



أمن الشبكات وحمايتها

إعداد المادة العلمية

الأستاذ بلال جناجرة

قسم تكنولوجيا المعلومات

2022

الفهرس

الوحدة الأولى

مقدمة في امن الشبكات

الوحدة الثانية

الجدران النارية

الوحدة الثالثة

مسح المنافذ

الوحدة الرابعة

مراقبة الشبكة ضد الإختراق

الوحدة الخامسة

التتبع والخصوصية على الإنترنت

الوحدة السادسة

المصادقة وتشفير البيانات

الوحدة السابعة

حماية الخوادم

الوحدة الثامنة

امن الشبكات الاسلكية

المشاريع

مقدمة فى أمن الشبكات

أصبحت الشبكات الإلكترونية من الضروريات الحاصلة فى عصرنا الحديث . بحيث لاغنى عنها فى المؤسسات والشركات والحكومات بل وحتى فى البيوت ، فحيثما أنت تجد من حولك أنواع عديدة من شبكات الحواسيب التى تنقل كمأ هائلاً من المعلومات والبيانات بين الأشخاص والمؤسسات على مستوى العالم . وتتنوع هذه المعلومات والبيانات فى أهميتها ودرجة سريتها من المعلومات العامة والعلمية العادية إلى المعلومات والإحصائيات الحكومية وميزانيات الدول والمعلومات الإستخبارتية بالغة الخطورة والسرية ، ولكل هذه الأنواع من المعلومات والبيانات إنما يتم تناقلها وحفظها فى غالب الأحيان عبر شبكات الحاسوب على إختلاف أنواعها وأماكنها .

ويمكننا تعريف " أمن شبكات المعلومات " على أنه مجموعة من الإجراءات التى يمكن خلالها توفير الحماية القصوى للمعلومات والبيانات فى الشبكات من كافة المخاطر التى تهددها ، وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية ، أو هي مجموعة من المعايير التى تحول دون وصول المعلومات المخزنة فى الشبكات إلى الأشخاص غير المخول لهم الحصول عليها .

أهداف أمن الشبكات

هناك مجموعة من الأهداف المحددة التى يتبناها علم أمن المعلومات ، ومن أهم تلك الأهداف ما يلي :

* توفير الحماية الكاملة لأنظمة الحاسوب التى يتم إستخدامها فى تخزين ومعالجة البيانات والمعلومات على الحواسيب .

* توفير كافة الضوابط الأمنية التى يتم إستخدامها من أجل حماية النظام .

* كما يعمل على دعم وحماية قنوات الإتصال المختلفة المستخدمة من أجل الوصول إلى البيانات والمعلومات .

* تعمل عناصر أمن المعلومات على توفير نظام عالي من السرية التى تهدف بشكل أساسى إلى إستمرار عملية الحماية والتأمين فى كافة الأوقات .

مقدمة حول الإختراق الأخلاقى introduction to ethical hacking

هناك الكثير من الحوادث التي حصلت منها تسريب بيانات أكثر من 140 مليون مستخدم على موقع Epay. مثل البريد الإلكتروني واسم المستخدم وكلمات المرور وتاريخ الميلاد حصلت

في عام 2013 و2014 وايضاً حادثة تطبيق google play تم رفع تطبيق خبيث من قبل شخص تركي ومنع وحجب ملفات Apk وهي ملفات خاصة للأندرويد وغيرها من الحوادث .

امن المعلومات : أي امر يتم أو إجراء يتم اتباعه للحفاظ على البيانات او البنية التحتية للشبكات وأجهزة وخوادم وغيرها من الأمور من أي عملية سرقة أو تعديل أو حجب الخدمات للتقليل من كفاءتها وقدرتها .

العلماء قامو بتصنيف أي نظام آمن إلى :

1.السرية والخصوصية Confidentiality

تعني أن البيانات أو الخدمات فقط يتم الحصول عليها والوصول لها من الأشخاص المصرح لهم بذلك أي أن شخص غير مصرح له للوصول إلى الخدمات أو البيانات يجب أن لا يكون له القدرة للوصول للبيانات وغيرها من أمور مختلفة.

2.التكاملية Integrity

هو عدم قدرة أي شخص غير مصرح له التعديل على البيانات سواء كان إضافة أو تدمير أو حذف .

3.التوفر Availability

المقصود به أن الخدمة أو البيانات يجب أن تكون متوفرة عند طلبها

4.المصادقة Authenticity

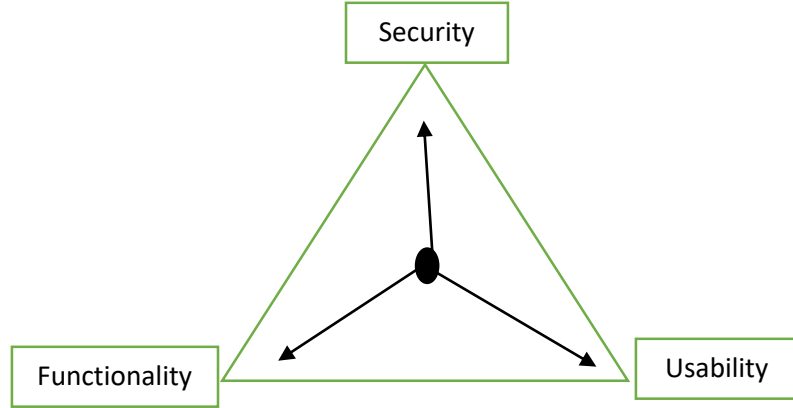
أي الوثوق من الجهة التي ارسلت البيانات مثل ارسال بيانات على البريد الإلكتروني أي التأكد من مرسل البيانات هل هو نفس الشخص أو إنتحال شخصية.

5.عدم الإنكار Non-Repudiation

المقصود به أن أي شخص قام في إرسال بيانات أو قام بعمل أمر معين لن يستطيع إنكار بأنه هو من قام بهذا الأمر.

مثال : شخص يرسل بريد إلكتروني فيه تهديد لا يستطيع الإنكار أنه هو من قام بذلك.

قوة أي نظام أو شبكة تقاس بثلاثة أمور رئيسية وهي :



Security : المقصود بها الأمن

Functionality : الوظائف الموجودة فيها

Usability : سهولة الإستخدام

هناك سؤال لماذا يوجد هناك ثغرات كثيرة في الأنظمة الكبيرة وهذه الأنظمة يعمل عليها الكثير من المطورين والمبرمجين والخبراء سواء كانت تطبيقات أو مواقع أو خدمات أو أنظمة تشغيل .

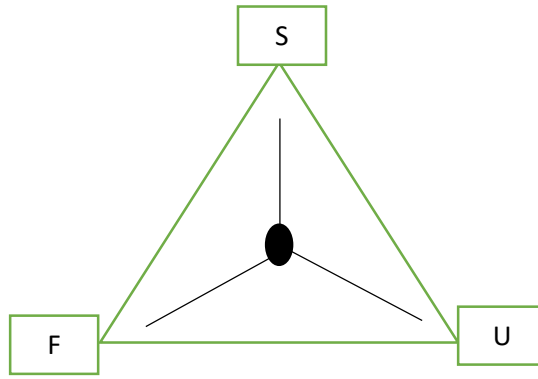
السبب الرئيسي عندما نقوم في إضافة خصائص أو قوة مثلاً functionality على نظام معين تقل كفاءة وقوة Usability و security وفي حالة زيادة خصائص وقوة على Usability تقل قوة security و functionality وفي حال تم زيادة القوة على security تقل قوة usability و functionality.

مثال : لدينا حساب على موقع مثلاً ليكن Facebook في حال تم تفعيل الخصائص الأمنية مثل التحقق بخطوتين هذا الأمر يؤدي إلى تقليل Usability أي كل ما ندخل من جهاز

آخر أو أي جهاز سيقوم Facebook بإرسال رمز إلى الموبايل سيقفل من سهولة الإستخدام للنظام.

هذا هو السبب الرئيسي لوجود الثغرات الأمنية أي كلما كثرت الوظائف وزيادة سهولة الإستخدام قل أمن المعلومات .

لذلك يحاول مطورو الأنظمة والشبكات أن يكونو قدر الإمكان أن يقدمو كثير من Usability و functionality و security أي يكونو في المنتصف .



بعض المفاهيم الرئيسية التي يجب معرفتها

- Hack Value

المقصود بها هل عملية الإختراق بالنسبة للمخترقين هي عملية مجدية وماهي الفوائد التي سيحصل عليها المخترقين هل هي فوائد مالية او سياسية او انتقام وغيرها من الأمور.

- Vulnerability (الثغرة)

المقصود بها هي عبارة عن أي نقطة ضعف سواء كانت برمجية أي من خلالها يمكن الوصول إلى المعلومات والبيانات الغير مصرح له للدخول إليها سواء كانت نظام أو شبكة.

- **Exploit (الإستغلال)**

هو عبارة عن الرمز الذي قام به المخترق في إستغلال الثغرة للوصول إلى أمر معين داخل النظام الذي يحاول إختراقه.

- **Payload**

هو جزء من exploit يقوم بأمر معين.

- **Zero – Day Attack (هجوم اليوم صفر)**

هي ثغرة تم إكتشافها والجهة التي قامت في إكتشافها لم تقوم بإصدار باتش لسد هذه الثغرة.

- **Daisy Chaining**

المقصود به هو عبارة عن استفادة المخترق من المعلومات التي تم جمعها للوصول إلى أجهزة أخرى داخل الشبكة أو النظام.

- **Doxing**

المقصود بها عبارة عن عملية نشر البيانات "بيانات تعريفية خاصة بـ شخص معين أو جهة معينة من خلال مواقع التواصل الإجتماعي وتجميع هذه البيانات منها.

- **Bot**

عبارة عن برنامج بسيط مجرد تثبيته على جهاز الضحية أو الجهاز المخترق يقوم هذا البرنامج في عملية إتصال مع جهاز المخترق لإستقبال أوامر منه من أجل تنفيذها.

حتى تحدث الهجمة يجب أن تتوفر ثلاثة عناصر رئيسية :

Attacks = Motive + Method + Vulnerability

Motive : حيث تمثل الدافع

Method : حيث تمثل الطريقة / المنهجية

Vulnerability : حيث تمثل القابلية

Attacks : حيث تمثل الهجمة / الهجمات

Motive

الدافع او الهدف من وراء الإختراق وهناك الكثير من الأهداف مثل سرقة البيانات أو الإنتقام أو سياسية أو مالية وغيرها.

Method

الطريقة أو المنهجية التي يقوم من خلالها المخترق لشن الهجمة .

Vulnerability

الثغرة سواء في النظام أو الشبكة أو إستغلال ثغرات في الأشخاص نفسهم وهي الهندسة الإجتماعية.

مجموعة من الهجمات التي يتم شنها

- TOP INFO-SEC ATTACK VECTORES

يستخدم هذه الهجمة مهاجمي الإنترنت لاستهداف المستخدمين أو سرقة بياناتهم الحساسة أو استغلال نظام الشبكة الخاص بهم.

- CLOUD COMPUTING THREATS

-

هجمات على وحدات التخزين السحابية المختلفة.

- ADVANCED PERSISTENT THREATS

عبارة عن هجمات أو حملات إلكترونية يتم من خلالها تجميع بيانات مختلفة عن الضحايا دون علمهم لفترات طويلة من خلال البرامج الخبيثة.

- MALWARES

هي عبارة عن برنامج او برامج ضارة او ملف يتسبب عمداً في الحاق الضرر بجهاز الحاسوب او الخادم.

- MOBILE THREATS

هي هجمات يتم شنّها على الموبايل.

- BOTNET

هي عبارة عن شبكة من BOTS. مثال : تثبيت برنامج على الشبكة يعمل على الأتصال مع المخترق والإنتظار منه لتنفيذ الأوامر ويكون هذا البرنامج على أكثر من جهاز يسمى BOTNET.

- INSIDER ATTACK

هي أخطر شئى أي يكون داخل الشركة يقوم بسرقة البيانات ويقوم في إختراق الشركة.

- INFO-SEC THREAT CATEGORIES

التهديدات الأمنية يمكن تصنيفها إلى ثلاث أصناف رئيسية(هذه التهديدات تتم على الشبكة)

1. NETWORK THREATS تهديدات على الشبكة

2. HOST THREATS تهديدات على الأجهزة الموجودة على الشبكة

3. APPLICATION THREATS التطبيقات والأنظمة الموجودة على المضيف

من الأمثلة على التهديدات الموجودة على الشبكة عملية جمع البيانات من الشبكة – معرفة ماهي الأجهزة المتصلة بالشبكة – معرفة أنظمة التشغيل الموجودة على الشبكة – عملية التنصت على الشبكة – عملية سرقة الجلسة SESSION – تسميم DNS ومحاولة فك كلمة المرور وغيرها .

التهديدات التي تتم على الأنظمة وهي اربعة أنواع (TYPE OFF ATTACKS ON SYSTEM)

- OS ATTACKS

هجمات على نظام التشغيل ويتم من خلالها إستغلال ثغره موجودة بنظام التشغيل أو ثغرة في الأصل موجودة ولم يتم تطبيق الحماية وسد هذه الثغرة ويتم من خلالها عمل هجمة.

- MIS – CONFIGURATION ATTACKS

هجمات الخطأ في الإعدادات
مثال: WEB SERVER مثل تفعيل عليه خاصية لملف معين و ثم رؤيته من قبل شخص غير مصرح له في الدخول أي تفعيل خاصية عن طريق الخطأ.

- APPLICATION LEVEL ATTACKS

مثل هجمات على الأنظمة مثل SQL ENJECTION

- SHRINK-WRAP CODE ATTACKS

هي إستغلال الثغرات في البرامج سيئة التكوين .
مثال : لدينا نظام قمنا في تطويره وفي حال نريد تطوير جزء معين نأخذ كود موجود على الإنترنت أو على نظام اخر DDL FILE ومجرد تطبيقه يكون فيه ثغرة امنية تؤدي إلى إختراق النظام.

* مصطلح الحرب على المعلومات (INFORMATION WARFARE)

الهدف منه سواء كان التنافس شركة مع شركة أو دولة مع دولة أي تحاول كل جهة الإستفادة من المعلومات من الجهة الأخرى لتحقيق أفضلية أكثر من الأخرى .

مثال : شركة A و B شركة A يجب أن يكون عندها أمرين DEFENSE أي الدفاع

و OFFENSE الهجوم .

أي كل جهة يجب أن يكون لديها DEFENSE أي تقوم بعمل إجراءات أمنية كبيرة داخل

شبكةها و أنظمتها وشركتها من أجل الحماية من الجهة الأخرى و OFFENSE محاولات

هذه الجهة من أجل شن هجمات على الجهة الأخرى للحصول على المعلومات منها وتكسب افضلية على الجهة الأخرى.

HACKING CONCEPTS مفهوم الإختراق

الإختراق : هي أي عملية يتم من خلالها إستغلال ثغرة أمنية موجودة في نظام معين تمكن المخترق من الحصول على صلاحيات غير مصرح له الوصول إليها سواءاً على نظام التشغيل أو الشبكة أو المصادر الموجودة عليه وبالتالي يمكن للمخترق أن يقوم بتعديل على نظام التشغيل والتعديل على الخصائص الموجودة على هذا النظام وسحب الملفات وتشفير الملفات وطلب فدية وتدمير الملفات والكثير من الأمور المختلفة .

الهاكر : هو شخص لديه مهارات عالية جداً في مهارات الكمبيوتر وشخص خبير في أنظمة الكمبيوتر والشبكات وفي الأنظمة والبرمجة وغيرها من الأمور وهذه المهارات تمكنه من كسر أي نظام كمبيوتر سواء كان هذا النظام شبكة وغيرها طبعاً عن طريق إكتشاف الثغرات الموجودة وكتابة إستغلال للثغرات وإستخدام ثغرات مكتوبة من قبل .

يمكن تصنيف المخترقين الى ثمانية أصناف مختلفة HACKER CLASSIFICATIONS

1.WHITE HAT HACKERS

هو الهاكر الأخلاقي الذي يستغل مهاراته المختلفة في الكمبيوتر وانظمته إلى إكتشاف الثغرات في الأنظمة ويقوم في ابلاغ الجهات الخاصة والتي يتم إكتشاف الثغرات فيها لئتم إصلاح هذه الثغرات .

