الكاملة لكنها تتطلب نسخًا احتياطيًا متعددة لاستعادة جميع بياناتك.

التفاضلية

النسخة الاحتياطية التفاضلية: هذه النسخة تنسخ جميع الملفات التي تغيرت منذ آخر نسخة احتياطية كاملة. هي أسرع في الاستعادة من النسخة الاحتياطية التزايدية لكنها أبطأ في الإنشاء.

النسخ الاحتياطي

كيف تخزن النسخ الاحتياطية؟



1 القرص الصلب الخارجي

يمكن فصله وتخزينه في مكان آمن.

2 التخزين الســـحابي

مثل جوجل درايف، دروب بوكس، أو ون درايف توفر خيارات نسخ احتياطي عبر الإنترنت مريحة وسهلة الوصول.

3 التخزين الشبكي المرفق

NAS - Network) (Attached Storage جهاز مخصص لتخزين النسخ الاحتياطية على شبكة منزلك أو مكتبك. إنه مثل وجود غرفة مخفية في منزلك حيث تحتفظ بأثمن مقتنياتك.

مكافحة
الفيروسات

برامج مكافحة الفيروسات هي برمجيات مصممة لاكتشاف الفيروسات والبرمجيات الخبيثة الأخرى ومنعها وإزالتها من حاسوبك، مما يحافظ على أمانه وسلامته.

وظائف برنامج مكافحة الفيروسات

يقوم بفحص ملفات وبرامج حاسوبك بانتظام بحثًا عن أي علامات للبرمجيات الخبيثة.

إذا اكتشف أي شيء غير عادي، فإنه يقارنه بقاعدة بيانات من البرمجيات الخبيثة المعروفة

إذا تأكد أن شيئًا ما هو بالفعل برمجية خبيثة، فإنه يقوم بحجزه أو حذفه لمنعه من التسبب في أي ضرر.

بعض برامج مكافحة الفيروسات تتخذ خطوة إضافية وتحاول منع البرمجيات الخبيثة من الدخول إلى نظامك في المقام الأول. قد تقوم بحجب المواقع الضارة أو فحص الملفات قبل تنزيلها.

أنواع برنامج
مكافحة الفيروسات

الكشف القائم على الاستدلال

يحلل سلوك الملفات والبرامج لاكتشاف الأنشطة المشبوهة، حتى إذا لم يكن توقيع البرمجية الخبيثة معروفًا.

الحماية القائمة على السحابة

بدلاً من الاعتماد على جهازك فقط، يستخدم برنامج مكافحة الفيروسات خوادم عبر السحابة لفحص الملفات واكتشاف أحدث التهديدات بسرعة، مما يوفر حماية محدثة باستمرار.

مكافح الفيروسات المعتمد على التوقيعات

يعتمد هذا النوع على قاعدة بيانات من توقيعات البرمجيات الخبيثة المعروفة

أمثلته:

نورتون Norton

مكافي McAfee

أفاست Avast

AVG

كاسبيرسكي Kaspersky

كيف تختار برنامج مكافحة الفيروسات المناسب؟

- اختر علامة تجارية معروفة وموثوقة.
- ابحث عن ميزات مثل الحماية في الوقت الفعلي، تصفية الويب، فحص البريد الإلكتروني، والحماية من البرمجيات الخبيثة.
- تأكد من أن برنامج مكافحة الفيروسات لا يبطئ من أداء جهاز الكمبيوتر الخاص بك كثيرًا.
- اختر برنامجًا سهل التثبيت والاستخدام.

التحديثات الدورية
وإدارة التصحيحات

يجب عليك أيضًا الحفاظ على تحديث نظام التشغيل والتطبيقات الخاصة بك. غالبًا ما تتضمن التحديثات البرمجية تصحيحات تقوم بإصلاح الثغرات الأمنية التي قد يستغلها المخترقون

التدابير الدفاعية الإضافية

• جدران الحماية

تعمل جدران الحماية كحاجز بين جهاز الكمبيوتر الخاص بك والإنترنت، حيث تتحكم في حركة المرور الشبكية الواردة والصادرة. يمكن أن تساعد في منع محاولات الوصول غير المصرح بها ومنع انتشار البرمجيات الخبيثة.

• أنظمة اكتشاف التسلل IDS- Intrusion Detection) (Systems

تقوم أنظمة اكتشاف التسلل بمراقبة حركة المرور الشبكية بحثًا عن الأنشطة المشبوهة وتنبهك إلى التهديدات المحتملة.

• تدريبات التوعية الأمنية

من الضروري تعليم نفسك والآخرين حول أفضل ممارسات الأمن السيبراني للدفاع. يشمل ذلك تعلم كيفية التعرف على رسائل البريد الإلكتروني الاحتيالية، وإنشاء كلمات مرور قوية، وتجنب السلوكيات الخطرة على الإنترنت.

6

دليل المخترق الأخلاقي

اختبارات الاختراق، أو ما يُعرف بـ "pen-testing"، هو هجوم إلكتروني محاكى مُصرح به على نظام حاسوب، يتم لتنفيذ تقييم لأمان النظام. في جوهره، هو وسيلة لاكتشاف مدى قوة دفاعاتك قبل أن يقوم المخترقون بذلك.

هل تعلم؟

يكتسب اختبار الاختراق زخمًا كبيرًا لدرجة أنه من المقدر أن يصبح صناعة بقيمة 4.5 مليار دولار بحلول عام 2026 (حسب تقديرات Gartner)

أخلاقيات
الاختراق

القانونية مقابل الأخلاق

الاختراق الأخلاقي Ethical hacking، المعروف أيضًا باختبار الاختراق penetration testing، هو قانوني تمامًا. لكن كونه قانوني لا يعني أنه مفتوح للجميع.

قبل إجراء أي اختراق أخلاقي، هناك اتفاق حاسم يُسمى قواعد الاشتباك (ROE- Rules of Engagement). يوضح هذا المستند:

- **الإذن:** يوضح بوضوح من هو المصرح له بإجراء اختبار الاختراق ومن يمنح الضوء الأخضر.
- **نطاق الاختبار:** يحدد بدقة الأنظمة أو الشبكات أو التطبيقات التي يمكن اختبارها.
- **القواعد:** يحدد القوانين المتعلقة بالأدوات والتقنيات المسموح بها وأية مناطق محظورة.

قواعد الاشتباك (ROE) - Rules of Engagement

تعمل قواعد الاشتباك كمرشد أخلاقي للمخترقين الأخلاقيين. تضمن أنهم يلتزمون بالحدود القانونية والأخلاقية لعملهم. إنها مثل مجموعة من القواعد للعبة - يعرف الجميع ما هو مسموح به وما هو غير مسموح به، لذا لا توجد مفاجآت.

أطياف
المخترقين

توجد ثلاث فئات رئيسية من المخترقين، كل منها يمتلك دوافع وحدود أخلاقية خاصة به:

القبعات البيضاء: الأبطال

هؤلاء هم الأفراد الطيبون – مخترقون أخلاقيون يستخدمون مهاراتهم لمساعدة المؤسسات على تحسين أمانها. يعملون ضمن إطار القانون ويتبعون قواعد أخلاقية صارمة.