2.BLACK HAT HACKERS

هم الهاكر الذين يقومون في عملية الإختراق لعمل أمر سيئ مثل تدمير البيانات وطلب فدية وأمور مالية وأمور مختلفة .

3.GRAY HAT HACKERS

هم الهاكر مابين وبين عباره عن هاكر يقومون في إكتشاف الثغرات وإبلاغ الجهات المختلفة لحل هذه الثغرات ويمكنهم شن هجمات لطلب فدية أي بين النوعين السابقين يصنفون.

4.SUICIDE HACKERS

هم الهاكر الإنتحارين وهم يقومون بشن هجمات وعمليات إختراق رغم معرفتهم أن هذه العمليات ستؤدي إلى سجنهم ومعاقبتهم رغم ذلك لايهتمون لذلك.

5.SCRIPT KIDDIES

هم هاكر لا يوجد لديهم معرفة في أنظمة الكمبيوتر والشبكات والحماية هم فقط يستخدمون

أدوات جاهزة وبرامج مثل برامج NJRAT و RAT وغيرها فقط محاولة الإختراق باستخدام البرامج .

6. CYBER TERRORISTS الإرهابيين الإلكترونيين

هم أشخاص وظيفتهم ودوافع سياسية أو إنتقامية شن هجمات إرهابية.

7. STATE SPONSORED

هم هاكر مدعومين من الجهات الحكومية وظيفتهم شن هجمات حكومية لتدمير الدول المعادية وتدمير الحكومات المعادية للدولة وغيرها من الأمور .

8. HACKTIVIST

هم ناشطين إلكترونيين يحولون أي عملية إختراق لنشر أهدافهم ممكن هذه الأهداف دينية أو للإنتقام من أمر معين مثل Anonamous الذين يقومون بشن هجمات وتشويه للمواقع الإلكترونية وتغيير الصفحة الرئيسية ووضع شئى خاص بهم.

مراحل الإختراق يمكن تصنيفها إلى خمس تصنيفات رئيسية

1. RECONNAISSANCE عملية جمع المعلومات

يقوم الهاكر بجمع المعلومات حول الهدف أو الجهة المراد إختراقها سواء التوصل المباشر مع هذا الهدف مثل هذه المعلومات معرفة اسماء الموظفين في الشركة و العنوان المنطقي IP والبريد الإلكتروني والنطاقات وغيرها.

2. SCANNING AND ENUMERATION

هدف هذه المرحلة معرفة عناوين الإنترنت الخاصة في الشبكة التي تعمل على أنظمة تشغيل موجودة في الشبكة والخوادم للشركة المراد إختراقها ومعرفة ماهي المنافذ المفتوحة ومعرفة ماهي الخدمات المتصلة في الخوادم وإصدار هذه الخدمات ووقت تشغيل الخدمات وغيرها.

3. GAINING ACCESS عملية الحصول على صلاحيات

عملية الإختراق وهي الوصول إلى نظام التشغيل من خلال الثغرة مثل فك كلمة المرور والثغرة .

4.MAINTAINING ACCESS الحفاظ على الوصول

يجب على الهاكر المحافظة على الوصول حتى بعد إغلاق الثغرة أي يعمل له عملية إتصال خاص حتى عن بعد إغلاق الثغرة أي تأمين نفسه لكي يبقى متصلاً.

5.COVERING TRACKS

يحاول المخترق بحذف أي أدلة جنائية لحماية نفسه من التتبع وكشفه في حال تم إجراء عملية تحقيق جنائي رقمي .

ETHICAL HACKING

هو عبارة عن مصطلح يمثل إستخدام عملية الإختراق على شركة معينه أو جهة معينة ولذلك لمساعدة هذه الجهة أو الشركة على حل الثغرات الأمنية والتعرف عليها لحلها.

ويقوم بإستخدام تقنيات لمحاكاة الهاكر من أجل الفحص وتأمين الشركة ومحاولة تجاوز أي نظام حماية موجود داخل الشركة من أجل الحماية.

VULNERABILITY ASSESSMENT تقييم الثغرات

هذا المصطلح عبارة عن عملية يتم من خلالها تحديد تصنيف الثغرات الأمنية في أنظمة الكمبيوتر المختلفة بالإضافة إلى ذلك فهي تقوم بتوقع وتنبوء مدى إستجابة الإجراءات الأمنية المتبعة في الشركة أو في الجهة المراد عمل تقييم ثغرات لها من أي عملية فحص أو محاولة إختراق.

الـ VULNERABILITY ASSESSMENT تحتوي على عدة أمور

- 1.نقوم بتعريف وتصنيف المصادر الموجودة في الأنظمة المراد عمل لها تقييم.
- 2.نقوم بتحديد درجة أهمية كل مصدر من هذه المصادر.
- 3.نقوم بتحديد أي تهديدات أمنية على كل مصدر من هذه المصادر .
- 4.تطوير إستراتيجية خاصة يمكن من خلالها التعامل مع مثل هذه الثغرات التي تم إكتشافها.
- 5.تعريف وتطبيق بعض الأمور الخاصة لتقليل من أثر هذه الثغرات

* إذا تم إكتشاف أي ثغرات أمنية من خلال عملية تقييم الثغرات فهناك الحاجة لتقديم هذه الثغرات وبياناتها لجهة محددة سواء كان شخص أو منظمة هذه الجهة تسمى CERT

CERT : COMPUTER EMERGENCY READINESS TEAM

هناك العديد من أنواع تقييم الثغرات TYPES OF VULNERABILITY ASSESSMENT

1.ACTIVE ASSESSMENT

إستخدام بعض الأدوات أي أدوات الفحص network scanners عبر الشبكة لتحديد الثغرات الموجودة في الشبكة لتحديد ماهي الأجهزة الموجودة في الشبكة وماهي أنظمة التشغيل والخدمات الموجودة وتحديد الثغرات.

2.PASSIVE ASSESSMENT

عبارة عن عملية تنصت على الشبكة للبيانات المتراصلة عبر الشبكة لمعرفة ماهي الأنظمة الفعالة حالياً والخدمات التي يتم التعامل معها داخل الشبكة والثغرات التي يمكن أن تتوفر وايضاً معرفة الأنظمة والتطبيقات .

3.HOST-BASED ASSESSMENT

عبارة عن وجود سيرفر معين أو جهاز معين يتم تنصيب وتثبيت برنامج معين عليه يقوم هذا البرنامج بفحص الجهاز من أي ثغرات مختلفة ومن الامثلة على البرامج المستخدمة

MICROSOFT BASELINE SECURITY ANALYZER OR MICROSOFT BASELINE ANALYZER.

4.INTERNAL ASSESSMENT

أي عمل فحص داخل البيئة الداخلية للشركة أو المنظمة.

5.EXTERNAL ASSESSMENT

محاولة إيجاد أي ثغرة من خارج الشركة أو المنظمة ومحاولة فحصها من الخارج عبر الإنترنت ومحاولة إيجاد ثغرات أمنية داخلها.

6.APPLICATION ASSESSMENT

فحص التطبيقات المختلفة سواءاً كانت تطبيقات الويب أو غيرها داخل الشركة أو المنظمة المراد عمل فحص لها من الثغرات الأمنية وإكتشاف هذه الثغرات .

7.NETWORK ASSESSMENT

المقصود بها تحديد جميع الهجمات والثغرات من الممكن أن يتم شنها داخل الشبكة الخاصة للمنظمة أو الشركة.

8.WIRELESS NETWORK ASSESSMENT

هو تحديد جميع الهجمات والثغرات الموجودة في الشبكة اللاسلكية الخاصة في المنظمة .

أي نوع من انواع VULNERABILITY ASSESSMENT يمر بمجموعة خطوات او مراحل

- ACQUISITION الإستيلاء

في هذه المرحلة يتم مراجعة أي تقارير سابقة وأي ثغرات سابقة تم إكتشافها وتحديد بعض الأمور الخاصة بالقوانين والمخطط المتبع داخل الشركة وغيرها من الأمور المختلفة .

- IDENTIFICATION عملية التهديد

يتم من خلالها إجراء بعض المقابلات مع الموظفين والزبائن الموجودين بالشركة ويتم من خلالها جمع المعلومات التقنية حول جميع المصادر والأجهزة الموجودة داخل الشبكة .

- ANALYZING تحليل

يتم من خلالها مراجعة أي مقابلة من المقابلات التي تم إجراؤها في المرحلة السابقة بعد ذلك يتم تحليل النتائج ويتم عمل تحديد الثغرات من خلال الفحص.

- EVALUATION تقييم

يتم من خلالها تحديد الثغرات وتحديد مدى إمكانية إستغلال الثغرات التي تم إكتشافها من قبل المخترقين وتحديد التحديثات المراد تنفيذها .

- REPORTING كتابة التقرير

يتم من خلاله تحديد جميع الأمور التي تم إكتشافها وتحديد التحديثات الأمنية التي يجب إجراؤها والتعديل على هذه الإجراءات الأمنية المتبعة ومدى إمكانية إختراق هذه الأنظمة من قبل المخترقين وغيرها من الأمور.

• VULNERABILITY RESEARCH

عبارة عن عملية يتم خلالها تحديد أو التعرف على الثغرات الأمنية في التقييمات المختلفة سواءاً كانت هذه التقييمات أنظمة تشغيل أو الشبكات أو غيرها .
في هذه العملية يمكن أن يتم عمل مايسمى بالهندسة العكسية REVERSE ENGINEERING
ويمكن تحليل الكود البرمجي CODE ANALYSIS و STATIC ANALYSIS

يتم تصنيف أي ثغرة أمنية إلى تصنيفين VULNERABILITIES CLASSIFIED BASED ON

- SEVERITY LEVEL (LOW-MEDIUM-HIGH)

درجة خطورة الثغرة سواء كانت منخفضة او متوسطة او عالية

- EXPLOIT RANGE (LOCAL OR REMOTE)

أي استخدام الكود البرمجي المراد تنفيذه داخل النظام نفسه أو عن بعد.

PENETRATION TESTING إختبار الإختراق

عبارة عن عملية يتم من خلالها تمثيل ومحاكاة لعملية إختراق لأي نظام كمبيوتر وذلك لمحاولة إكتشاف الثغرات الموجودة فيه ومحاولة إستغلال لهذه الثغرات والوصول لصلاحيات داخل هذه الأنظمة طبعاً لسد هذه الثغرات.

PENETRATION TESTING أنواع

- WHITE BOX , BLACK BOX , GRAY BOX

- WHITE BOX

إن مختبر الإختراق سيكون لديه معرفة كاملة بجميع الأمور الموجودة داخل الجهة المراد إختبار إختراقها سواء من أنظمة الحماية وأجهزة الشبكات والإجراءات الأمنية المتبقية وأنظمة التشغيل والخدمات المتوفرة ومواقع الويب وغيرها.

- BLACK BOX

إن الشخص أو الجهة التي تقوم بإجراء عملية إختبار الإختراق لا تعلم أي شيء حول البنية التحتية والأنظمة في الجهة المراد إختبار إختراقها.

-GRAY BOX

ان الشخص أو الجهة التي ستقوم بعملية إختبار الإختراق لديها معلومات قليلة ومحددة حول الجهة المراد إختبار إختراقها وليست معلومات تفصيلية.

عملية إختبار الإختراق PENETRATION TESTING تساعد أي جهة لحماية نفسها من أي ثغرات أمنية ولذلك لتطبيق أي إجراءات أمنية لحماية هذه الشركة بالإضافة لفحص أنظمة الحماية بالشركة.

*بعد عملية إنهاء إختيار الإختراق يجب على الشخص الذي يقوم بعملية الإختيار أن يقدم تقرير كامل للجهة التي كلفته لعمل الإختيار من أجل حل المشاكل الأمنية المختلفة .

بعض المصطلحات الهامة

-SECURITY AUDIT(التدقيق الأمني)

فحص إذا كانت الجهة تتبع المعايير المختلفة داخل هذه الشركة مثل الايزوو وغيرها من المعايير المختلفة .

-VULNERABILITY ASSESSMENT(تقييم الضعف)

تحديد واستكشاف الثغرات الأمنية في انظمة الكمبيوتر المختلفة ولكن بدون اعطاء الجهة ان هذه الثغرات يمكن استغلالها.

-PENETRATION TESTING(إختبار الإختراق)

عبارة عن عملية دمج لكن من المصطلحين السابقين وذلك لتقديم تقرير شامل للشركة في عملية الثغرات التي تم إكتشافها وإثبات بأن هذه الثغرات تم إستغلالها بشكل صحيح.

مراحل أساسية تمر بها أي عملية إختبار الإختراق وهي ثلاثة مراحل

-PRE-ATTACK(مرحلة ما قبل الإختراق)

هي يتم من خلالها تخطيط وتحضير لعملية الإختراق أو الهجمة وتحديد المنهجية التي يتم إتباعها وجمع المعلومات حول الشبكة والأنظمة المراد إختراقها.

-ATTACK PHASE(مرحلة الإختراق)

يتم من خلالها مهاجمة الشبكة والإستحواذ على الأجهزة والسيطرة عليها ورفع الصلاحيات وتنفيذ بعض البرامج من أجل المحافظة على الوصول للأنظمة مثل الباك دور .

-POST-ATTACK PHASE(مرحلة ما بعد الهجوم)

هي عملية كتابة التقارير وتنظيف أي عملية إختراق التي تمت من أجل محو أي أمر تم إستغلاله حتى لا تهدد الشركة التي قمت في إختبارها.

مجموعة من المنهجيات الخاصة PENETRATION TESTING

المنهجية: عبارة عن مجموعة من الخطوات والمراحل التي يتم إتباعها في أي عملية إختبار الإختراق لكشف الثغرات الأمنية والتحقق منها موجودة فعلياً ام لا .

OWASP

هي عبارة عن منظمة تقوم بوضع منهجيات خاصة لإختبار المواقع الإلكترونية أو التطبيقات الخاصة بالويب بالإضافة إلى إختبار إختراق تطبيقات الأجهزة الذكية .

بعض المصطلحات الهامة في أمن المعلومات والهكر الأخلاقي

Information Assurance

عبارة عن مصطلح يهدف إلى عملية التأكد من أن البيانات وأنظمة البيانات والمعلومات محمية أثناء عملية تخزينها وإستخدامها ومعالجة داخلها وتراسل البيانات داخلها وبيت ذلك عبر العديد من الأمور المختلفة مثل وضع سياسات خاصة لمعالجة البيانات وضع إستراتيجيات خاصة للتحقق من المستخدمين داخل الشبكة وعمل تقييم الثغرات وتقليل من التهديدات الأمنية وتدريب الموظفين الذين يعملون في الأمور القنية.

Threat Modeling

هو مصطلح وعبرة عن عملية يتم من خلالها تحليل أمن لأي نظام أو أي تطبيق أو برنامج وذلك عن طريق التقاط وتحليل البيانات التي يمكن أن تؤثر على أمن المعلومات عن طريق عدة خطوات .

Enterprise Information Security Archctecture(EISA)

عبرة عن مجموعة من المتطلبات والعمليات التي تهدف لتحديد هيكلية وعمل أي نظام معلوماتي هدفها تقليل تسريب المعلومات داخل الشركة ومراقبة الشبكة والأنظمة .

Network Security Zoning

يتم من خلاله تقسيم وإدارة الشبكة داخل الشركة والشبكة تحتوي على خوادم وخدمات وأنظمة وتطبيقات وأجهزة وتسمى zoning الهدف منها حماية ومراقبة البيانات من اي جهاز داخل أو خارج الشبكة.

DMCA(Digital Millennium Copy Right Act)

هو معيار خاص لحماية حقوق الملكية في أمريكا اي له علاقة في حماية حقوق الفكرية

FISMA(Federal Information Security Management Act)

هو معيار من قوانين الأمن الإلكتروني وهو قانون إدارة أمن المعلومات الفيدرالي.