القبعات السوداء: الأشرار

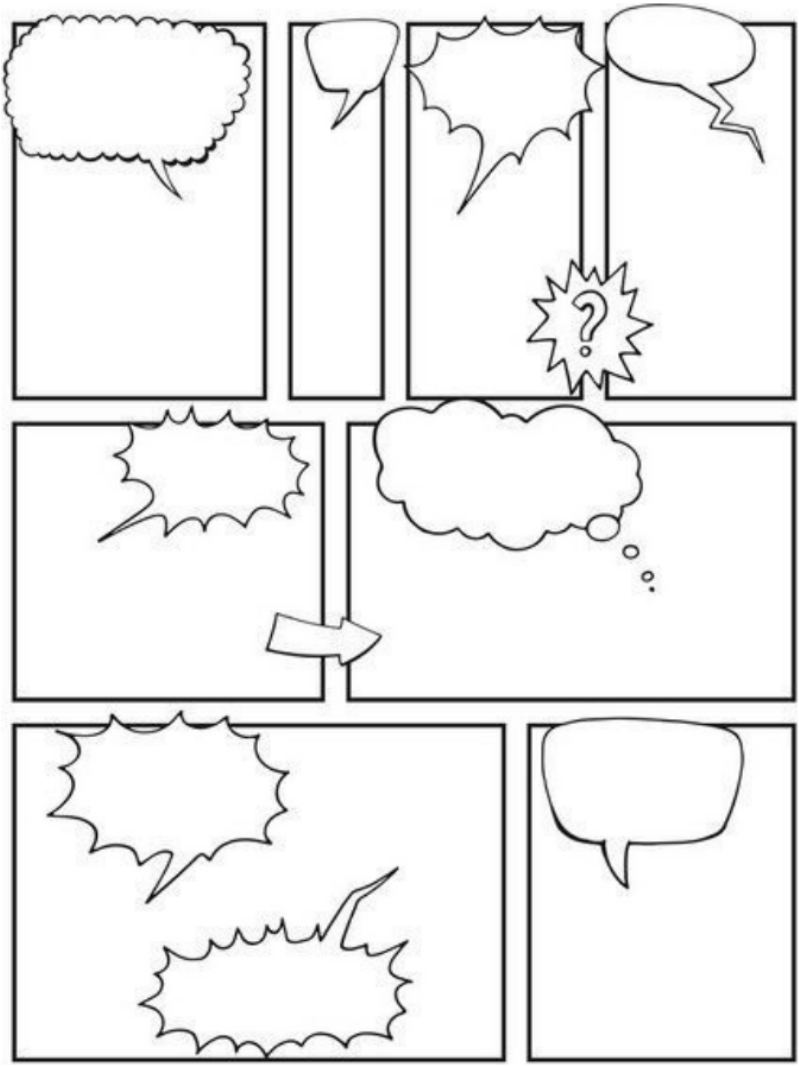
هؤلاء هم الأفراد السيئون – مخترقون خبيثون يستغلون الثغرات لتحقيق مكاسب شخصية أو ربح مالي أو لإحداث ضرر. أفعالهم غير قانونية وغالبًا ما تتضمن جريمة إلكترونية.

القبعات الرمادية: الغامضون

هؤلاء المخترقون يقعون في منطقة غير واضحة. قد يكتشفون الثغرات دون إذن، ولكنهم غالبًا ما يبلغون عنها إلى المؤسسة، على أمل أن يتم إصلاحها. يمكن أن تكون أفعالهم مفيدة وأخلاقية مشكوك فيها في ذات الوقت.

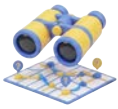
وقت الخيال!

استخدم أنواع المخترقين كشخصياتك (الأبيض والأسود والرمادي) لرسم قصة حول الاختراق...



مراحل
اختبار الاختراق

المراحل الخمسة لاختبار الاختراق



1. الاستطلاع (Reconnaissance)
مهمة جمع المعلومات الاستخباراتية للمخترق

2. الفحص (Scanning)
البحث عن الثغرات

3. الاستغلال (Exploitation)
اختراق الدفاعات

4. ما بعد الاستغلال (Post-Exploitation)
تأسيس موطئ قدم

5. إعداد التقرير (Reporting)
تقرير المحقق

هل تعلم؟

أن شركات مثل Google وFacebook وMicrosoft تدير برامج مكافآت اكتشاف الأخطاء، حيث تدفع للمتسللين للعثور على الثغرات الأمنية والإبلاغ عنها. لقد كسب بعض المتسللين أكثر من مليون دولار بمجرد العثور على الأخطاء!
هل تريد أن تعرف أكثر؟ مزيد من التفاصيل القادمة.

مراحل
اختبار الاختراق

1 Reconnaissance (Recon)

في هذه المرحلة، يجمع مختبرو الاختراق أكبر قدر ممكن من المعلومات عن النظام المستهدف قبل بدء الاختبار. ويشبه ذلك عمل المحقق الذي يجمع الأدلة قبل حل القضية. وقد يستخدمون مصادر المعلومات العامة (OSINT)، أو تحليل الموقع الإلكتروني، أو البحث عن النطاقات والخدمات وعناوين IP، أو الهندسة الاجتماعية إذا كانت ضمن نطاق الاختبار المصرح به، وذلك لفهم بيئة النظام وتحديد نقاط الضعف المحتملة.

2 الفحص scanning

بعد جمع المعلومات، يبدأ مختبر الاختراق بفحص النظام لاكتشاف الأجهزة النشطة، والمنافذ المفتوحة، والخدمات التي تعمل، ثم يبحث عن الثغرات الأمنية المحتملة. ويشبه ذلك مفتشًا يفحص المبنى غرفةً تلو الأخرى بحثًا عن أبواب أو نوافذ غير مؤمنة.

3 الاستغلال exploitation

إذا وجد المخترقون ثغرة، فسيحاولون استغلالها للوصول إلى النظام. قد يشمل ذلك استخدام استغلال معروف، أو تصميم هجوم مخصص، أو حتى خداع المستخدم لينقر على رابط ضار. إنه مثل لص يجد طريقة لفتح قفل.

4 ما بعد الاستغلال post-exploitation

بعد الحصول على الوصول إلى النظام، يقوم مختبرو الاختراق بتقييم التأثير المحتمل للاختراق. ويحددون الموارد التي يمكن الوصول إليها، وما إذا كان من الممكن تصعيد الصلاحيات، ومدى قدرة المهاجم على التنقل داخل البيئة المستهدفة، مع تجنب التسبب في أي تعطيل غير ضروري للأنظمة.

5 إعداد التقرير reporting

أخيرًا، سيقوم المخترقون الأخلاقيون بتوثيق نتائجهم والإبلاغ عنها لمالك النظام. سيشمل هذا التقرير تفاصيل حول الثغرات التي وجدوها، كيف استغلوها، وتوصيات لإصلاحها. إنه مثل محقق يكتب تقرير قضيته.

الإطارات القانونية
والاعتماد الصناعي

مثل أي مهنة، يعمل الاختراق الأخلاقي ضمن إطار من القواعد واللوائح. تضمن هذه الأطر أن يتم إجراء اختبار الاختراق بشكل قانوني وأخلاقي وبدرجة عالية من الاحترافية.

معايير وشهادات القطاع :

دليل منهجية اختبار الأمان مفتوح المصدر (OSSTMM): هو دليل شامل يغطي جوانب مختلفة من اختبار الأمان، بما في ذلك جمع المعلومات، فحص الثغرات، والتقرير. يشتهر بتغطيته المتعمقة ومرونته، ولكن يمكن أن يكون معقدًا ويستخدم مصطلحات فريدة.

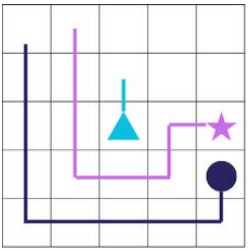
مشروع أمان تطبيقات الويب المفتوح (OWASP): هو مشروع يقوده المجتمع ويركز على أمان تطبيقات الويب. يوفر OWASP إطار عمل شائع الاستخدام لاختبار تطبيقات الويب، بالإضافة إلى قائمة بأهم 10 مخاطر لأمان تطبيقات الويب. إنه سهل الفهم ويتم تحديثه بانتظام، ولكنه قد لا يكون دائمًا واضحًا في كيفية تصنيف الثغرات المتداخلة.

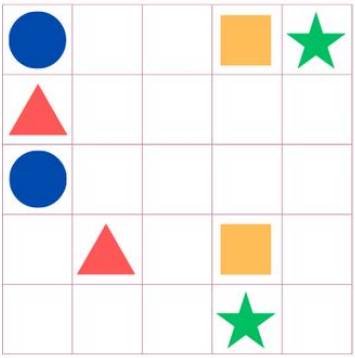
إطار عمل الأمن السيبراني لـ NIST: تم تطويره من قبل المعهد الوطني للمعايير والتقنية (NIST)، ويوفر هذا الإطار إرشادات لإدارة وتقليل مخاطر الأمن السيبراني. يتم اعتماده على نطاق واسع من قبل المؤسسات في الولايات المتحدة ويوفر نهجًا منظمًا للأمن السيبراني. ومع ذلك، يمكن أن يكون معقدًا وقد لا يلبي بالكامل الاحتياجات الفريدة لكل مؤسسة.

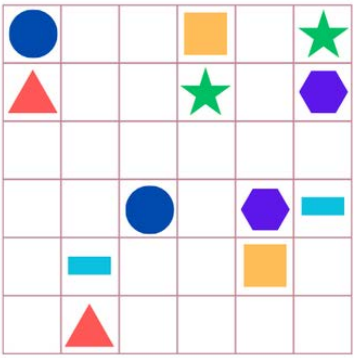
إطار تقييم الأمن السيبراني لـ NCSC: يساعد هذا الإطار المدعوم من الحكومة البريطانية المؤسسات على تقييم وإدارة مخاطرها السيبرانية. يغطي مجموعة واسعة من الموضوعات، بما في ذلك أمن البيانات، وأمن النظام، والاستجابة للحوادث. على الرغم من أنه مدعوم من قبل سلطة موثوقة، إلا أنه يعتبر جديدًا نسبيًا وقد لا يكون معتمدًا على نطاق واسع مثل الإطارات الأخرى.

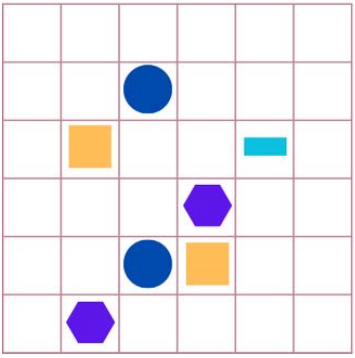
توصيل الأشكال المتشابهة

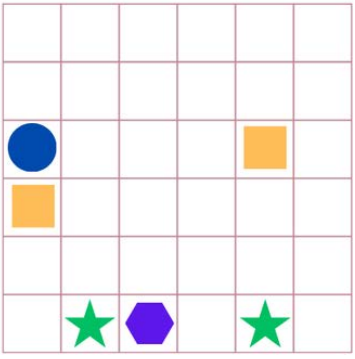
هل يمكنك رسم خطوط لربط كل زوج من الأشكال المتطابقة معًا؟ يجب ألا تتقاطع الخطوط أو تتلامس مع بعضها البعض، ويسمح بوجود خط واحد فقط على كل مربع. لا يمكنك استخدام الخطوط القُطرية.











اختبارات الاختراق
الصندوق الأسود، والأبيض، والرمادي

هل تعلم؟

كانت أول مجموعة قرصنة أخلاقية هي "فرق النمر Tiger Teams" التي تشكلت في السبعينيات لاختبار مدى أمان أنظمة الكمبيوتر من خلال محاولة اختراقها.

الصندوق الأسود

أنت لا تعرف شيئًا عن كيفية عمل المنظمة الداخلية. ستعتمد على مهارات الملاحظة والهندسة الاجتماعية لربط وجمع المعلومات.

الصندوق الرمادي

لديك بعض المعلومات المحدودة عن المنظمة، ربما مخطط الطوابق أو قائمة الموظفين. ستحتاج إلى دمج معرفتك مع الملاحظة والهندسة الاجتماعية لتحقيق النجاح.

الصندوق الأبيض

لديك وصول كامل إلى مخططات المنظمة، وبروتوكولات الأمان، وسجلات الموظفين. يمكنك استخدام هذه المعرفة للتخطيط للاختراق بدقـة.

برامج مكافآت
اكتشاف الثغرات

فهم برامج مكافآت اكتشاف الثغرات

برامج مكافآت اكتشاف الثغرات تشبه خريطة الكنز للهاكرز الأخلاقيين. تقوم الشركات بإنشاء هذه البرامج ودعوة الهاكرز لاكتشاف 'الثغرات' (نقاط الضعف الأمنية) في مواقعها على الويب أو تطبيقاتها أو شبكاتها. إذا اكتشفت ثغرة صحيحة، تقوم بالإبلاغ عنها للشركة، وتكافئك الشركة بالنقود أو جوائز أخرى.

كيف تنفع برامج مكافآت اكتشاف الثغرات الجميع؟

الشركات: تحصل على المساعدة في العثور على الثغرات وإصلاحها قبل أن يستغلها الأشخاص السيئون.

المخترقون: يستخدمون مهاراتهم لأغراض جيدة، ويحصلون على الاعتراف، ويكسبون المال.

الإنترنت: يصبح مكانًا أكثر أمانًا للجميع مع اكتشاف المزيد من الثغرات وإصلاحها.

أفضل الممارسات لصيد مكافآت اكتشاف الثغرات

1. **ابق ضمن النطاق**
2. **كن دقيقاً**
3. **كن محترمًا**
4. **لا تستغل الثغرات أبدًا**

كيف تشارك في برامج مكافآت اكتشاف الثغرات؟

- **اختر منصة:** تستضيف العديد من المنصات برامج مكافآت اكتشاف الثغرات، مثل HackerOne وBugcrowd. اشترك واستكشف البرامج المتاحة.

- **اختر هدفك:** اختر برنامجًا يثير اهتمامك ويتناسب مع مستوى مهاراتك.

- **اقرأ القواعد:** لكل برنامج مجموعة خاصة من القواعد والنطاق. تأكد من فهمك لما هو مسموح وما هو غير مسموح.

- **ابحث عن الثغرات:** استخدم مهاراتك في الاختراق الأخلاقي للعثور على الثغرات ضمن نطاق البرنامج.

- **أبلغ عن اكتشافاتك:** اكتب تقريرًا مفصلًا يوضح الثغرة، وكيفية إعادة إنتاجها، وتأثيرها المحتمل.

- **احصل على المكافأة!** إذا كان تقريرك صحيحاً، ستحصل على مكافأة (عادة نقدية) واعتراف بعملك.

7

استخبارات التهديدات السيبرانية

يمكن تعريف اســتخبارات التهديـدات الســيبرانية (CTI - Cyber Threat Intelligence) على أنها معرفة قائمة على الأدلة حول الخصوم، بما في ذلك مؤشراتهم وتكتيكاتهم ودوافعهم ونصائح قابلة للتنفيذ ضدهم. يمكن استخدام هذه المعلومات لحماية الأصول الحيوية وإبلاغ فرق الأمن السيبراني وإدارة القرارات التجارية.

هل تعلم؟

يبحث المحترفون المعروفون باسم "صائدي التهديدات السيبرانية" بشكل استباقي عن أي مؤشرات تدل على وجود تهديد داخل الشبكة قبل أن يسبب ضررًا. ويشبه ذلك حارس أمن يتجول داخل المبنى بحثًا عن أي شخص مشبوه قبل أن يرتكب جريمة.

Data البيانات	مؤشرات منفصلة مرتبطة بالخصم، مثل عناوين IP أو عناوين URL أو الرموز (hashes).
Information المعلومات	مزيج من عدة نقاط بيانات تجيب على أسئلة مثل "كم مرة قام الموظفون بالوصول إلى tryhackme.com خلال الشهر؟
Intelligence الاستخبارات	ربط البيانات والمعلومات لاستخراج أنماط من الإجراءات بناءً على التحليل السياقي

تصنيفات
استخبارات التهديدات

الاستخبارات الاستراتيجية

استخبارات عالية المستوى تدرس مشهد التهديدات للمنظمة وترسم مناطق المخاطر بناءً على الاتجاهات والأنماط والتهديدات الناشئة التي قد تؤثر على القرارات التجارية.

الاستخبارات التكتيكية

تقيّم تكتيكات وأساليب وإجراءات الخصوم (TTPs - Tactics Techniques, and Procedures). يمكن لهذه الاستخبارات تعزيز ضوابط الأمان ومعالجة الثغرات من خلال التحقيقات في الوقت الفعلي.