بعض البرامج المستخدمة في أمن المعلومات والشبكات

يوجد نوعين من الحماية فيزيائي و برمجي او اجهزة حماية

Physical Security

يجب ان تتوفر في الشركة العديد من الامور مثلاً تتوفر بوابات إلكترونية وأي موظف داخل المؤسسة يجب أن يكون معه بطاقة من أجل الدخول للتحقق من أي شخصية أو بصمة مثل بصمة الأصبع او العين ووضع ايضاً كميرات مراقبة للتأكد من الأشخاص الداخليين والخارجيين والبوابات الخاصة في غرف البيانات المركزية وغيرها من امور الحماية

مصطلح إدارة الحوادث الأمنية : عبارة عن مجموعة من العمليات التي تحد وتحلل وتصف وتقوم بحل أي حوادث أمنية حدثت داخل الشركة مثلاً في حال حدوث عملية إختراق يجب تحليلها من ناحية قبل عملية الإختراق وبعد عملية الإختراق.

القوانين والمعايير الخاصة في امن المعلومات Information Security And Stanards

المعيار : هو مجموعة من الخطوات والأمور التي يجب أن يتم تطبيقها للحصول على أمر معين – مثل معيار الأيزو اي يطبق ضمن خطوات وفي حال مؤسسة ينطبق عليها هذه الخطوات تأخذ المعيار.

ويوجد معيار كثيرة مثل معيار حماية المعلومات وادارة امن المعلومات ومعيار الامور المالية وغيرها .

الجدار الناري (جدار الحماية) FIREWALL

ماهو الجدار الناري ؟

الجدار الناري هو نظام صمم لمنع الوصول غير المصرح به إلى شبكة خاصة ، وذلك عن طريق تصفية المعلومات القادمة من الإنترنت ، الجدار الناري يمنع حركة مرور البيانات غير المرغوب فيها ، ويسمح بدخول حركة المرور المصرح لها.

يقوم الجدار الناري بعمل عازل أمني بين الشبكة الخاصة والشبكة العامة (الإنترنت)، فمن الإنترنت يمكن ان يصل مخترقين إلى الشبكة الخاصة.

الجدار الناري مهم جدا بالنسبة للشركات والمؤسسات الكبيرة التي تحوي على عدد كبير من أجهزة الكمبيوتر والخوادم التي تكون حساسة جدا بالنسبة للشركة ، فلا يجب دخول ان كان إلى شبكة المؤسسة بدون تصريح .

جاء إسم الجدار الناري من إسم الحاجز الذي يوضع في المنشآت والمسمى بالجدار الناري ، فمبدأ عمله مشابه لمبدأ عمل الجدار الناري في الشبكات ، فالجدار الناري في المؤسسات يوفر عازلاً في حال اندلاع حريق في جزء من المبنى بحيث يمنع إنتشار الحريق إلى باقي أجزاء المبنى ، في حال عدم وجوده سينتشر الحريق إلى باقي أجزاء المبنى.

يعمل الجدار الناري عن طريق فلترة كل حركة المرور الداخلة إلى الشبكة حسب القواعد المعدة ضمن الجدار الناري (تعرف هذه القواعد بقائمة التحكم بالوصول access control list) هذه القواعد قابلة للتعديل والمسؤول عنها هو مدير النظام ، لمدير النظام أيضاً تحديد القواعد التي تحكم ليس فقط حركة المرور الداخلة ولكن أيضاً حركة المرور الخارجية .
قواعد جدار الحماية لا تستند فقط إلى عناوين الـip، ولكن أيضاً أسماء المجالات ، البروتوكولات ، البرامج ، المنافذ وأيضاً الكلمات المفتاحية .

جدار الحماية : هو نظام أمان الشبكة يقوم بمراقبة حركة المرور الشبكة الواردة والصادرة والتحكم فيها بناءً على قواعد الأمان المحددة مسبقاً. يؤسس جدار الحماية عادة حاجزاً بين شبكة داخلية موثوقة وشبكة خارجية غير موثوق بها مثل الإنترنت .









غالباً ما يتم تصنيف جدران الحماية على انها جدران **حماية للشبكة** أو جدران **حماية قائمة على المضيف** . تقوم جدران الحماية للشبكة بتصفية حركة المرور بين شبكتين أو أكثر وتشغيلها على أجهزة الشبكة . تعمل جدران الحماية للشبكة المستندة إلى المضيف على أجهزة الكمبيوتر المضيفة وتتحكم في حركة مرور الشبكة داخل وخارج هذه الأجهزة.

جدار الحماية في الوندوز Windows Firewall










في windows 10 & windows 11 لم يتغير جدار الحماية كثيراً منذ نظام التشغيل في Vista بشكل عام ، يتم حظر الإتصالات الواردة إلى البرامج مالم تكن مدرجة في القائمة المسموح بها . لا يتم حظر الإتصالات الصادرة إذا لم تتطابق مع قادة . لديك أيضاً ملف تعريف شبكة عام وخاص لجدار الحماية ويمكنك التحكم بالضبط في البرنامج الذي يمكنه الإتصال على الشبكة الخاصة بدلاً من الإنترنت .
على الرغم من عدم حظر الإتصالات الصادرة إفتراضياً ، يمكنك تكوين قواعد جدار الحماية الخاصة بك في نظام التشغيل windows ، يمكنك إما فتح لوحة التحكم وفتح جدار الحماية من هناك أو يمكنك النقر فوق ابدأ وكتابة كلمة firewall.

Adjust your computer's settings

View by: Category

-  **System and Security**
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
-  **Network and Internet**
View network status and tasks
-  **Hardware and Sound**
View devices and printers
Add a device
Adjust commonly used mobility settings
-  **Programs**
Uninstall a program
-  **User Accounts**
Change account type
-  **Appearance and Personalization**
-  **Clock and Region**
Change date, time, or number formats
-  **Ease of Access**
Let Windows suggest settings
Optimize visual display

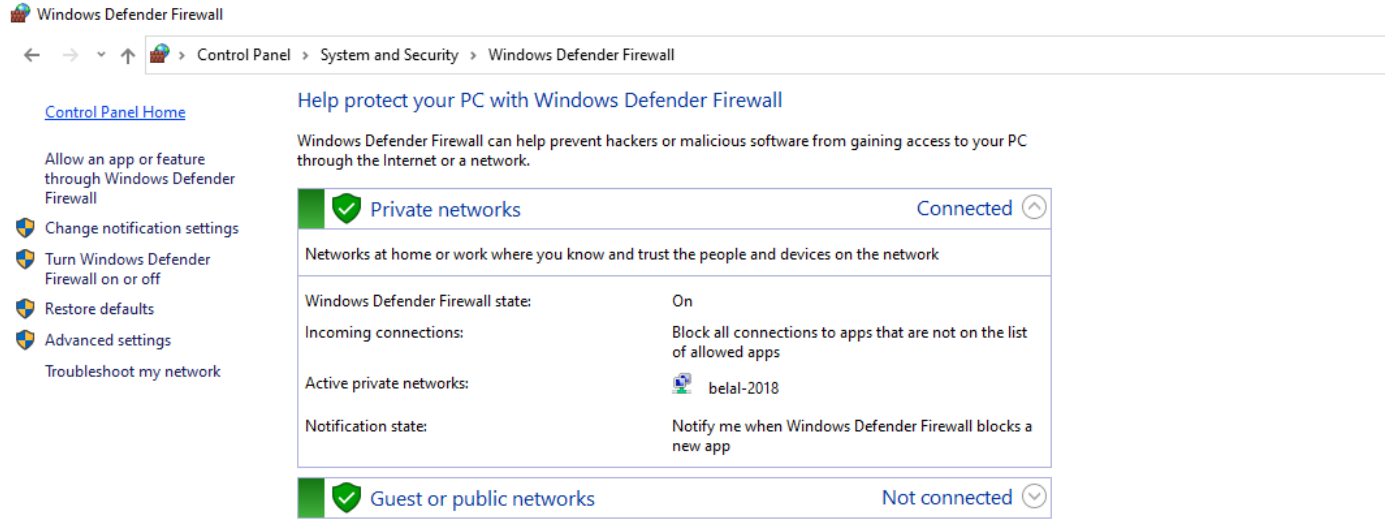
Best match

-  **Windows Firewall**
Control panel
-  **Windows Firewall with Advanced Security**
Desktop app
- Settings**
-  **Check firewall status**
-  **Allow an app through Windows Firewall**
- Web**
-  **firewall**
-  **firewall movie**
-  **firewall settings**
-  **firewall protection**
- Store**
-  **Windows8FirewallPanel**

My stuff Web

firewall

سيؤدي ذلك إلى إظهار مربع حوار جدار حماية windows حيث يمكنك التحكم في جميع الإعدادات المختلفة لجدار الحماية .

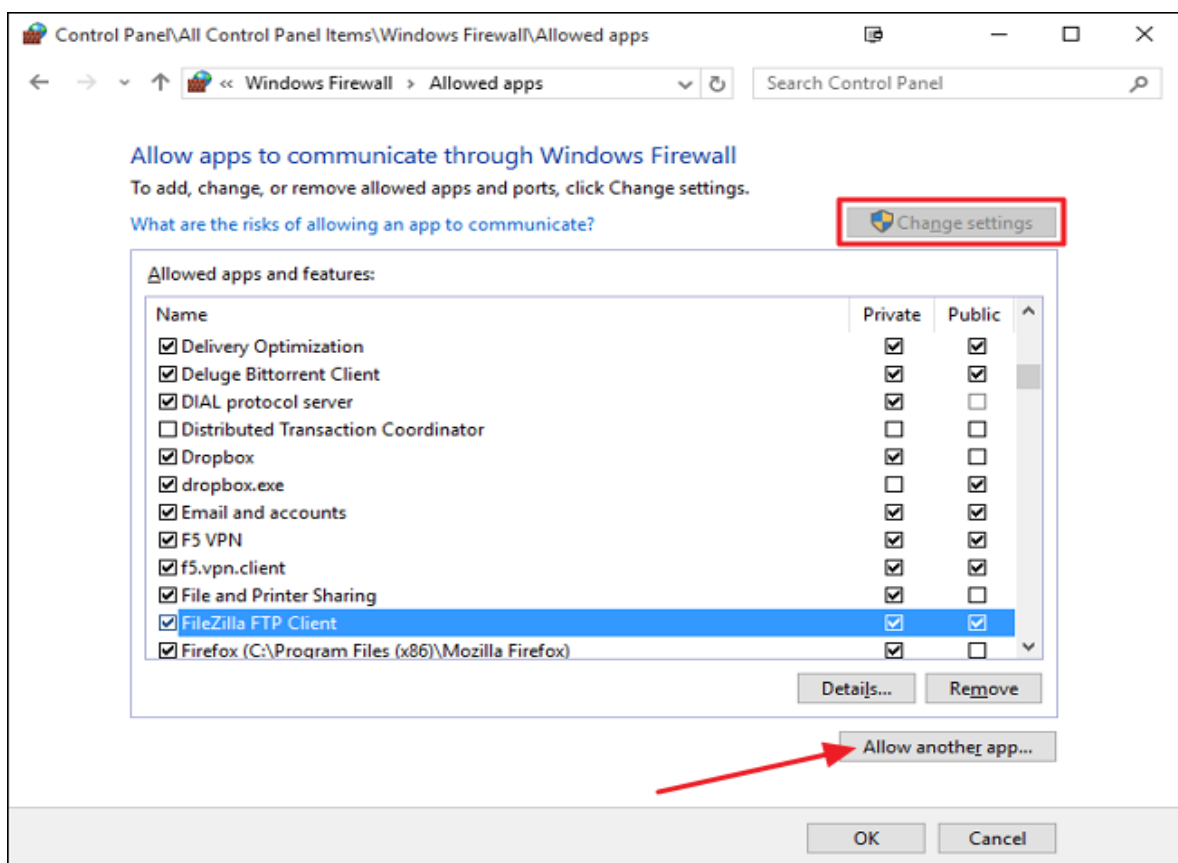
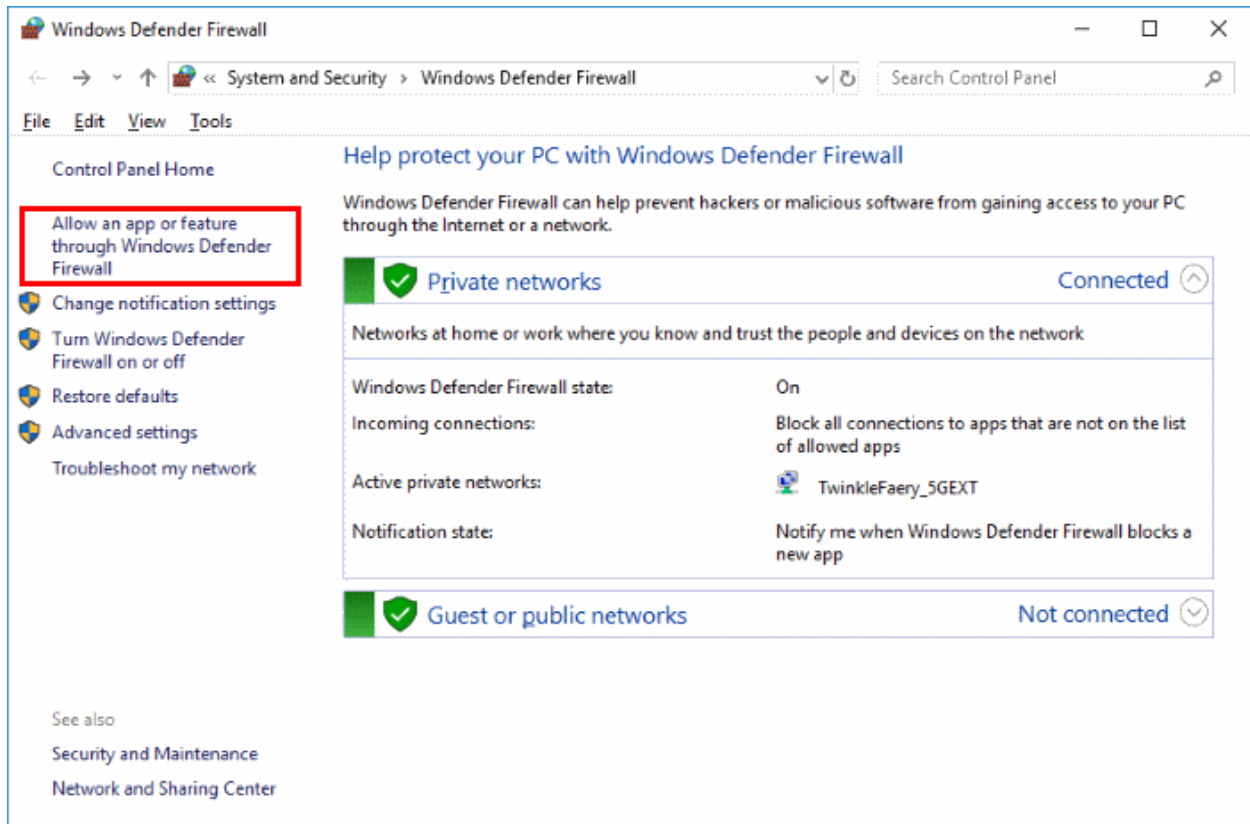


على الجانب الأيمن ، يقسم العرض إلى شبكات خاصة وضيء أو شبكات عامة . يجب أن تظهر شبكتك اللاسلكية المنزلية ضمن الشبكات الخاصة ، ولكن إذا لم يحدث ذلك ، فربما يتعين عليك إخبارها يدوياً أن الشبكة هي شبكة منزلية وليست شبكة عامة.

السماح للبرامج من خلال جدار الحماية

السبب الرئيسي الذي يجعل معظم الناس يعثون بجدار الحماية هو السماح لبرنامج ما بالعمل من خلال جدار الحماية ، عادة ما يتم ذلك تلقائياً بواسطة البرنامج نفسه ، ولكن في بعض الحالات ، عليك القيام بذلك يدوياً. يمكنك القيام بذلك عن طريق النقر فوق

Allow an app or feature through windows firewall

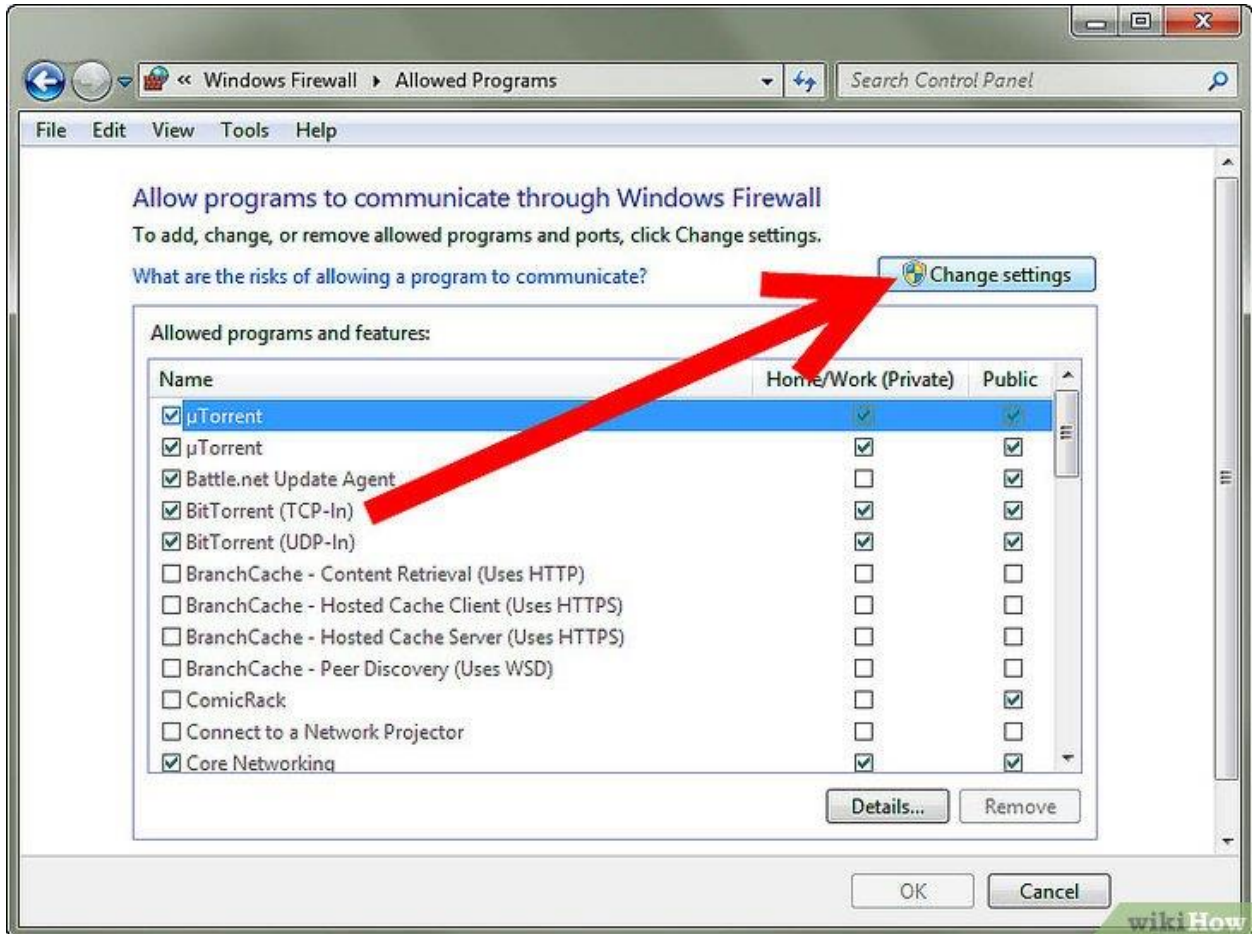


كما ترى بالنسبة لكل برنامج أو ميزة من ميزات windows، يمكنك إختيار السماح بالإتصالات الواردة على الشبكات الخاصة والعامة بشكل منفصل ، يعد هذا الفصل مفيداً لأشياء مثل مشاركة الملفات والطابعات ومجموعات المشاركة المنزلية نظراً لأننا لا نريد أن يتمكن شخص ما من شبكة wifi العامة من الأتصال بمشاركة شبكة أو مجموعة مشاركة منزلية محلية ، للسماح لأحد التطبيقات ، ما عليك سوى العثور عليه في القائمة ثم تحديد المربع الخاص بنوع الشبكة التي تريد السماح بالاتصالات الواردة عليها.

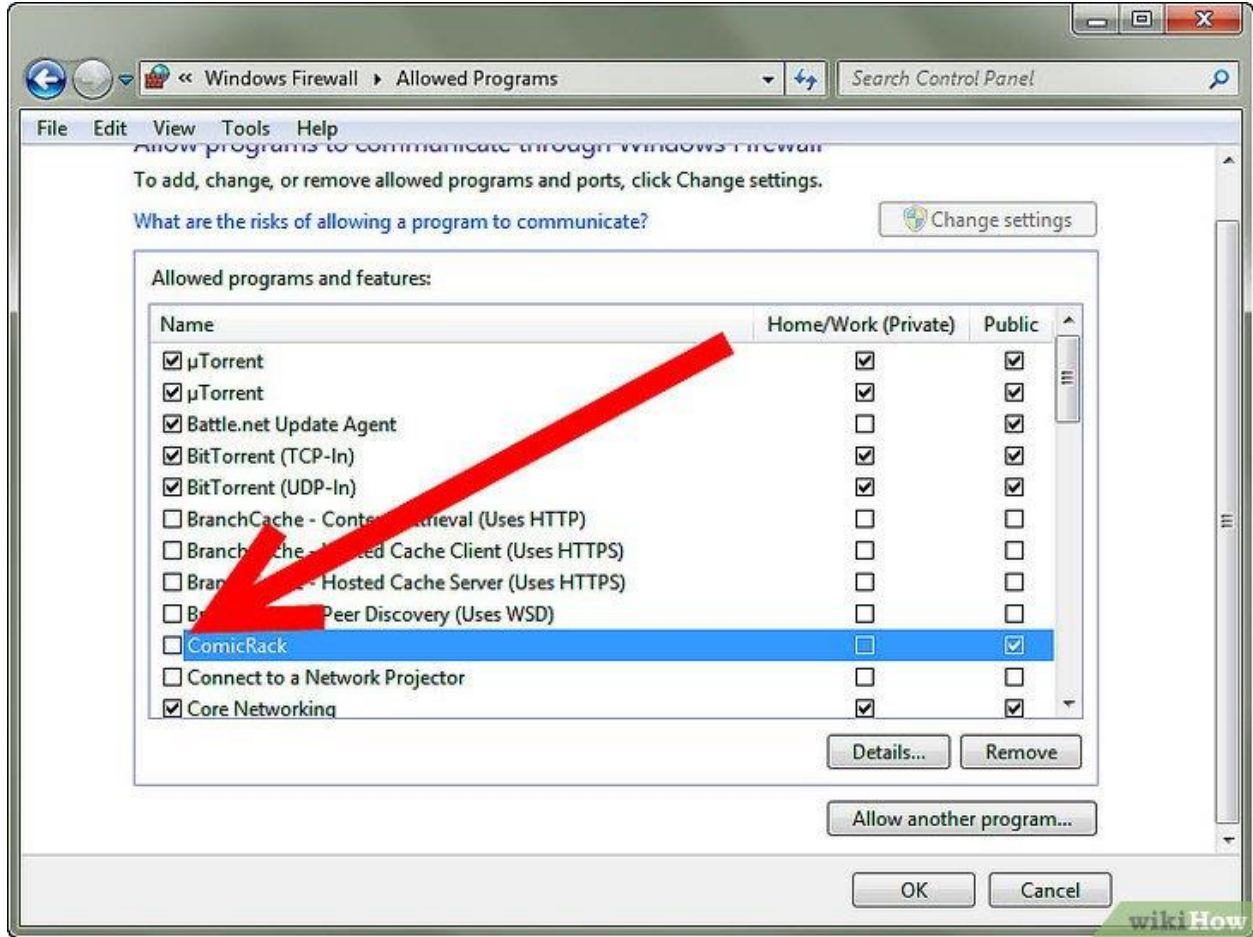
إذا لم يكن التطبيق مدرجاً ،فيمكنك النقر فوق الزر allow another app والأختيار من قائمة أو النقر فوق الزر browse للعثور على برنامجك تحديداً. إذا كان الزر غير نشط فانقر فوق change settings اولاً.

مثال : قم بحضر برنامج معين مثلاً برنامج comicRack؟

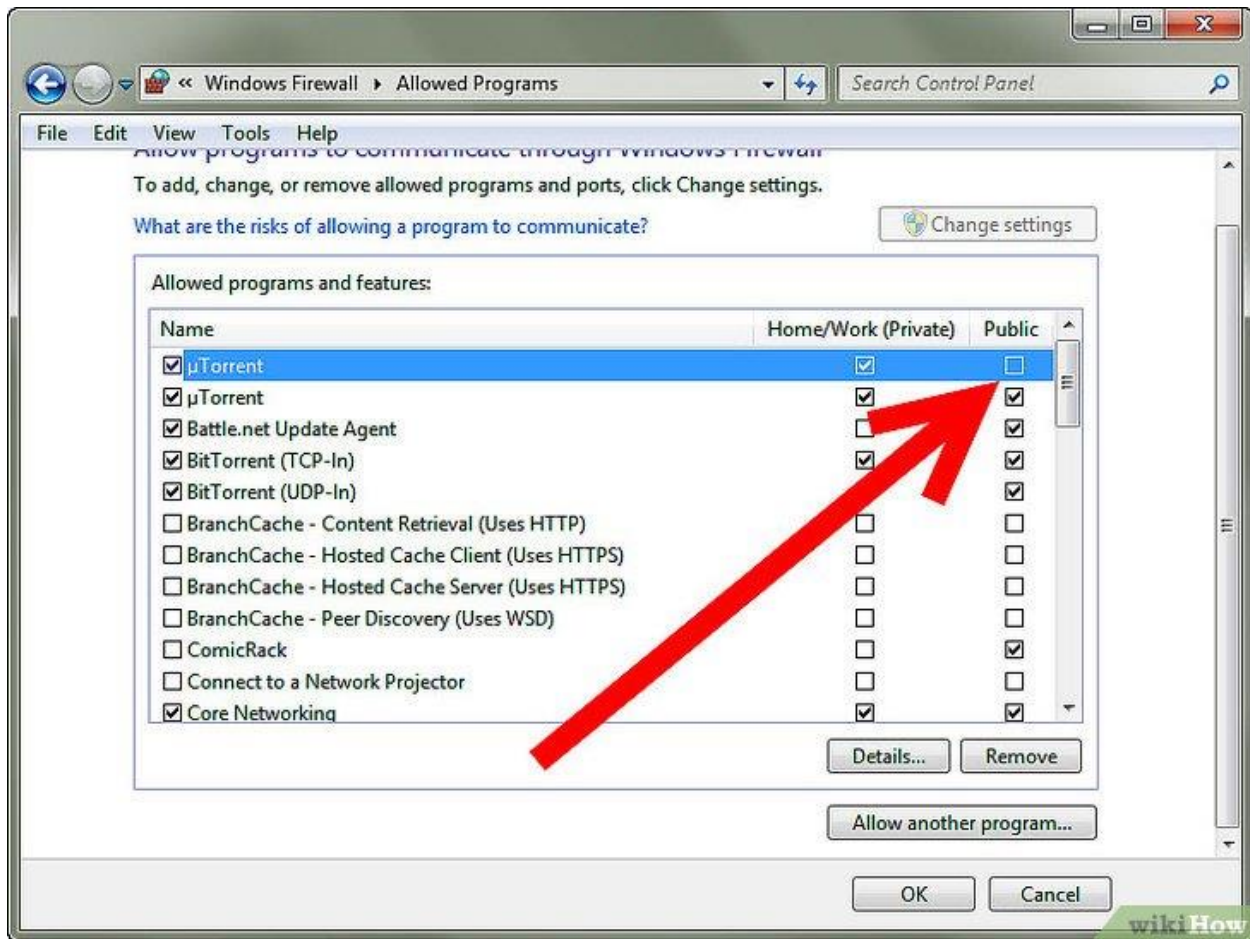
الحل : بعد فتح الجدار الناري نضغط على تغيير الإعدادات(Change settings)



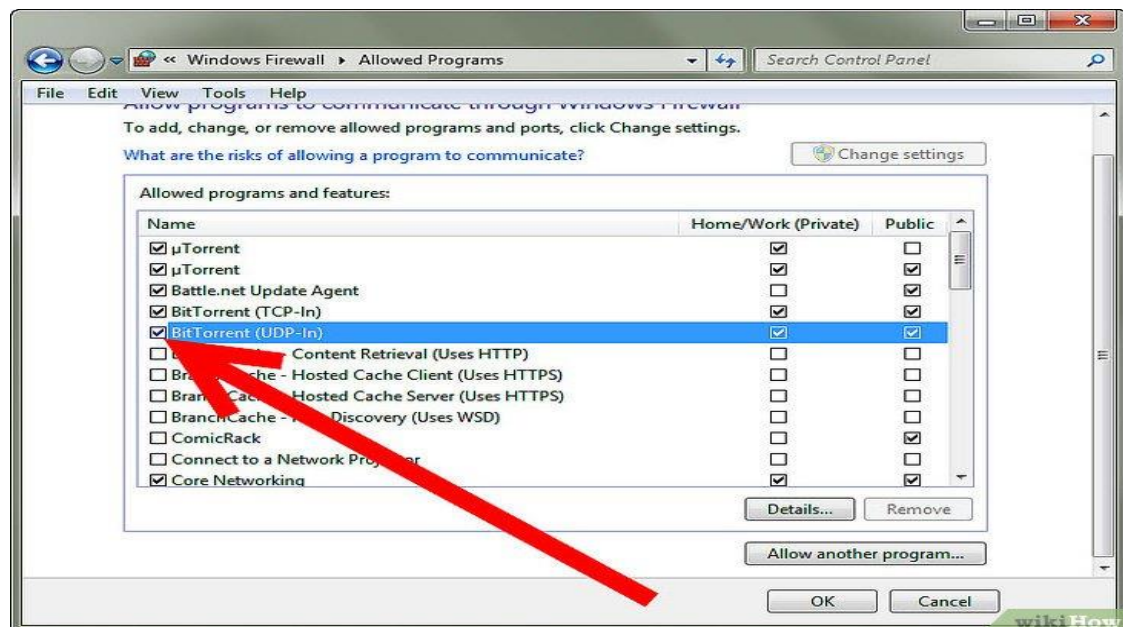
قم بإلغاء تحديد خانة البرنامج الذي تريد حظره. عندما تقوم بإلغاء تحديد الخانة، سوف يحظر جدار الحماية هذا البرنامج من خلال الاتصال بالإنترنت.