الاستخبارات التقنية

تدرس الأدلة والآثار للهجمات التي يستخدمها الخصم. يمكن لِفرق الاستجابة للحوادث استخدام هذه الاستخبارات لإنشاء سطح هجوم أساسي لتحليل وتطوير آليات الدفاع.

الاستخبارات التشغيلية

تدرس دوافع ونوايا الخصم الخاصة لتنفيذ هجوم. قد تستخدم فرق الأمان هذه الاستخبارات لفهم الأصول الحيوية المتاحة في المنظمة (الأشخاص، والعمليات، والتقنيات) التي قد تكون مستهدفة.

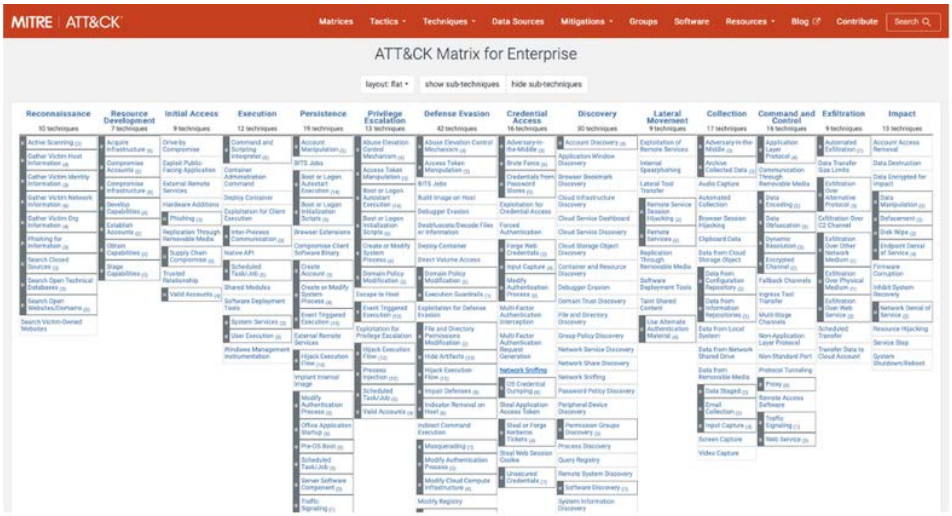
دورة حياة
CTI

معايير وإطارات
استخبارات التهديدات السيبرانية

تقدم المعايير والإطارات هياكل لتنظيم توزيع واستخدام استخبارات التهديدات عبر الصناعات. كما أنها تتيح استخدام مصطلحات موحدة، مما يساعد في التعاون والتواصل.

إطار MITRE ATT&CK

هو قاعدة معرفة توثق الأساليب التي يستخدمها المهاجمون أثناء الهجمات الإلكترونية، مثل التكتيكات والتقنيات المختلفة. ويستخدمه محللو الأمن لفهم سلوك المهاجمين، والتحقيق في الحوادث الأمنية، وتحسين وسائل الكشف والدفاع.



معايير وأطر
استخبارات التهديدات السيبرانية

TAXII

TAXII (Trusted Automated eXchange of Intelligence Information) هو بروتوكول يتيح تبادل معلومات استخبارات التهديدات تلقائيًا وبشكل آمن بين المؤسسات وأدوات الأمن السيبراني. ويساعد ذلك على مشاركة أحدث معلومات التهديدات بسرعة، مما يحسن قدرة الأنظمة على اكتشاف الهجمات والوقاية منها والاستجابة لها.

STIX

STIX (Structured Threat Information eXpression) هو معيار يُستخدم لوصف وتوثيق معلومات التهديدات السيبرانية بطريقة منظمة يمكن لأنظمة الأمن المختلفة فهمها ومشاركتها. ويشمل معلومات مثل المؤشرات (Indicators)، وأساليب المهاجمين (TTPs)، وحملات الهجوم، والأدوات المستخدمة، والعلاقات بينها.

سلسلة القتل السيبرانية

طورتها شركة لوكهيد مارتن Lockheed Martin، وتقوم سلسلة القتل السيبرانية بتفكيك أفعال الخصوم إلى خطوات. يساعد هذا التفكيك المحللين والمدافعين في تحديد الأنشطة المرتبطة بكل مرحلة عند التحقيق في الهجوم.

نموذج الألماس

هو إطار يُستخدم لتحليل الهجمات الإلكترونية وفهم كيفية تنفيذها. ويربط بين أربعة عناصر رئيسية تساعد محللي الأمن على تتبع نشاط المهاجمين وفهم العلاقة بين مكونات الهجوم.

الخصم

التركيز هنا على الفاعل المهدد وراء الهجوم ويسمح للمحللين بتحديد الدافع وراء الهجوم.

الضحية

الطرف المقابل للخصم ينظر إلى فرد أو مجموعة أو منظمة تأثرت بالهجوم.

القدرات

تشير القدرات إلى الأدوات والبرمجيات الخبيثة والاستغلالات والتكتيكات والتقنيات والإجراءات (TTPs) التي يستخدمها المهاجم لتنفيذ الهجوم.

البنية التحتية

تشير البنية التحتية إلى الموارد التي يعتمد عليها المهاجم لتنفيذ الهجوم، مثل أسماء النطاقات، وعناوين IP، والخوادم، والمواقع الإلكترونية، وأنظمة التحكم والسيطرة (C2). يساعد تحليل هذه البنية في اكتشاف الأنشطة الخبيثة وتتبعها وتعطيلها.

أدوات
استخبارات التهديدات

استخبارات التهديدات هي تحليل البيانات والمعلومات باستخدام الأدوات والتقنيات لتوليد أنماط ذات مغزى حول كيفية التخفيف من المخاطر المحتملة المرتبطة بالتهديدات الحالية أو الناشئة التي تستهدف المنظمات أو الصناعات أو القطاعات أو الحكومات.

Open-Source Intelligence (OSINT)

1. UrlScan.io

هو خدمة مجانية تم تطويرها للمساعدة في مسح وتحليل المواقع الإلكترونية. تُستخدم لأتمتة عملية تصفح ومسح المواقع لتسجيل الأنشطة والتفاعلات. عند تقديم عنوان URL، تشمل المعلومات المسجلة المجالات وعناوين IP المتصلة، الموارد المطلوبة من المجالات، لقطة لصفحة الويب، التقنيات المستخدمة، وبيانات وصفية أخرى عن الموقع.

يوفر الموقع عرضين، الأول يظهر أحدث عمليات المسح التي تم إجراؤها، والثاني يعرض عمليات المسح الحية الحالية.

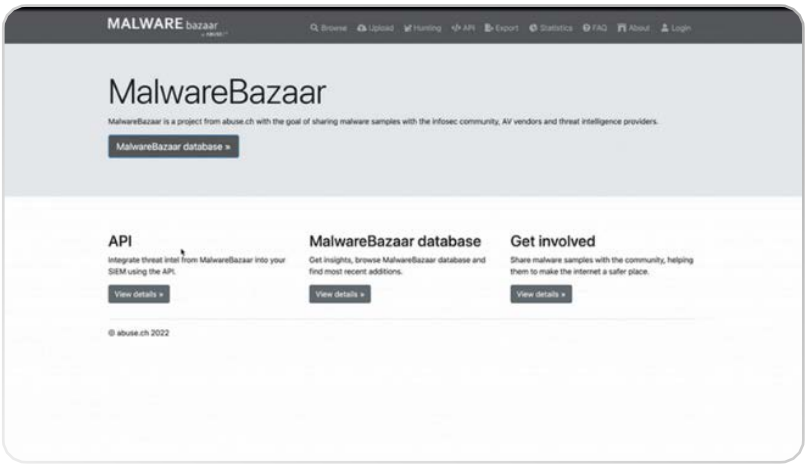
2. Abuse.ch

هو مشروع بحثي مستضاف من قبل معهد الأمن السيبراني والهندسة في جامعة برن للعلوم التطبيقية في سويسرا. تم تطويره لتحديد وتتبع البرمجيات الضارة وشبكات الروبوتات من خلال عدة منصات تشغيلية تم تطويرها ضمن . تشمل هذه المنصات