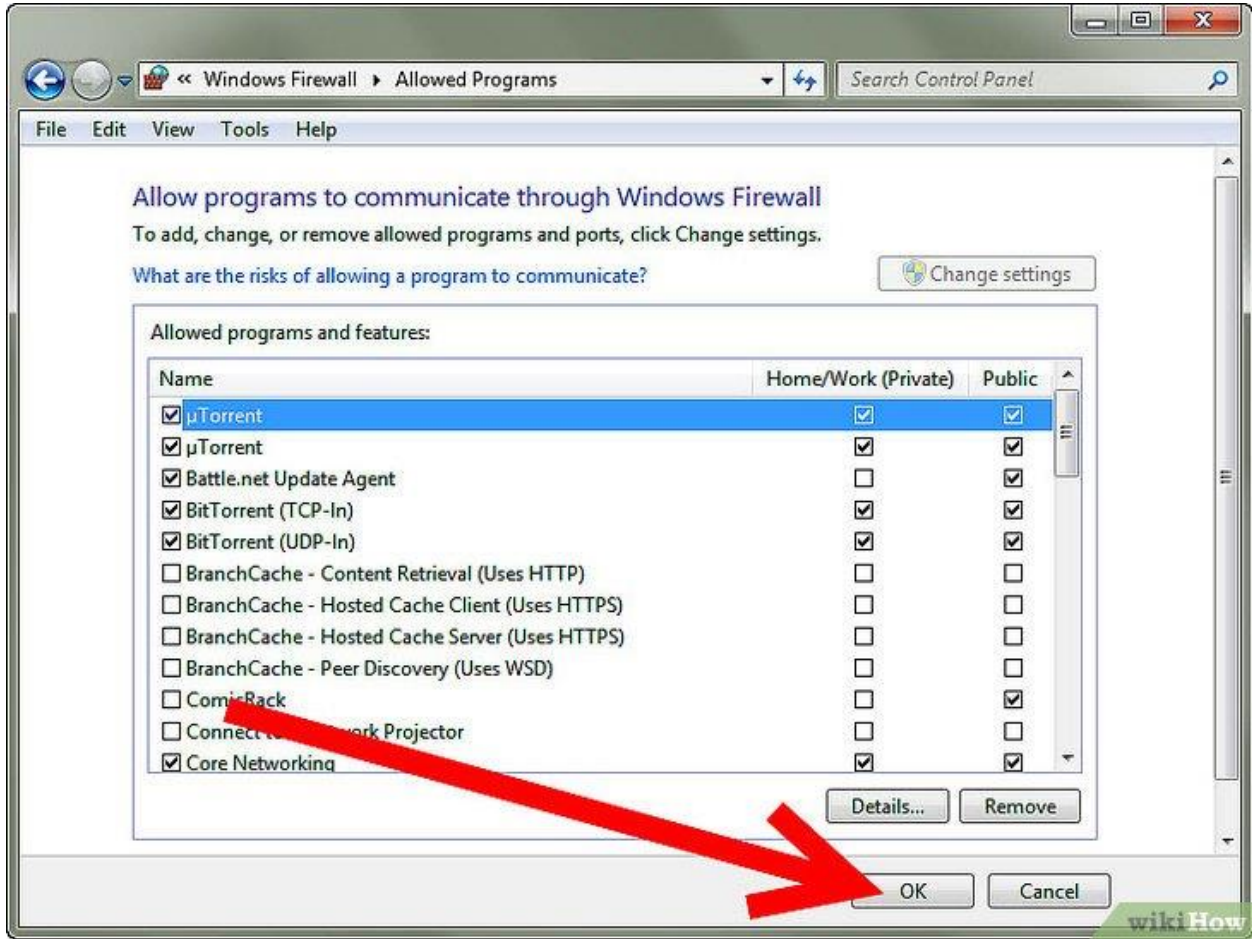
إذا كنت ترغب في حظر برنامج عند اتصاله بالشبكة العامة ورفع الحظر عند اتصاله بشبكة اتصال خاصة، أو العكس بالعكس، فقم بتحديد وإلغاء تحديد الخانات المناسبة على يمين قائمة البرنامج.



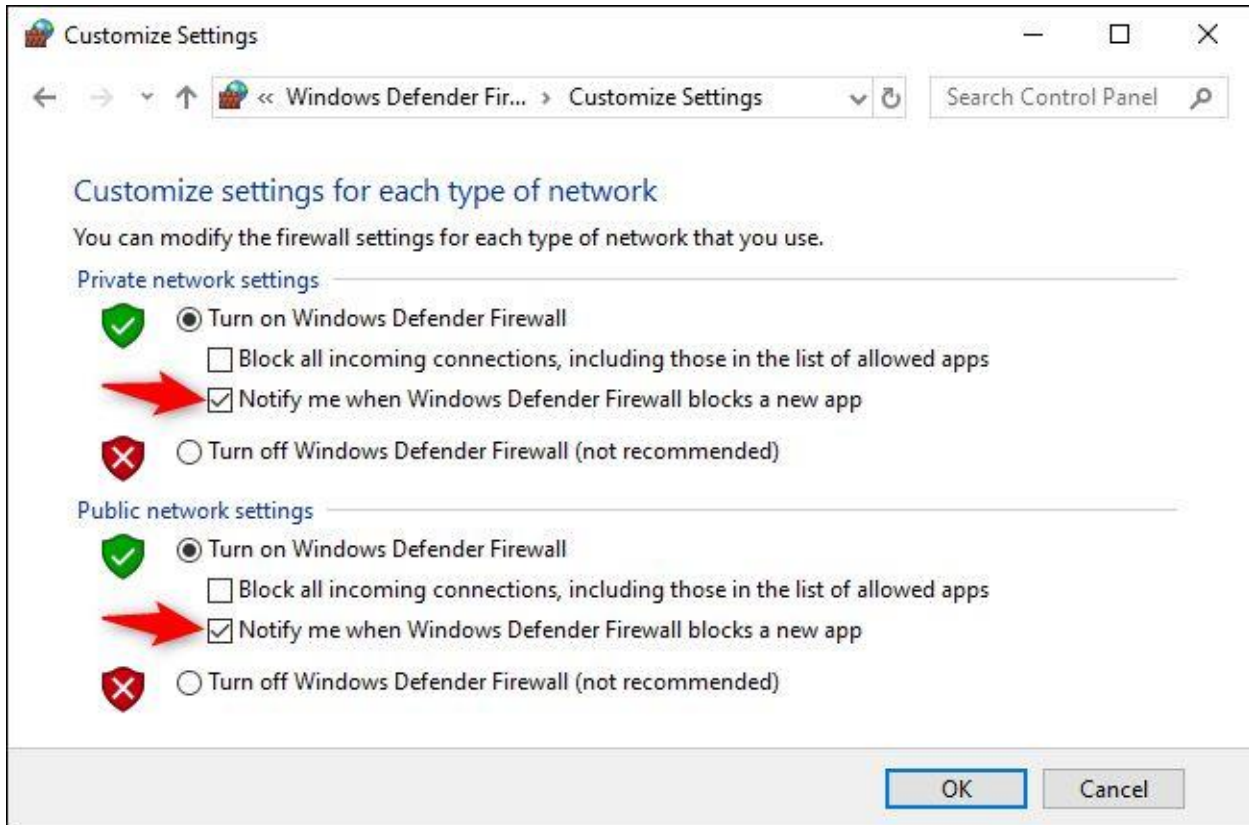
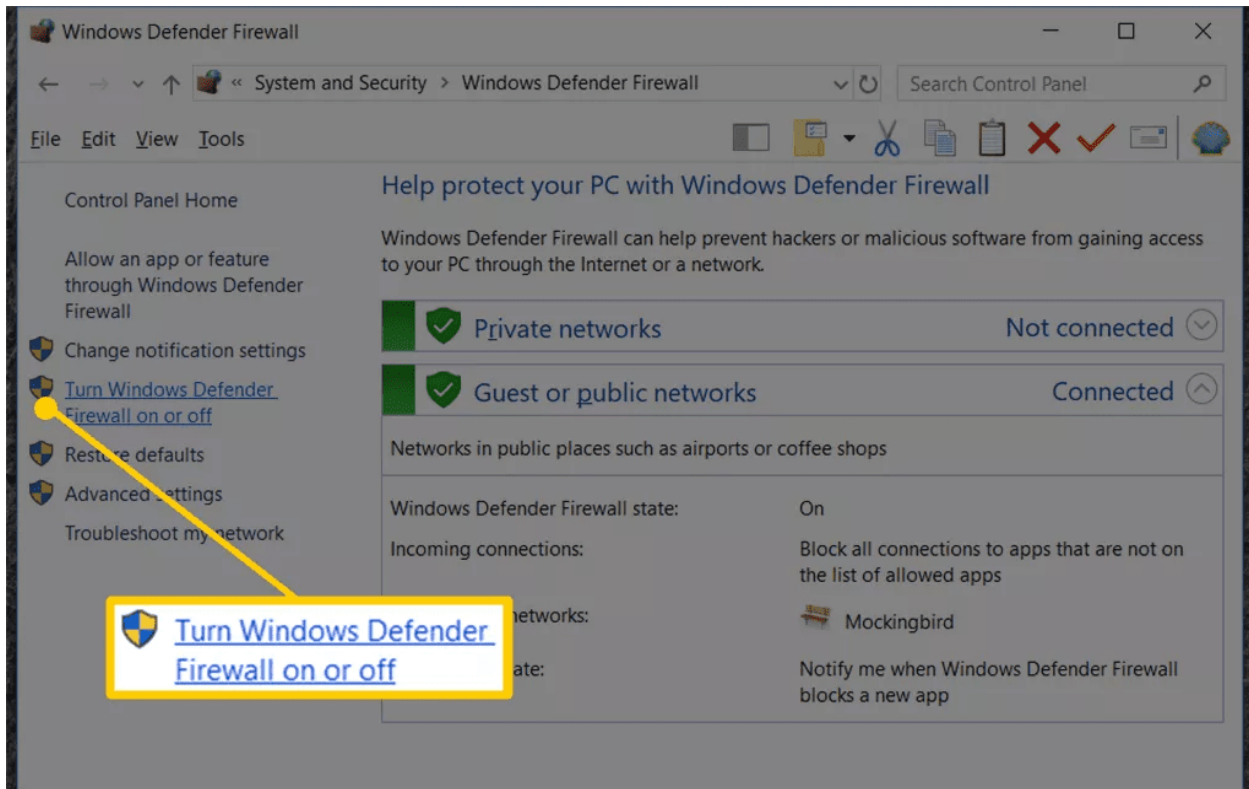
تحديد الخانات سوف يسمح للبرنامج بالاتصال بالإنترنت لذلك ينبغي السماح فقط بالبرامج التي تثق بها.



احفظ الإعدادات. بمجرد الانتهاء من إجراء التغييرات، انقر فوق زر موافق لحفظ إعدادات جدار الحماية.



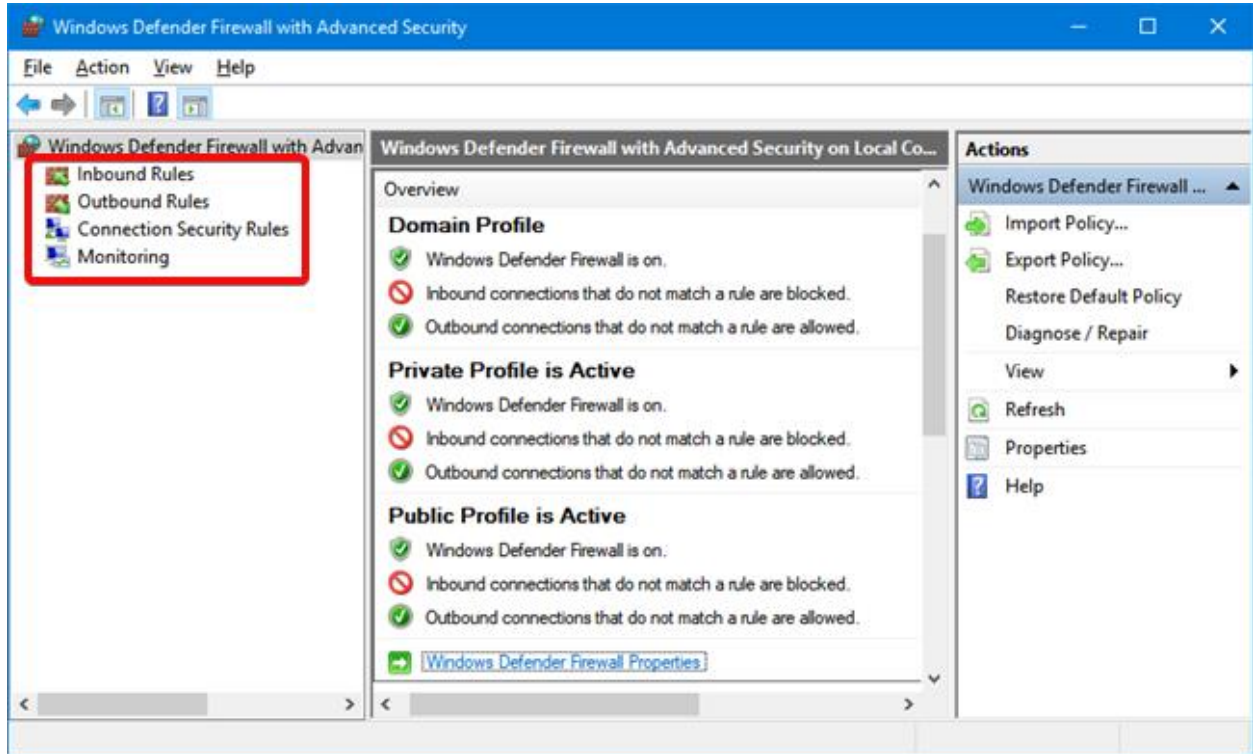
إذا عدت إلى مربع حوار جدار الحماية الرئيسي، فهناك رابط آخر في الجزء الأيمن يسمى Turn windows firewall on or off إذا قمت بالنقر فوق ذلك ، فستحصل على مجموعة من الخيارات كما هو موضح إدناه :



يمكنك إيقاف تشغيل جدار الحماية في نظام التشغيل Windows تماماً ، ولكن هذا سيسمح لكل شيء عبر جدار الحماية. يمكنك أيضاً حظر جميع الاتصالات الواردة إلى جهاز الكمبيوتر الخاص بك ، حتى بالنسبة للتطبيقات المسوح فيها ، وهو امر مفيد في مواقف معينة ، على سبيل المثال إذا كنت في مكان عام مثل فندق أو مطار وتريد أن تكون أكثر أماناً أثناء الإتصال بالشبكة لايزال بإمكانك تصفح الإنترنت باستخدام مستعرض ويب، ولكن لن يتمكن أي برنامج من إنشاء إتصال وارد من كمبيوتر آخر على الشبكة المحلية أو من خادم على الإنترنت.

الإعدادات المتقدمة

أنقر فوق الرابط advanced settings في الجزء الأيمن في مربع الحوار الرئيسي لجدار الحماية ، سيؤدي ذلك إلى إظهار نافذة Windows firewall with advanced security



على الشاشة الرئيسية ، نظرة عامة سريعة على إعدادات جدار الحماية الخاص بك للمجال والشبكات الخاصة والشبكات العامة إذا لم يكن جهاز الكمبيوتر الخاص بك منضمماً إلى مجال فلا داعي للقلق بشأن هذا الملف الشخصي ، يمكنك أن ترى بسرعة كيف تدار الاتصالات الواردة والصادرة بواسطة جدار الحماية إفتراضياً يسمح بجميع الاتصالات الصادرة إذا كنت ترغب في حظر إتصال خارجي ، نقوم ماييلي :

* نضغط على Outbound Rules في الجهة اليسرى ثم نضغط على New Rule
سيظهر لك مربع حوار يسأل عن نوع القاعدة
إذا ضغطنا على المنفذ port من أجل حظر جميع الإتصالات الصادرة على المنفذ 80
منفذ HTTP المستخدم من قبل كل متصفح ويب. من الناحية النظرية يجب أن يمنع هذا
الوصول إلى الإنترنت في المتصفح IE,Edge,Chrome والمتصفحات الأخرى
أنقر فوق التالي ، وحدد TCP واكتب رقم المنفذ.

New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

Program
Rule that controls connections for a program.

Port
Rule that controls connections for a TCP or UDP port.

Predefined:
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.

Custom
Custom rule.

< Back Next > Cancel

New Outbound Rule Wizard ×

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

TCP
 UDP

Does this rule apply to all remote ports or specific remote ports?

All remote ports
 Specific remote ports:

Example: 80, 443, 5000-5010

ثم نختار بعد الضغط على التالي الإجراء الذي نريده ولاننا نريد حظر الاتصال نضغط على

Block The Connection

New Outbound Rule Wizard ×

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

Allow the connection
This includes connections that are protected with IPsec as well as those are not.

Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

Block the connection

ثم نختار الملفات الشخصية التي نريد أن نطبق القاعدة عليها فنختار مثلاً الجميع:

New Outbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

Domain
Applies when a computer is connected to its corporate domain.

Private
Applies when a computer is connected to a private network location, such as a home or work place.

Public
Applies when a computer is connected to a public network location.

< Back Next > Cancel

في حال فتحنا المتصفح سيظهر رسالة خطأ اي تم تطبيق القاعدة بنجاح .

وإذا اردنا ان نطبقها على المنفذ UDP نكرر نفس الخطوات مع إختيار المنفذ.

نفس الفكرة في حال نريد التطبيق على الإتصالات الواردة Inbound Rules

في حال نريد حظر برنامج معين نختار بدل Port حظر برنامج وهي

Does this rule apply to all programs or a specific program?

All programs
Rule applies to all connections on the computer that match other rule properties.

This program path:

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

All programs اي كافة البرامج اما this program path نحن نحدد المسار وهكذا للبقية .

جدار الحماية في راوتر FortiGate

هذا الراوتر موجه للمؤسسات والشركات مثل راوتر جونيبر او سيسكو سنقوم بشرح الجدار الناري بهذا الراوتر لمعرفة كيف يمكن استخدام أمن المعلومات في المؤسسات ونترك لك عزيزي الدارس في التعمق ببقية الراوتر الموجودة .

ملاحظة : للتطبيق نقوم بتحميل نسخة الفيروول من موقع الانترنت وتنزيلها على النسخة workstation الوهميه اسم نسخة الفيروول :

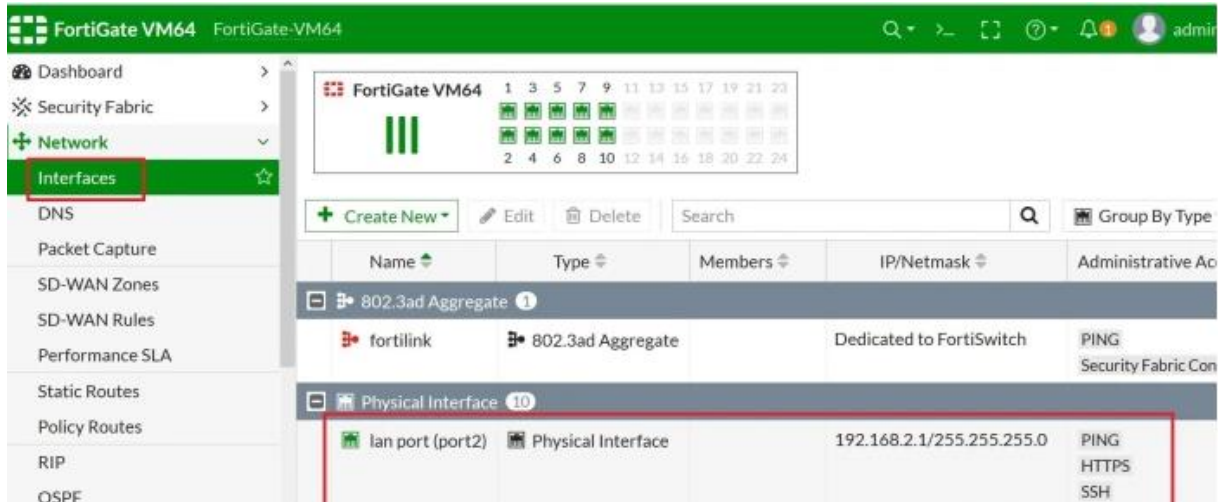
نقوم باختيار مكان fortigate vm والتي باسم FortiGate-VM64.ovf

او ممكن استخدام الموقع التالي للدخول على الراوتر :

<https://www.avfirewalls.com/Online-Demos.asp>

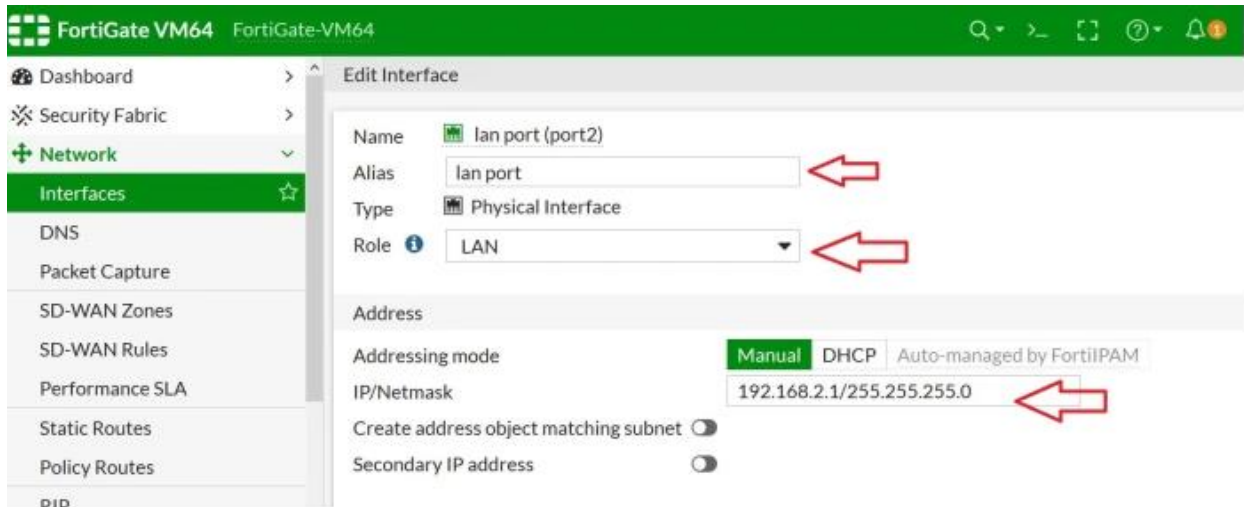
[https://fortigate.fortidemo.com/login?redir=%2Fng%2Fsystem%2Fdash
board%2F1](https://fortigate.fortidemo.com/login?redir=%2Fng%2Fsystem%2Fdashboard%2F1)

username: demo / password : demo

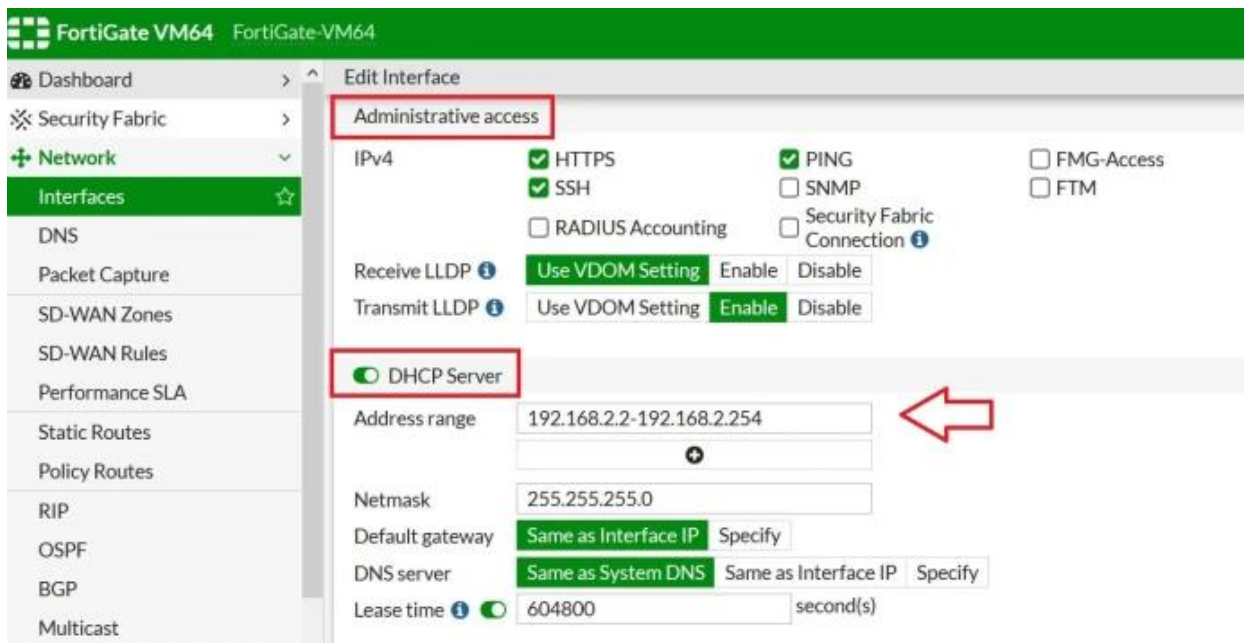


نختار منفذ lan port او Role:lan ونضع العنوان المنطقي التالي 192.168.1.170

والعبارة الافتراضية 255.255.255.0



في هذا السيناريو ، يتم توفير الوصول الإداري إلى PING و SSH و HTTPS
 تم تكوين خادم DHCP أيضًا (نطاق العنوان 192.168.2.2 – 192.168.2.254



WAN port configuration

تكوين wan الخطوات التالية :

To configure the WAN port go to

Network → *Interfaces*

Select the port you need to configure

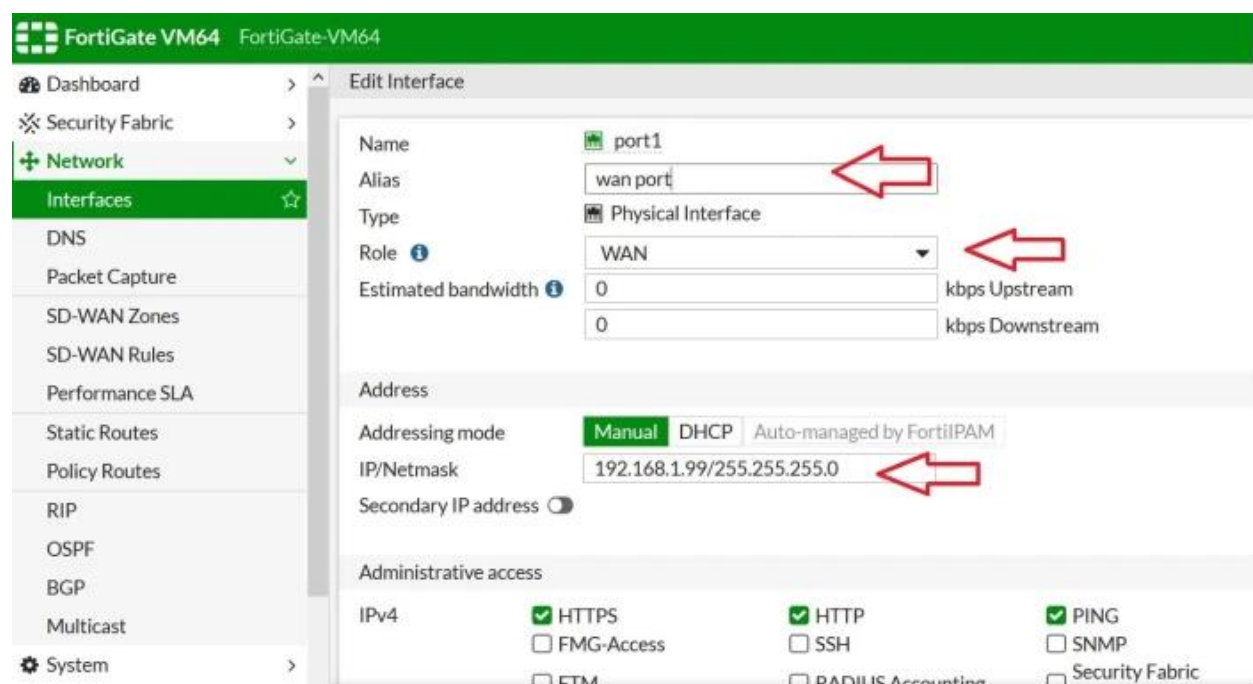
port 1

Provide the appropriate details

Alias: wan port

Role : WAN

IP address: 192.168.1.99 /255.255.255.0

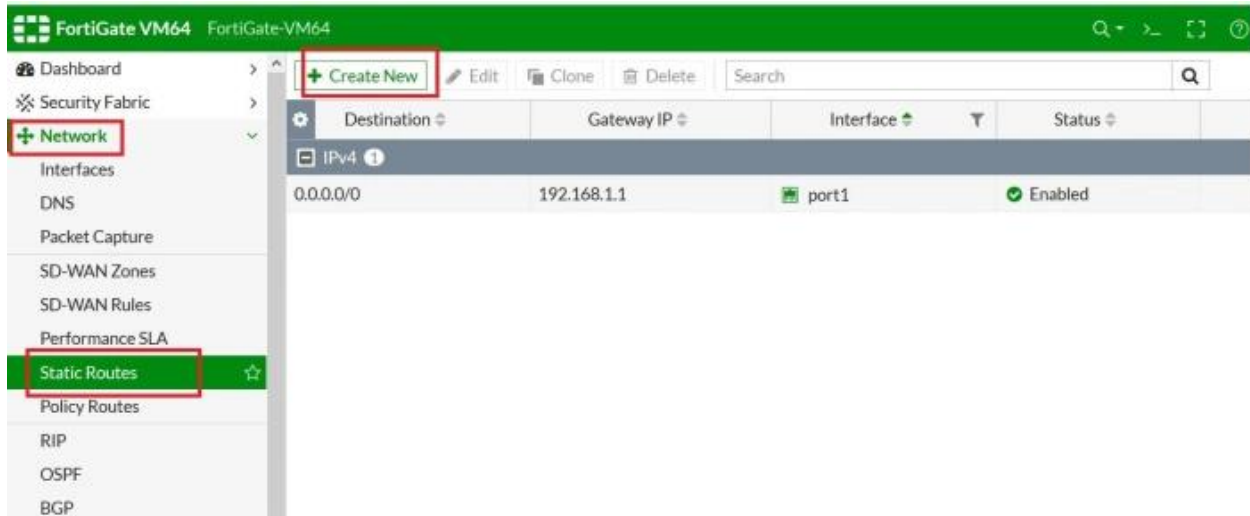


تكوين المسار الثابت

Static route configuration

To configure the **static route** go to

Network → Static Routes → Create New

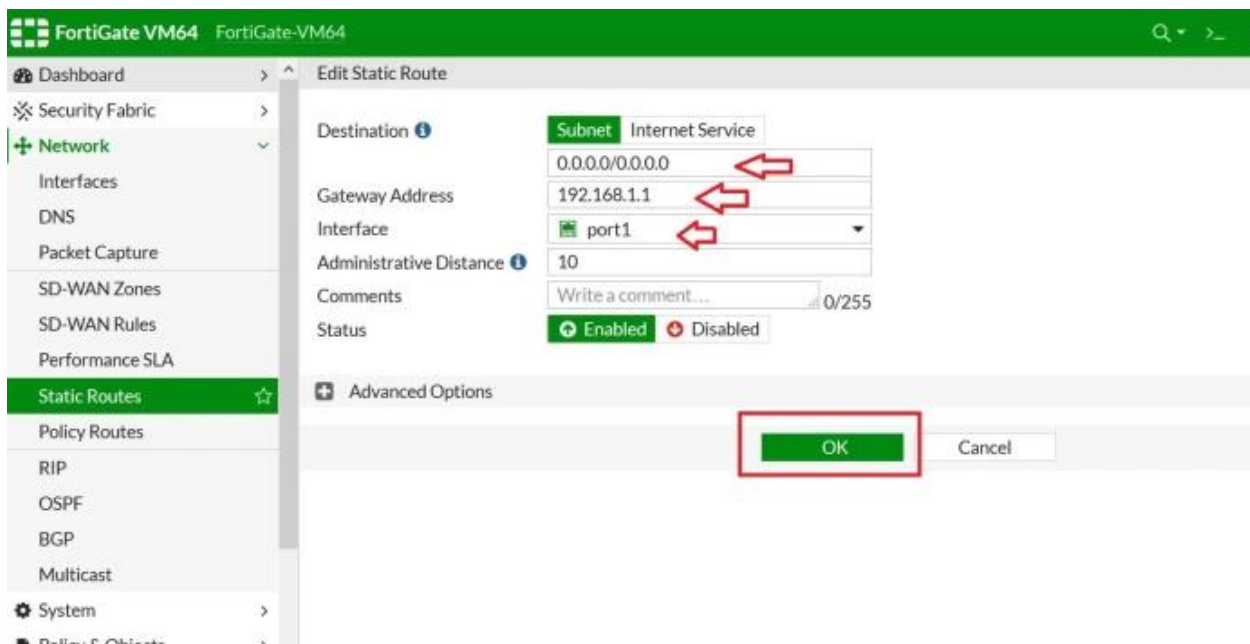


Provide the details

Subnet: 0.0.0.0/0.0.0.0

Gateway Address: 192.168.1.1

Interface: port1 (this is the previously configured WAN interface)