هذه المنصات هي

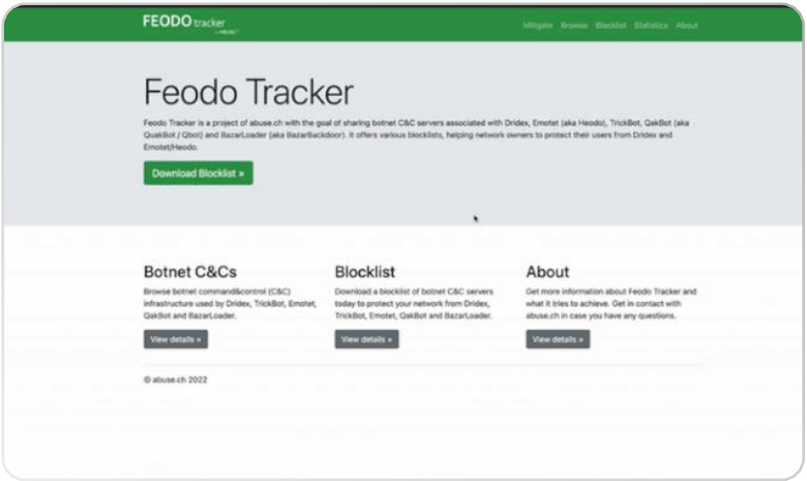
سوق البرمجيات الخبيثة

مصدر لمشاركة عينات البرمجيات الخبيثة



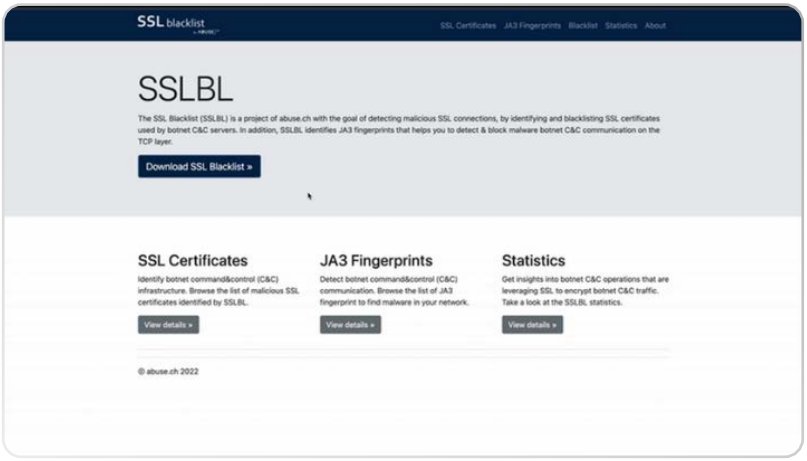
متعقب فيودو Feodo Tracker

مورد يُستخدم لتتبع البنية التحتية للتحكم والقيادة (C2) لشبكات البوتنت المرتبطة بـ Dridex، Emotet، وTrickBot.



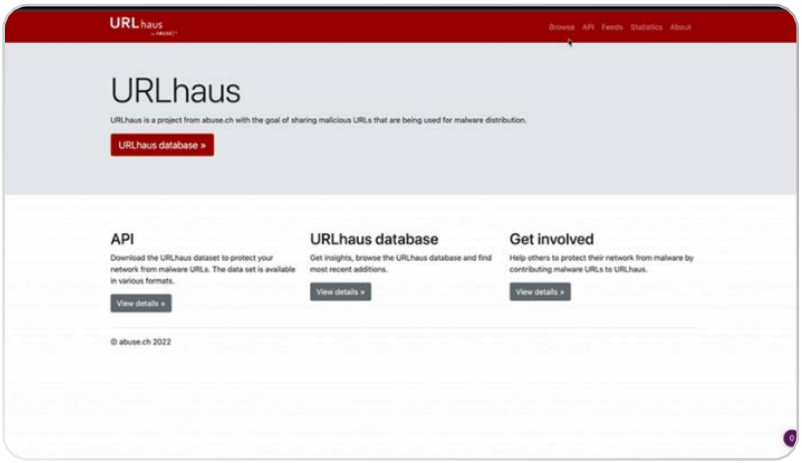
قائمة الحظر SSL

مصدر لجمع وتوفير قائمة حظر للشهادات SSL الضارة وبصمات JA3/JA3s.



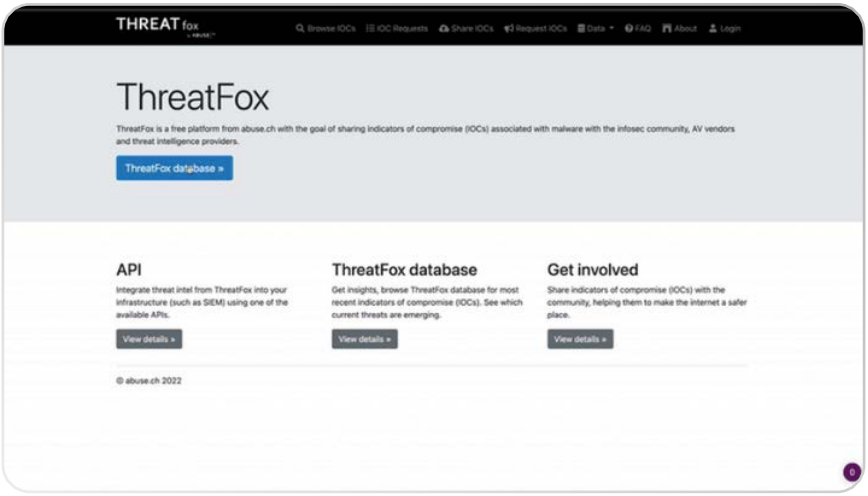
URL Haus

مصدر لمشاركة مواقع توزيع البرمجيات الخبيثة.



ثريت فوكس Threat Fox

مصدر لمشاركة مؤشرات الاختراق (IOCs).



PhishTool

هو أداة مصممة لمساعدتك في تحليل الرسائل الإلكترونية المشبوهة وكشف الحيل التي يستخدمها المجرمون السيبرانيون لمحاولة سرقة معلوماتك. الاحتيال عبر البريد الإلكتروني هو إحدى أكثر الطرق شيوعًا التي يحاول بها المجرمون السيبرانيون خداعك.
إنهم يرسلون رسائل إلكترونية تبدو وكأنها من مصدر موثوق، مثل البنك الخاص بك أو منصة وسائل التواصل الاجتماعي، لكنها في الحقيقة مزيفة.

الميزات
الأساسية

الاستخبارات الاستدلالية

يتم دمج المعلومات المفتوحة المصدر (OSINT) في الأداة لتزويد المحللين بالاستخبارات اللازمة للبقاء على اطلاع على الهجمات المستمرة وفهم التكتيكات والأساليب والإجراءات (TTPs) التي تم استخدامها لتفادي ضوابط الأمان وتمكين الخصم من استخدام الهندسة الاجتماعية لاستهداف الضحية.

إجراء تحليل البريد الإلكتروني

يقوم PhishTool باسترجاع بيانات التعريف من رسائل البريد الإلكتروني الاحتيالية ويقدم للمحللين الشروحات والقدرات اللازمة لمتابعة سلوك الرسالة، والمرفقات، وروابط URL لتصنيف الوضع.

التصنيف والتقارير

يتم إجراء تصنيفات لرسائل البريد الإلكتروني الاحتيالية لتمكين المحللين من اتخاذ إجراءات بسرعة. بالإضافة إلى ذلك، يمكن إنشاء تقارير لتوفير سجل جنائي يمكن مشاركته.

منصات
استخبارات التهديدات

منصات استخبارات التهديدات (TIPs - Threat intelligence platforms) تشبه وجود فريق كامل من خبراء الأمن السيبراني يعملون لديك. تقوم هذه المنصات بجمع وتحليل ومشاركة بيانات استخبارات التهديدات من مصادر متعددة، مما يوفر لك رؤية شاملة لمشهد التهديدات.

Anomali

هذه المنصة مثل مساعد ذكي للغاية يساعدك على أتمتة تحليل استخبارات التهديدات. يمكنها تنقيح جبال من البيانات والعثور على الأدلة الأكثر أهمية، حتى تتمكن من التركيز على اتخاذ الإجراءات.

ThreatConnect

هذه المنصة تشبه مركز القيادة لعمليات استخبارات التهديدات لديك. تساعدك على جمع البيانات من مصادر مختلفة، وتحليلها، ثم مشاركة نتائجك مع الآخرين.

دمج استخبارات التهديدات

دمج استخبارات التهديدات في عمليات الأمن الخاصة بك يشبه وجود فريق من الخبراء يراقبون مشهد التهديدات بشكل مستمر، ويحللون البيانات، ويزودونك برؤى قابلة للتنفيذ. يتيح لك ذلك اكتشاف التهديدات والاستجابة لها بسرعة أكبر، وتعزيز دفاعاتك، وحماية منظمتك من الأضرار في النهاية.

MISP(منصة مبادلة معلومات البرمجيات الخبيثة)

هي منصة مفتوحة المصدر لملفات المعلومات التهديدية التي تسهل جمع وتخزين وتوزيع استخبارات التهديدات ومؤشرات الاختراق (IOCs - Indicators of Compromise) المتعلقة بالبرمجيات الضارة، والهجمات السيبرانية، والاحتيال المالي، أو أي استخبارات ضمن مجتمع من الأعضاء الموثوقين

أنظمة إدارة المعلومات الأمنية والأحداث (SIEM)

نظام إدارة المعلومات الأمنية والأحداث (SIEM - Security Information and Event Management) هو مثل الجهاز العصبي المركزي لشبكتك. يجمع النظام ويحلل سجلات الأمان من جميع أجهزتك، باحثًا عن علامات النشاط المشبوه. من خلال دمج استخبارات التهديدات مع نظام SIEM الخاص بك، يمكنك تعزيز قدراته على الكشف. على سبيل المثال، يمكن لنظام SIEM الخاص بك أن يقوم تلقائيًا بحظر حركة المرور من عنوان IP الذي تم تحديده كخبيث بواسطة مصدر استخبارات التهديدات.

اكتشـف الأخطـاء

From: support@rnicrosoft.co.uk
Sent: 16/05/2023 12:30
To: John Smith <John.Smith@company.com>
Subject: Urgent Action Needed!

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.

please verify your account within 24 hours to avoid any disrupton in your service.

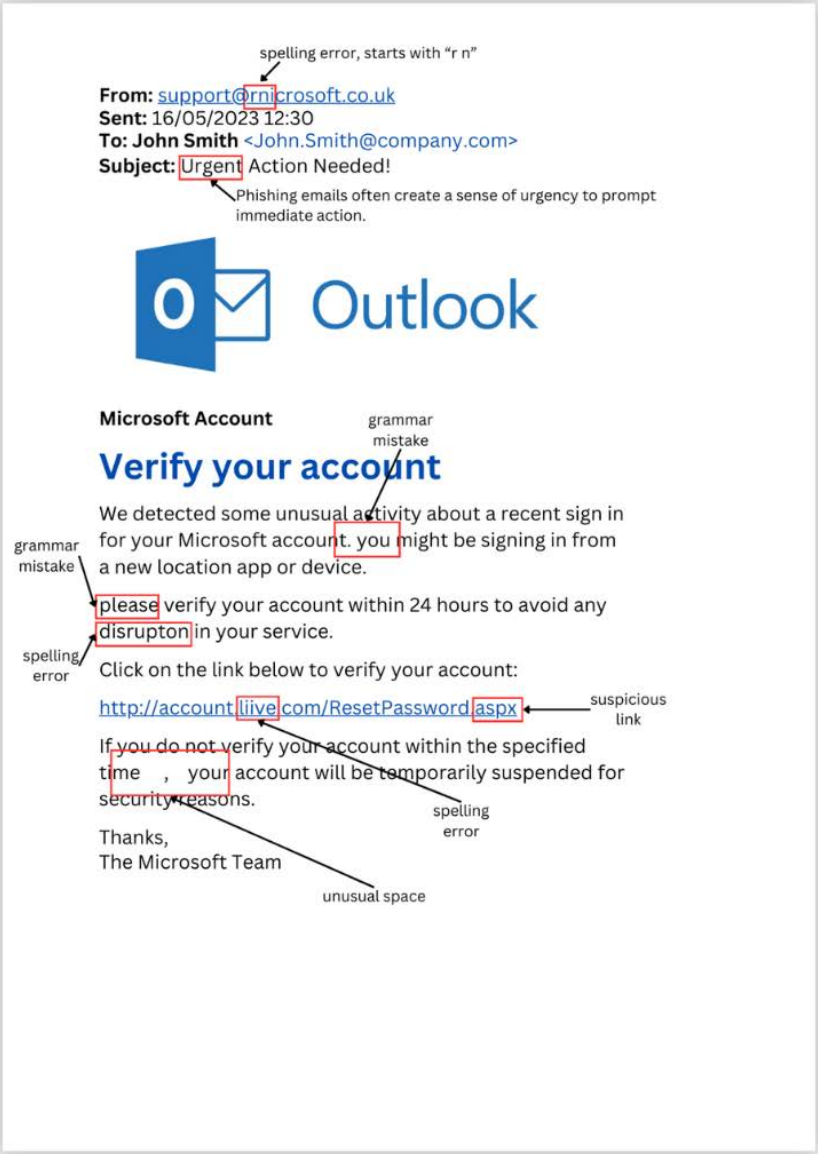
Click on the link below to verify your account:

http://account.liive.com/ResetPassword.aspx

If you do not verify your account within the specified time , your account will be temporarily suspended for security reasons.

Thanks,
The Microsoft Team

الإجابة


spelling error, starts with "r n"
From: support@rnicrosoft.co.uk
Sent: 16/05/2023 12:30
To: John Smith <John.Smith@company.com>
Subject: Urgent Action Needed!
Phishing emails often create a sense of urgency to prompt immediate action.
Outlook
Microsoft Account
grammar mistake
Verify your account
We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.
grammar mistake
please verify your account within 24 hours to avoid any disrupton in your service.
spelling error
Click on the link below to verify your account:
http://account.liive.com/ResetPassword.aspx
suspicious link
If you do not verify your account within the specified time , your account will be temporarily suspended for security reasons.
spelling error
Thanks,
The Microsoft Team
unusual space

التحليل الرقمي للأدلة الجنائية واستجابة الحوادث
Digital Forensics and Incident Response (DFIR)

يغطّي هذا المجال جمع الأدلة الجنائية من الأجهزة الرقمية مثل الحواسيب، وأجهزة الوسائط، والهواتف الذكية للتحقيق في حادثة. يساعد هذا المجال المتخصصين في الأمن على تحديد الآثار التي يتركها المهاجم عند حدوث حادث أمني، واستخدامها لتحديد مدى التهديد في البيئة، واستعادة البيئة إلى الحالة التي كانت عليها قبل وقوع الحادث.

من يقوم ب DFIR؟

التحليل الرقمي للأدلة الجنائية

هؤلاء المحترفون متخصصون في تحديد الأدلة الجنائية أو آثار النشاط البشري في الأجهزة الرقمية.

الاستجابة للحوادث

المستجيبون للحوادث هم خبراء في الأمن السيبراني ويستخدمون المعلومات الجنائية لتحديد النشاط المهم من منظور أمني.

منهجيات التحليل الرقمي
للأدلة الجنائية

المؤشرات الجنائية

المؤشرات الجنائية هي قطع الأدلة التي تشير إلى النشاط الذي تم تنفيذه على النظام. عند إجراء التحليل الرقمي للأدلة الجنائية والاستجابة للحوادث، يتم جمع المؤشرات الجنائية لدعم فرضية أو ادعاء حول نشاط المهاجم.

الحفاظ على الادلة

عند إجراء التحليل الرقمي للأدلة الجنائية والاستجابة للحوادث، يجب علينا الحفاظ على سلامة الأدلة التي نقوم بجمعها. يجب أن نلاحظ أن أي تحليل جنائي يلوث الأدلة. لذلك، يتم أولاً جمع الأدلة وحمايتها من الكتابة. ثم، يتم استخدام نسخة من الأدلة المحمية من الكتابة للتحليل.