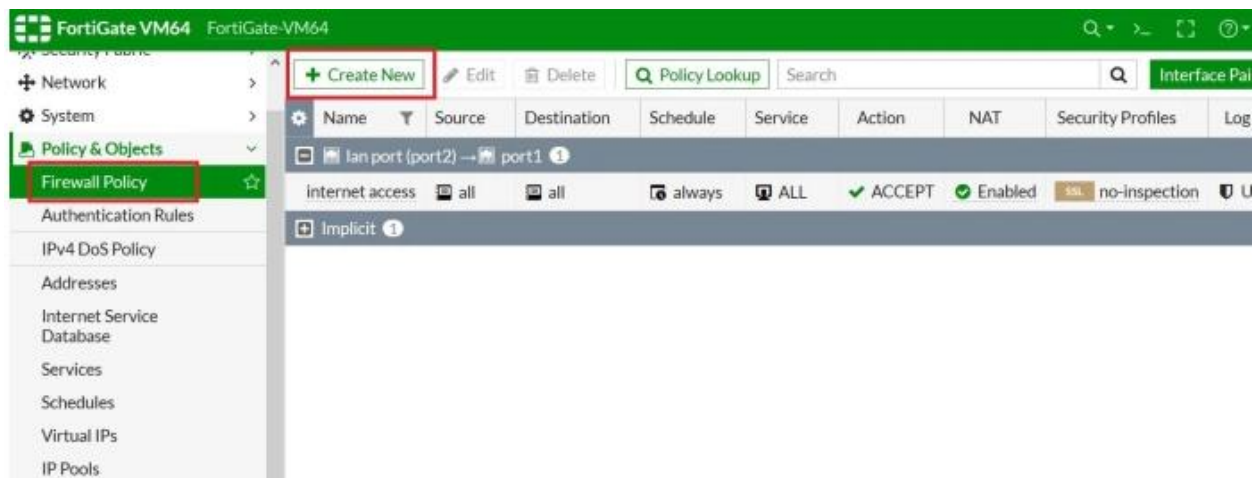


IP route 0.0.0.0 0.0.0.0 Fa0/0 in plain English means “packets from any IP address with any subnet mask get sent to Fa0/0”. Without any other more specific routes defined, this router will send all traffic to Fa0/0.”

4.0 Firewall policy configuration

To configure the **firewall policy** go to

Policy & Objects → *Firewall Policy* → *Create New*



Provide the details

Name: Internet access

Incoming Interface: lan port (port2)

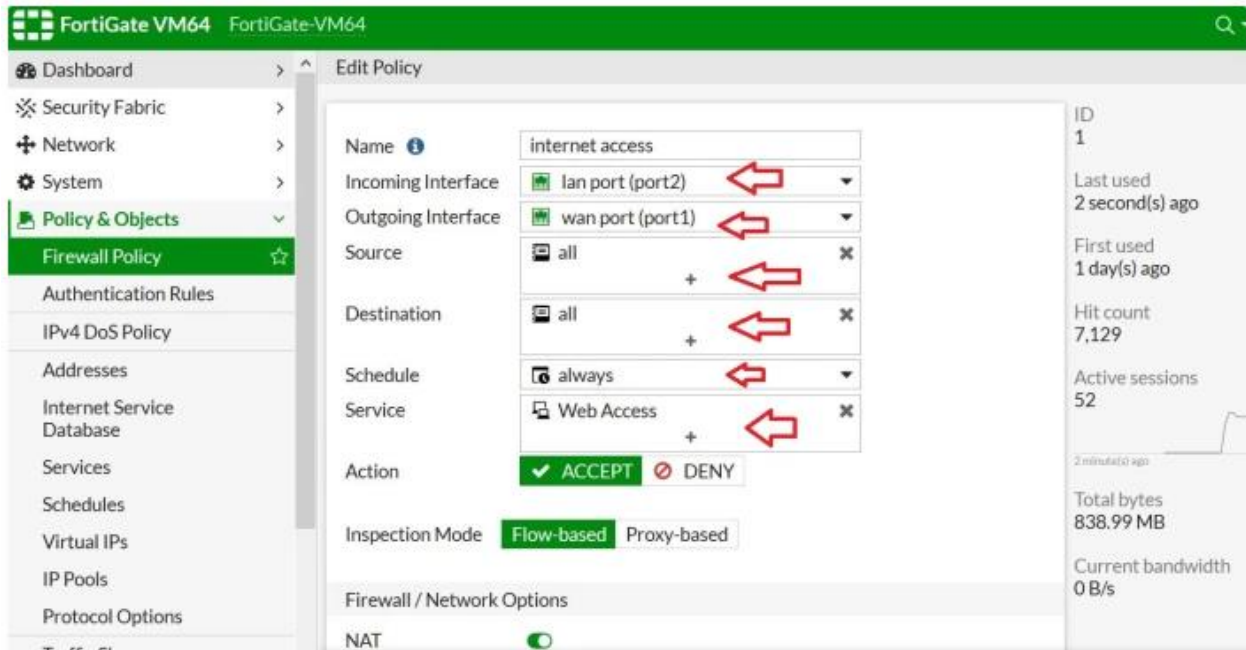
Outgoing Interface: wan port (port1)

Source: all

Destination: all

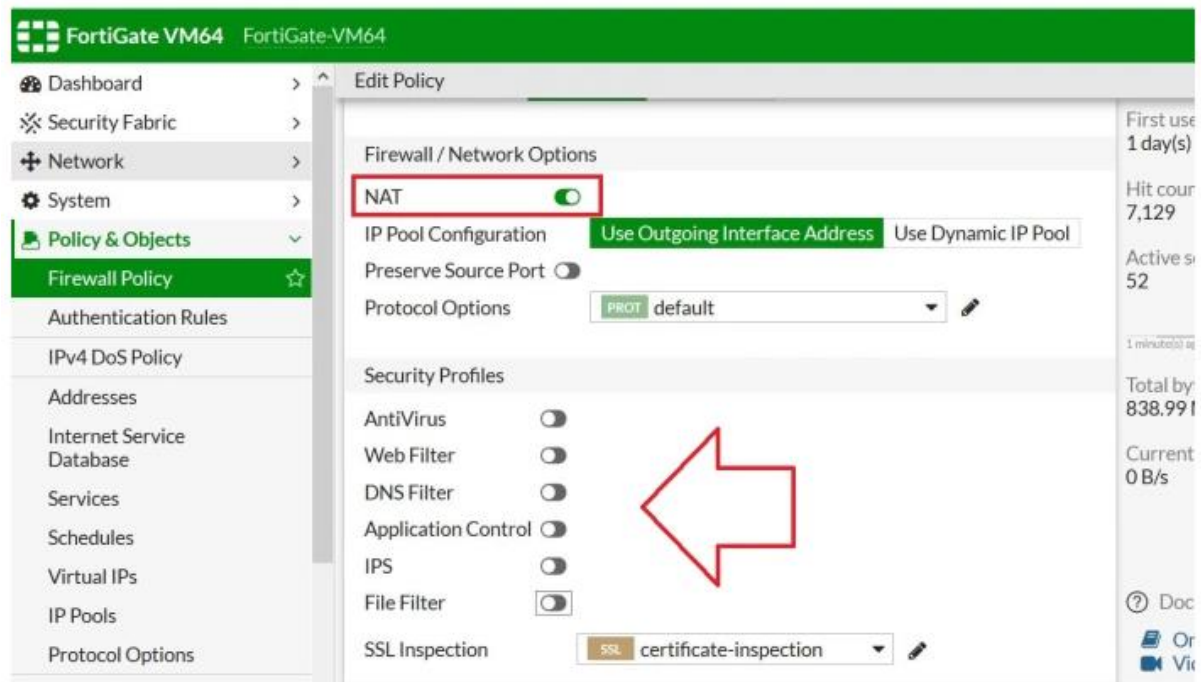
schedule: always

Service: Web Access



Firewall/ Network option: NAT

Security profiles: (Not configured in this case)



يمكن تطبيق ايضا ذلك على راوتر المنزل والتعمق اكثر في خصائصه وايضا خصائص جهاز الاسلكي

أمن الشبكات اللاسلكية

أمن الشبكات اللاسلكية أو الأمن اللاسلكي هي عملية منع الوصول الغير المصرح به أو تلف أجهزة الحاسب الآلي أو البيانات بإستخدام الشبكات اللاسلكية والتي تشمل شبكات wifi

النوع الأكثر شيوعاً من استخدام هذه الشبكات هو نوع أمن **wi-fi**

والذي يتضمن الخصوصية المكافئة للشبكات السلكية **wep** والوصول الآمن اللاسلكي **wpa**

يعد **wep** معيار امان سيئ السمعة حيث نسبة الامان والحماية فيه ضعيفة في الغالب يمكن اختراق كلمات المرور التي تستخدمها في بضع دقائق بإستخدام حاسب آلي محمول مع بعض الأدوات البرمجية المتاحة على نطاق واسع .يعد **WEP** معيار امني قديم منذ عام 1997 والذي تم إستبداله في عام 2003 بمعيار أمني أكثر كفاءة وهو **WPA** او **WI-FI**

Protected Access كان **WPA** بديلاً سريعاً لتحسين الأمان على **wep** المعيار الحالي والأكثر أمناً وحماية هو **WPA2** حيث أنه لايمكن لبعض الأجهزة أن تدعم **WPA2** دون ترقية البرامج الثابتة أو إستبدالها يستخدم **WPA2** جهاز تشفير أقوى مما يساعد بتشفير الشبكة بإستخدام مفتاح بطول 256 بت بشكل عام يعمل طول المفتاح الأطول على تحسين الأمان عبر **WEP** .

الفرق بين WEP و WPA

لحماية البيانات المرسله عبر الويرلس، يجب أن تكون كل نقاط الدخول مجهزة بواحدة من مستويات الأمان، وباختيار أحدها فإنك ستحدث فرقاً بين حماية الشبكة أو تركها عرضة للاختراق.

الخصوصية السلكية المتكافئة WEP- Wired Equivalent Privacy

هو نموذج الأمان الأقدم والأكثر انتشاراً في أنحاء العالم. كان معيار الجيل الأول من أجهزة الشبكة اللاسلكية ويُستخدم لحماية البيانات المنقولة عبرها. وظهر في أيلول 1999 كأول طريقة تشفير خاصة لمعيار IEEE 802.11 ، وصمم لتأمين مستوى حماية مثل شبكات LAN السلكية.

سليبيات WEP

1. وجود عدة نقاط ضعف تسمح للمهاجمين باستخدام برنامج لخرق المفتاح خلال دقائق.
2. استخدام WEP لخاصية التحقق بالمفتاح المشترك وإرسال نفس المفتاح مع حزم البيانات المنقولة عبر الشبكة اللاسلكية ما يعني أنه عند امتلاك المهاجمين لوقت كاف وتجميعهم لبيانات وافية تكون الفرصة مواتية لهم لتشكيل مفاتيحهم الخاص.
3. في حال الحاجة لتغيير المفتاح الرئيسي يجب أن يغير بشكل يدوي على كل الأجهزة المتصلة بالشبكة. وهي مهمة مملّة في حال كانت الأجهزة كثيرة.

إيجابيات WEP

1. أولى فوائد استخدام WEP أنه عندما يجد المستخدمون الشبكة خلال البحث عن الوايرلس، فإن عزيمتهم ستفتر عندما تتطلب إدخال مفتاح. وسيفهموا أنه غير مرحّب بهم.
2. تقدم WEP إمكانية التوافق، فبما أن كل الأجهزة اللاسلكية تدعم تشفير WEP الأساسي. هذا قد يكون مفيداً عند محاولة استخدام أجهزة أقدم وتحتاج إلى توصيل لاسلكي.

الولوج اللاسلكي المؤمن WPA Wireless Protected Access

لوغاريتمية تشفير أقوى أنشأتها مصانع الشبكات خصيصاً لتلافي WPA يملك بروتوكول وتم تطوير هذا المعيار واعتماده رسمياً عام 2003. WEP. أخطاء وبتشابه WPA مع WEP من حيث استخدام نفس طريقة التشفير وفك التشفير لكن لا تستخدم نفس المفتاح الرئيسي. فالأجهزة المتصلة بها تستخدم مفاتيح مؤقتة تتغير ديناميكياً للاتصال.

وقد حسّن WPA الحماية اللاسلكية من خلال استخدام مفتاح ذو 256 بت و TKIP بروتوكول سلامة المفتاح المؤقت بالإضافة إلى EAP (Extensible Authentication Protocol)

على نظام (Temporal Key Integrity Protocol) وهو اختصار لـ TKIP تم بناء بدلاً من المفتاح الواحد الثابت الذي أضاف خاصية per-packet key مفتاح لكل حزمة WEP جديدة عن طريق استخدام مفتاح تشفير مؤقت وغير ثابت وهو بالتأكيد أكثر أماناً من التحقق من هوية المستخدم والتخلص من الحاجة إلى ضبط x فقد أضاف WPA 802.1 أما وهو نمط من السهل اكتشافه وسرقة. MAC الدخول إلى الوايرلس من خلال عناوين

جاء WPA لسد ثغرات ونقائص WEP لكن ورث عنه أيضًا بعض ضعفه، فبالرغم من تمتعه بصلاية أكبر، إلا أن إمكانية اختراقه واردة بعدة طرق منها مهاجمة WPS.

طرق عمل WPA

تعمل WPA (إما بطريقة WPA-PSK المفتاح المشترك أو WPA Personal أو طريقة WPA-802.1x أو WPA Enterprise).

في الطريقة الشخصية الأولى تستخدم شبكة الواي فاي مفتاح مشترك مسبقًا أو عبارة مرور. ويجب أن تكون هذه العبارة هي نفسها على جميع الحواسيب المتصلة بالشبكة اللاسلكية.

أما الطريقة الثانية الاحترافية فتكون أكثر صعوبة عند الضبط، وتستخدم مخدمات 802.1x RADIUS وبروتوكول EAP للتحقق أما WPA2 المطورة عنها فتستخدم AES بدلاً من بروتوكول TKIP للتزود بآلية تشفير أصلب.

ولا تعتبر WPA-PSK أصعب عند البناء أو التشكيل من WEP لكن قد لا تتوافر على بعض المنتجات الأقدم.

ويجب أن يستخدم نفس نوع الأمان كل من الحواسيب، نقاط الوصول، ومحول اليرلس.

إيجابيات WPA

1. تزود بمستوى حماية لاسلكية قوي جدًا.
2. تضيف خاصية التحقق إلى نظام تشفير WEP الأساسي.
3. تقدم دعم متوافق مع WEP للأجهزة غير القابلة للتحديث.
4. تندمج مع سيرفر RADIUS لتسمح بالإدارة، التدقيق، والولوج.

سلبات WPA

1. ماعدا عند استخدام مفتاح المشترك WPA-PSK فإن تصميم وإعداد الشبكات المعقد والمطلوب يعد صعبًا على مستخدمي المنزل التقليديين.
2. البرامج الثابتة القديمة firmware غير مؤهلة لدعمه (غير محدثة).
3. عدم التوافق مع أنظمة التشغيل القديمة مثل Windows 95.
4. أعلى تكلفة وحمولة من WEP.
5. يبقى عرضة لهجمات حرمان الخدمة. Denial of Service attacks.

تمارين :

- 1 : ادخل على راوترك المنزلي وقم بتغيير كلمة المرور ؟
- 2 : ضبط اعدادات الموجه الاسلكي المتصل في الراوتر؟
- 3.قم في الإطلاع على التشفير والجدار الناري داخل الراوتر؟
- 4.قم بتحديد المستخدمين المصرح لهم في الاتصال بالراوتر عن طريق العنوان الفيزيائي؟

نظام كالي KALI

كالي لينكس (kali linux) هي توزيعة لينكس مبنية على دبييان ، وهي متخصصة في الأمن والحماية المعلوماتية وإختبار الإختراق (Penetration Testing) . تم الإعلان عن صدورها في 13 مارس 2013 .