سلسلة العهدة Chain of Custody

هي التوثيق الزمني الكامل لكيفية جمع الأدلة وحفظها ونقلها وتحليلها حتى استخدامها كدليل، بهدف ضمان عدم التلاعب بها وإثبات موثوقيتها.

منهجيات التحليل الرقمي
للأدلة الجنائية

ترتيب التطاير Order of volatility

ليست جميع الأدلة الرقمية متساوية؛ فبعضها قد يختفي خلال ثوانٍ، بينما يبقى بعضها الآخر لفترة طويلة.
لذلك يحرص محققو الأدلة الرقمية على جمع الأدلة الأكثر عرضة للفقدان أولًا، مثل البيانات الموجودة في ذاكرة RAM، قبل الانتقال إلى الأدلة الأكثر ثباتًا، مثل الملفات المخزنة على القرص الصلب. ويساعد ذلك على الحفاظ على الأدلة المهمة وعدم فقدانها أثناء التحقيق.

إنشاء الجدول الزمني

بمجرد أن نقوم بجمع الأدلة والحفاظ على نزاهتها، نحتاج إلى تقديمها بطريقة مفهومة للاستفادة الكاملة من المعلومات التي تحتوي عليها.

يجب إنشاء جدول زمني للأحداث لتحليل فعال ودقيق. يضع هذا الجدول الزمني جميع الأنشطة بالترتيب الزمني. تُسمى هذه العملية إنشاء الجدول الزمني.

نشاط - الأدلة

المشهد

في صباح يوم 10 يوليو 2024، اكتشف قسم تكنولوجيا المعلومات في شركة TechSecure Inc. نشاطًا غير عادي في سجلات خادم قاعدة البيانات الرئيسي. عند الفحص الدقيق، وجدوا العديد من محاولات تسجيل الدخول الفاشلة تلتها محاولة تسجيل دخول ناجحة في الساعة 2:30 صباحًا. مدركين خطورة الوضع، قام القسم على الفور بتنبيه فريق الأمن السيبراني في الشركة.

بدأ فريق الأمن السيبراني، بقيادة المحللة جين سميث، تحقيقهم. عزلوا الخادم المعرّض للخطر لمنع الوصول غير المصرح به، وقاموا بإنشاء صورة جنائية للقرص الصلب للتحليل التفصيلي. في الوقت نفسه، فحص المتخصص في تكنولوجيا المعلومات مايكل جونسون سجلات حركة مرور الشبكة، التي كشفت عن عنوان IP مشبوه يقوم بالاتصالات خلال وقت الاختراق.

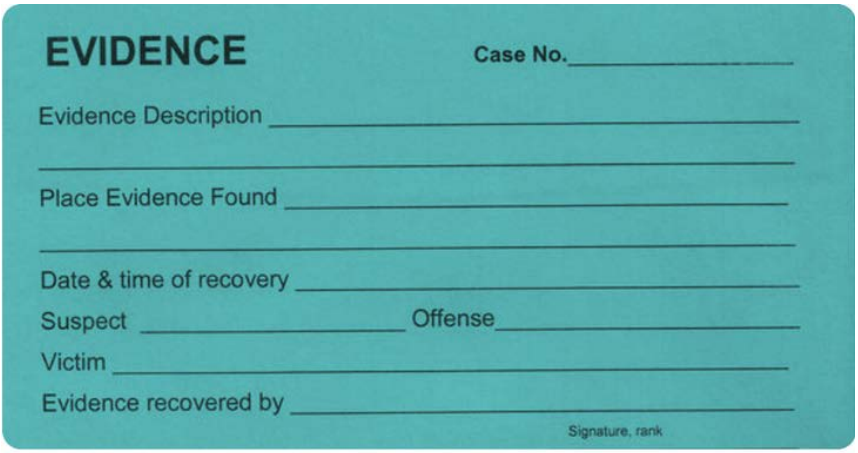
في 12 يوليو 2024، كشفت التحقيقات الإضافية في سجلات الموظفين أن عنوان IP مرتبط بجون دو، وهو موظف في إجازة حاليًا. قررت جين ومايكل فحص صندوق بريد جون دو الإلكتروني واكتشفوا رسالة تصيد أُرسلت إليه في 9 يوليو 2024، تحتوي على رابط خبيث مصمم لسرقة بيانات تسجيل الدخول الخاصة به. باستخدام الأدوات الجنائية، وجدت جين آثار رسالة التصيد التي أدت إلى تسجيل الدخول الناجح في الساعة 2:30 صباحًا في 10 يوليو. كانت رسالة التصيد قد خدعت جون للكشف عن بياناته، والتي استخدمها المهاجم للوصول إلى قاعدة البيانات.

بحلول 12 يوليو 2024، كان فريق الأمن السيبراني قد جمع جميع الأدلة، بما في ذلك رسالة التصيد وسجلات الشبكة وصورة القرص الجنائية، والتي كانت حاسمة في فهم الاختراق. وثقوا نتائجهم في تقرير، محددين استخدام بيانات تسجيل الدخول المسروقة نتيجة لهجوم تصيد كسبب للاختراق.

قامت شركة TechSecure Inc. على الفور باتخاذ إجراءات لتأمين أنظمتها، وقامت بتنفيذ المصادقة المتعددة العوامل، وبدأت تدريبًا شاملاً للشركة بأكملها حول الوعي بالتصيد الاحتيالي. كما قامت بالاتصال بإنفاذ القانون بالأدلة لتتبع الجاني ومنع الحوادث المستقبلية.

لم تساعد هذه التحقيقات المفصلة في تحديد سبب الخرق فحسب، بل ضمنت أيضًا أن تتمكن TechSecure Inc. من تحسين تدابير الأمان الخاصة بها للحماية ضد هجمات مماثلة في المستقبل.

تقرير الأدلة


EVIDENCE

Case No._____

Evidence Description _____

_____

Place Evidence Found _____

_____

Date & time of recovery _____

Suspect _____ Offense_____

Victim _____

Evidence recovered by _____

Signature, rank

منهجيات

استجابة الحوادث

استجابة الحوادث (IR - Incident response) هي نهج منظم للتعامل مع إدارة تداعيات اختراق الأمان أو الهجوم السيبراني. الهدف هو التعامل مع الوضع بطريقة تحد من الأضرار وتقلل من وقت وتكلفة الاستعادة.

اثنان من الإطارات المعروفة هي:

1) إطار NIST SP 800-61

يحدد هذا الإطار **أربع مراحل** رئيسية للاستجابة للحوادث الأمنية:

الإعداد (Preparation): الاستعداد للحوادث من خلال وضع الخطط والأدوات والإجراءات.

الكشف والتحليل (Detection and Analysis): اكتشاف الحادث وتحليل سببه وتأثيره.

الاحتواء والإزالة والتعافي (Containment, Eradication, and Recovery): احتواء الحادث، وإزالة سبب الاختراق، واستعادة الأنظمة إلى وضعها الطبيعي.

النشاط بعد الحادث (Post-Incident Activity): توثيق الحادث واستخلاص الدروس لتحسين الاستجابة مستقبلًا.

2) منهجية SANS PICERL

هي طريقة لتذكر مراحل الاستجابة للحوادث، ويتكون اسمها من الأحرف الأولى للمراحل التالية:

(الإعداد Preparation)

(التعرّف على الحادث Identification)

(الاحتواء Containment)

(الإزالة Eradication)

(التعافي Recovery)

(الدروس المستفادة Lessons Learned)

أفضل الممارسات في التحقيقات الرقمية واستجابة الحوادث

يتحمل المحترفون في مجال التحقيقات الرقمية واستجابة الحوادث (DFIR) مسؤولية إجراء تحقيقاتهم بطريقة قانونية وأخلاقية. وهذا يعني:

احترام الخصوصية: علينا أن نكون حريصين على عدم الوصول إلى المعلومات الشخصية أو مشاركتها دون داع.

الحفاظ على السرية: علينا الحفاظ على سرية المعلومات الحساسة، حتى بعد اكتمال التحقيق.

اتباع القانون: علينا الالتزام بجميع القوانين واللوائح المنطبقة، مثل قانون الخصوصية في الاتصالات الإلكترونية (ECPA).

التوثيق والتقارير

التوثيق ضروري في التحليل الجنائي الرقمي واستجابة الحوادث. يجب علينا الاحتفاظ بسجلات مفصلة لكل ما نقوم به، بدءًا من الكشف الأولي عن الحادث وصولاً إلى الحل النهائي. يمكن استخدام هذه الوثائق لتحسين عمليات استجابة الحوادث، وتدريب الموظفين الجدد، وحتى استخدامها كأدلة في المحكمة.

التقارير أيضًا جزء مهم من التحليل الجنائي الرقمي واستجابة الحوادثDFIR . يجب علينا التواصل مع أصحاب المصلحة بشأن نتائجنا بطريقة واضحة وموجزة. قد يتضمن ذلك كتابة تقرير تقني لموظفي تكنولوجيا المعلومات، أو تقرير ملخص للمديرين التنفيذيين، أو حتى بيان صحفي للجمهور.

مقدمة في أدوات التحليل الجنائي الرقمي

استجابة الحوادث (DFIR)

لقد طورت الصناعات الأمنية أدوات متنوعة متخصصة للمساعدة في عملية التحليل الجنائي الرقمي واستجابة الحوادث.

تساعد هذه الأدوات على توفير الوقت الثمين وتعزيز قدرات المتخصصين في الأمن.

أدوات التصوير

الجنائي الرقمي

تُستخدم لإنشاء نسخة جنائية مطابقة للأصل بتًا ببت (Bit-by-Bit) من وسائط التخزين الرقمية، مثل الأقراص الصلبة ووسائط التخزين الأخرى. وتحافظ هذه النسخة على جميع البيانات كما هي، مما يسمح للمحققين بتحليل الأدلة دون المساس بالأصل.

أدوات التصوير الجنائي في ويندوز

FTK Imager

هذه الأداة الشهيرة من AccessData هي عنصر أساسي في العديد من مختبرات التحليل الجنائي الرقمي.
تُعرف بواجهة المستخدم السهلة وقدرتها على إنشاء صور جنائية لمجموعة متنوعة من أجهزة التخزين، بما في ذلك الأقراص الصلبة، أجهزة USB، وبطاقات الذاكرة.

KAPE

(Kroll Artifact Parser and Extractor)

تم تطويره بواسطة إريك زيمرمان الشهير، يقوم kape بأتمتة جمع وتحليل الآثار الجنائية، مما يوفر الوقت والجهد الثمينين.

أدوات التحليل

الجنائي الرقمي

أدوات التحليل الجنائي الرقمي تشبه عدسة المكبر ومجموعة بصمات الأصابع لدينا، تساعدنا في الغوص في البيانات وكشف الأدلة المخفية.

أدوات التحليل الجنائي في ويندوز

Eric Zimmerman's Tools

إريك زيمرمان هو خبير أمن سيبراني مشهور قام بتطوير مجموعة من الأدوات القوية خصيصًا لتحليل أنظمة ويندوز.
تساعدنا هذه الأدوات في الغوص بعمق في سجل ويندوز، أنظمة الملفات، وأدوات أخرى لكشف أدلة النشاط الخبيث.

Autopsy

هذه المنصة مفتوحة المصدر هي متجر شامل للتحليل الجنائي. تتميز بواجهة مستخدم سهلة الاستخدام ونطاق واسع من الميزات، مما يجعلها خيارًا شائعًا لكل من المبتدئين والمحترفين في التحقيقات.

أدوات

استجابة الحوادث

أدوات استجابة الحوادث هي أسلحتنا في المعركة ضد التهديدات السيبرانية. تساعدنا هذه الأدوات على الكشف السريع، والاحتواء، والقضاء على الهجمات، مما يقلل الأضرار ويعيد العمليات إلى طبيعتها.

Wireshark

مُحلل بروتوكولات الشبكة هذا يشبه التنصت على شبكتك. يقوم بالتقاط وتحليل حركة مرور الشبكة، مما يتيح لك رؤية البيانات التي يتم إرسالها واستلامها.

Sysinternals Suite

هذه المجموعة من الأدوات من مايكروسوفت تشبه صندوق أدوات مليئًا بالأدوات المتخصصة لأنظمة ويندوز. تشمل أدوات مثل Process Explorer (لمراقبة العمليات الجارية)، وProcess Monitor (لتتبع نشاط نظام الملفات والسجل)، وAutoruns (لتحديد البرامج التي تبدأ تلقائيًا). يمكن أن تساعدك هذه الأدوات في تحديد والتحقق من النشاط المشبوه على نظام مخترق.

(Redline) FireEye

هذه الأداة تشبه مجموعة المستجيبين الأوائل لجهاز الكمبيوتر الخاص بك. تقوم بجمع البيانات الجنائية من النظام بسرعة، مما يعطيك لمحة عما يحدث ويساعدك في تحديد التهديدات المحتملة.

تكامل أدوات التحليل الجنائي الرقمي واستجابة الحوادث

القوة الحقيقية للتحليل الجنائي الرقمي واستجابة الحوادث تأتي من دمج الأدوات والتقنيات المختلفة. من خلال دمج أدوات التحليل الجنائي الرقمي الخاصة بك مع أدوات أمان أخرى، مثل أنظمة إدارة معلومات الأمان والأحداث (SIEM Security Information and Event Management) ومنصات تنسيق الأمان والأتمتة والاستجابة (SOAR - Security Orchestration Automation, and Response) ، يمكنك إنشاء نظام دفاع قوي يكون دائمًا في حالة تأهب للتهديدات.

الإجابات

مغامرة في عالم الأمن السيبراني
p.07

1- Malware
2- firewall
3- ransomware
4- privacy
5- worms
6- cyberattack
7- phishing
8- encryption
9- patch
10- hacking

التسلسل الهرمي للنطاق
p.31

اخترق كلمة المرور
p.93

IT TAKES A FRIEND
TO MAKE A FRIEND.
HEY YOU FIGURED
OUT MY PASSWORD!
YOU ARE RAD!

فك التشفير
p.100

authentication

لعبة ترتيب الكلمات
p.40

PING
CHAT
RANGE
CLIENT
DOMAIN
PORT
STRING
FOLDER
METHOD
QUERY
UNIFORM
DISK

رمز حالة HTTP :
page not found

تقرير الأدلة
p.138

رقم القضية: 0710-TSI-2024
وصف الدليل: صورة جنائية للقرص الصلب للخادم المخترق، ورسالة تصيد إلكتروني، وسجلات الشبكة، وسجلات تسجيل الدخول، وسجلات الموظفين.
مكان العثور على الدليل: شركة TechSecure Inc. – خادم قاعدة البيانات الرئيسي، سجلات الشبكة، والبريد الإلكتروني الخاص بالموظف John Doe.
تاريخ ووقت استعادة الدليل: 12 يوليو 2024
المشتبه به: مهاجم مجهول
نوع الجريمة: دخول غير مصرح به باستخدام بيانات اعتماد مسروقة نتيجة هجوم تصيد إلكتروني.
الضحية: شركة TechSecure Inc. (تم اختراق بيانات اعتماد الموظف John Doe)
تم جمع الدليل بواسطة:
Jane Smith (محللة أمن سيبراني رئيسية)
و Michael Johnson (أخصائي تقنية معلومات)

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

للتواصل

مع الأكاديميـة الوطنيـة للأمن السيبراني
بشأن المخيـم، يرجى التواصـل عبر الأرقـام التاليـة:

مركز الاتصـال
16555

أرقـام الهواتـف
00974 4046 6379
00974 4046 6623
00974 5104 5944

الإيميـل
academy@ncsa.gov.qa

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المخيم الشبابي للأمن السيبراني 2026
CYBER SECURITY YOUTH CAMP 2026

academy.ncsa.gov.qa