توزيعة كالي هي عبارة عن إعادة بناء لتوزيعة باك تراك حيث قام المطورون ببناؤها على دبييان بدل اوبونتو ، وهي مدعومة وممولة من طرف offensive security ltd . كالي لينكس متخصصة في الأمن والحماية المعلوماتية وتحتوي مسبقاً على عدة برامج وأدوات موجهة لإختبار الإختراق حيث تتضمن برامج تقوم بالمسح الأمني للمنافذ Nmap وبرامج لتحليل الحزم المتبادلة على الشبكات مثل Wireshark ، وبرامج لكسر كلمات المرور كبرنامج John The Ripper، وبرامج Aircrack-ng الخاص بإختبار إختراق الشبكات المحلية اللاسلكية wireless lans و burp suite و owasp و zap لفحص سلامة تطبيقات الويب بالإضافة إلى أدوات أخرى لإختبارات أمنية متعددة.

تنزيل وتثبيت نظام الكالي

يمكنك تحميل ملفات تثبيت نظام كالي من موقع المنظمة على الإنترنت مجاناً، كما يوفر موقع كالي عدة أشكال لملفات التثبيت .

يمكن تنزيل التوزيعه من الموقع الرسمي لها وهو :

<https://www.kali.org/get-kali/#kali-bare-metal>

النسخة بصيغة ISO ثم نقوم في تنزيلها بأحد البرامج التالية :

1.Oracle vm virtualbox manager.

2. VMware Workstation Pro.

بدءاً من 2020.1 لم يعد هناك حساب مستخدم متميز (Super User) وأصبح المستخدم الافتراضي الآن مستخدماً قياسياً غير مميز في kali linux 2020.1 كل من اسم المستخدم وكلمة المرور الافتراضيين هما kali .

I am root!

معظم العمليات التي سنقوم بها في نظام كالي تحتاج مستخدم ذو صلاحيات مميزة ، وبما أننا دخلنا كمستخدم عادي غير مميز ، فليس لدينا هذه الصلاحيات ، لذا سنحتاج للدخول بحساب root للقيام بذلك نقوم بالتالي :

نكتب الامر التالي في ال terminal :

\$sudo su

سيسألك النظام عن كلمة المرور ، ادخل كلمة المرور الافتراضية kali عند نجاح كلمة المرور ندخل الامر التالي :

#passwd root

عند نجاح العملية ، نقوم بتسجيل الخروج من النظام ثم نقوم بالدخول مرة أخرى بإسم المستخدم root وكلمة المرور الجديدة التي تم إدخالها.

يوفر linux kernel نظام تصفية حزم يسمى netfilter والواجهة التقليدية لمعالجة netfilter هي مجموعة أوامر iptables حلاً كاملاً لجدار الحماية يتميز بدرجة عالية من المرونة.

Iptables

Iptables هو برمجية جدار ناري يسمح لمسؤول النظام بتكوين قواعد تصفية حزم ip لجدار حماية linux kernel الذي يتم تنفيذه كوحدات netfilter مختلفة. يتم تنظيم المرشحات في جداول مختلفة والتي تحتوي على سلاسل من القواعد لكيفية التعامل مع حزم مرور الشبكة تستخدم وحدات وبرامج kernel المختلفة حالياً لبروتوكولات مختلفة ، ينطبق iptables

على ipv4 و ipv6 على iptables و arptables على ARP و ebttables على إطارات Ethernet .

يتطلب iptables إمتيازات عالية للعمل ويجب أن يتم تنفيذه بواسطة جدار المستخدم root وإلا فإنه يفشل في العمل . في معظم أنظمة linux .

#apt-get install iptables

لمشاهدة قائمة بجميع القواعد ، إستخدام هذا الأمر

#iptables -L

```
root@kali:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@kali:~# █
```

نرى قائمة بالسلاسل وهي INPUT و FORWARD و OUTPUT

INPUT : هي القواعد الواردة أو حركة المرور الواردة ، لذلك إذا كانت تريد من شخص آخر إختبار إتصال جهاز الكمبيوتر الخاص بك أو الوصول إلى مجلد مشترك ، يمكنك تعيين هذه القواعد هنا.

FORWARD : التحكم في القواعد الواردة أيضاً ولكن لتسليم الحزم المستلمة إلى وجهة أخرى مثل جهاز التوجيه يقوم تمرير الحزم إلى وجهة أخرى .

OUTPUT : هي القواعد الصادرة أو حركة المرور الصادرة ، إذا كنت تريد أن يصل متصفحك إلى الإنترنت فأنت بحاجة إلى إضافة قواعد هنا.

• يوجد بجانب كل سلسلة Policy Accept

هناك ثلاثة خيارات لاستخدام السلاسل reject و drop و accept ستقرر هذه السياسة

الإفتراضية إذا لم يتم العثور على قاعدة أو عنوان معين في السلسلة وستعمل بالسياسة الإفتراضية التي تعد واحدة من الخيارات السابقة .

Accept : سيتم قبول جميع الحزم في حال عدم العثور على قاعدة معينة بخصوص الحزمة.

Drop : إسقاط جميع الحزم في حال لم يتم العثور عليها في القائمة .

Reject : سوف تسقط جميع الحزم ولن ترسل إستجابة إلى الطالب (الوجهة غير قابلة للوصول هو سيراه الطالب) .

لتغيير السياسة الإفتراضية لأي من السلاسل ، نقوم بإضافة الأمر P ثم تحديد السلسلة ثم تحديد السياسة ان كانت بالقبول او الرفض .

مثال :

نقوم بتغيير السياسة الإفتراضية في سلسلة input لقبول جميع الحزم بشكل إفتراضي

#iptables -P INPUT ACCEPT

لإضافة قواعد إلى أي من السلاسل ، دعنا نرى الأوامر التالية :

تسمح هذه القاعدة لجميع الحزم الواردة إلى المضيف المحلي لقبولها

#iptables -A INPUT -i lo -j ACCEPT

تسمح هذه القاعدة لجميع الحزم الصادرة من المضيف المحلي لقبولها

#iptables -A OUTPUT -o lo -j ACCEPT

نرى في الشاشة القبول

شرح الأمر فيما يلي :

-A	إلحاق قاعدة أو أكثر بنهاية السلسلة المحددة
INPUT	في اي سلسلة سنضع القاعدة
-i	اسم الواجهة التي تم من خلالها استلام الحزمة فقط للحزم التي تدخل الى سلاسل INPUT و FORWARD
-o	اسم الواجهة التي تم من خلالها استلام الحزمة فقط للحزم التي تدخل الى سلاسل OUTPUT و FORWARD
lo	الواجهة المحلية
-j	اختصار لكلمة jump يحدد هدف القاعدة
ACCEPT	سياسة القاعدة

ملاحظة: للاطلاع على معاني الاوامر المتعلقة في iptables او باي امر من اوامر shell او حتى لتجربة ان كان الامر مكتوباً بشكل صحيح ام لا.

<https://explainshell.com/explain?cmd=iptables+-A+INPUT+-i+lo+-j+ACCEPT>

لاستعراض المزيد من المعلومات عن اي امر معين يمكننا استخدام الامر `verbose`

`#iptables -L -v`

لمعرفة المزيد من المعلومات بالإضافة الى رقم القاعدة :

`#iptables -L -v - -line -number`

Or

`#iptables -L -v - -line -numbers`

Exam:

```
iptables -L --line-numbers
```

Below is example output of above command which shows line numbers for some of the filters under INPUT policy.

```
# iptables -L --line-number
Chain INPUT (policy DROP)
num target prot opt source destination
1 ACCEPT all -- 10.10.10.20 anywhere
2 ACCEPT all -- localhost anywhere

Chain FORWARD (policy ACCEPT)
num target prot opt source destination

Chain OUTPUT (policy ACCEPT)
num target prot opt source destination
```


للاطلاع على مزيد من المعلومات بالإضافة إلى رقم القاعدة ، ستظهر عناوين المصدر والوجهة كأرقام بدلاً من الأسماء.

```
#iptables -L -v - -line-number -n
```

إذا كنت ترغب في تصفح الويب فستكون هناك حاجة للمنفذ 53 لحل استعلامات dns سنحتاج الى اضافة هذه القاعدة :

```
#iptables -A OUTPUT -o eth0 -p udp - -dport 53 -j ACCEPT
```

-o	الواجهة
-p	برتوكول
-m	الوحدة
--dport	منفذ الوجهة
--sport	منفذ المصدر

مثال 1 :

اضافة منفذ http 80 :

```
#iptables -A OUTPUT -o eth0 -p tcp - -dport 80 -m state - -state NEW -j ACCEPT
```

مثال 2 :

اضافة منفذ http 443 :

```
#iptables -A OUTPUT -o eth0 -p tcp - -dport 443 -m state - -state NEW -j ACCEPT
```

يمكننا تجربة ما اذا كان منفذ الـ dns ومنفذ الـ http من خلال الامر التالي :

```
#wget www.google.com
```

يمكننا تجربة ما اذا كان منفذ الـ dns ومنفذ الـ https من خلال الامر التالي :

```
#wget https://www.google.com
```

تظهر النتيجة

```

Enter Your Command:$ wget https://dl.google.com/linux/direct/google-chrome
-stable_current_amd64.deb
--2020-01-04 00:31:48-- https://dl.google.com/linux/direct/google-chrome-
stable_current_amd64.deb
Resolving dl.google.com (dl.google.com)... 172.217.18.46, 2a00:1450:4006:8
01::200e
Connecting to dl.google.com (dl.google.com)|172.217.18.46|:443... connecte
d.
HTTP request sent, awaiting response... 200 OK
Length: 62181264 (59M) [application/x-debian-package]
Saving to: 'google-chrome-stable_current_amd64.deb'

google-chrome-stab 100%[=====] 59.30M 638KB/s in 1m 43s

2020-01-04 00:33:32 (588 KB/s) - 'google-chrome-stable_current_amd64.deb'
saved [62181264/62181264]

```

لرؤية جميع الأوامر التي ادخلناها لإضافة القواعد ، من خلال الأمر التالي :

#iptables -S

لحذف أي قاعدة بالرقم :

#iptables -D OUTPUT 5

لحفظ أو الالتزام بالقواعد التي أنشأناها مسبقاً :

/sbin/iptables-save > /etc/rules.v4

لاسترجاع القواعد التي أنشأناها مسبقاً :

/sbin/iptables-restore < /etc/rules.v4

لإفراغ جميع قواعد الـ iptables

#iptables -F

لمنع ip معين من الوصول إلى خدمات مثل الـ ftp او الـ ssh من خلال الربط

<https://www.tecmint.com/block-ssh-and-ftp-access-to-specific-ip-and-network-range/>

شرح الأوامر :

-L	عرض قائمة السلاسل
----	-------------------

-P	تغيير السياسة العامة لسلسلة معينة
-A	إحاق قاعدة أو أكثر بنهاية السلسلة المحددة
-i	اسم الواجهة التي تم من خلالها استلام الحزمة فقط للحزم التي تدخل سلاسل INPUT و FORWARD
-o	اسم الواجهة التي تم من خلالها استلام الحزمة فقط للحزم التي تدخل سلاسل OUTPUT و FORWARD
-j	اختصار لكلمة jump يحدد هدف القاعدة
-p	برتوكول
--dport	منفذ الواجهة
--sport	منفذ المصدر
-m	الوحدة
state	تسمح هذه الوحدة عند دمجها مع تتبع الاتصال بالوصول الى حالة تتبع الاتصال لهذه الحزمة / الاتصال
conntrack	نفس عمل state ولكن بإضافات أكثر (تقوم نسخ النواة الحديثة بترجمة state الى conntrack- ايضا هناك من يقول ان state قد اهملت لصالح conntrack
NEW	بدأت الحزمة اتصالاً جديداً أو مرتبطة بطريقة أخرى باتصال لم يتم رؤية الحزم في كلا الاتجاهين
ESTABLISHED	الحزمة مرتبطة باتصال تمت فيه رؤية الحزم في كلا الاتجاهين
RELATED	تبدأ الحزمة اتصالاً جديداً ، ولكنها مرتبطة باتصال موجود ، مثل نقل بيانات FTP او خطأ ICMP

تمرين

باستخدام الـ iptables في نظام اللينوكس ، نفذ التالي :

- أفرغ جميع قواعد الـ iptables rules
- غير القاعدة الافتراضية للـ INPUT لكي يسمح لأي إتصال بالحاسوب
- غير القاعدة الافتراضية للـ OUTPUT لتحجب جميع الإتصالات
- أضف قاعدة جديدة للسماح للكل (الواردة والصادرة) بالاتصال بالـ local (lo) host
- أضف قاعدة جديدة للـ DNS (53) ليتم ترجمة النطاقات المطلوبة من قبل المستخدم
- أضف قاعدة جديدة للاتصال عبر بروتوكول https (443)

باستخدام الـ iptables في نظام اللينوكس ، نفذ التالي :

- غير القاعدة الافتراضية للـ FORWARD لكي يسمح لأي اتصال بالحاسوب
- غير القاعدة الافتراضية للـ OUTPUT لتحجب جميع الاتصالات
- أضف قاعدة جديدة للسماح بالحزم الصادرة بالاتصال بالـ local host (lo)
- أضف قاعدة جديدة للـ DNS (53) ليتم ترجمة النطاقات المطلوبة من قبل المستخدم
- أضف قاعدة جديدة للاتصال عبر بروتوكول HTTP (80)

خدمة البريد

تستمتع خوادم البريد مثل postfix و sendmail الى تشكيلة واسعة من المنافذ بناء على البروتوكولات المستخدمة لتوصيل البريد ، إذا كنت تشغل خادم بريد إلكتروني ، فحدد البروتوكولات التي تستخدمها واسمح للاتصالات الموافقة لها .سنستعرض ايضاً مثلاً عن إنشاء قاعدة لحجب بريد smtp الصادر.

حجب بريد smtp الصادر ربما تريد ان تحجب بريد smtp الصادر اذا لم يكن من المفترض لخدمك ان يرسل بريداً إلكترونياً ، استخدام الأمر الاتي لحجب بريد smtp الصادر (الذي يستخدم المنفذ 25).

```
#iptables -A OUTPUT -p tcp -dport 25 -j REJECT
```

يضبط الأمر السابق خادمك لتجاهل كل البيانات المرسلة على المنفذ 25 ، إذا أردت أن تحجب خدمة أخرى عبر رقم منفذها ، فضع رقم رقم المنفذ الخاص بها بدلاً من 25.

السماح لجميع اتصالات smtp الواردة

للسماح لخدمك بالرد على اتصالات smtp على المنفذ 25، فعليك تنفيذ الأمرين الاتيين:

```
iptables -A INPUT -p tcp -dport 25 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -p tcp -sport 25 -m conntrack -ctstate ESTABLISHED -j ACCEPT
```

الأمر الثاني الذي يسمح بمرور بيانات التراسل الشبكي لاتصالات smtp المنشأة (مطلوب فقط إذا لم تكن سياسة OUTPUT مضبوطة إلى ACCEPT

ملاحظة : من الشائع لخوادم smtp ان تستخدم المنفذ 587 للبريد الصادر.

السماح لجميع اتصالات IMAP الواردة

للسماح لخادمك بالرد على اتصالات IMAP على المنفذ 143 فعليك تنفيذ الأمرين الاتيين:

```
iptables -A INPUT -p tcp - -dport 143 -m conntrack - -ctstate  
NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -p tcp - -sport 143 -m conntrack - -ctstate  
ESTABLISHED -j ACCEPT
```

الأمر الثاني الذي يسمح بمرور بيانات التراسل الشبكي لاتصالات IMAP المنشأة (مطلوب فقط إذا لم تكن سياسة OUTPUT مضبوطة إلى ACCEPT

تمرين

السماح لجميع اتصالات IMAPS الواردة

للسماح لخادمك بالرد على اتصالات IMAPS على المنفذ 993 .

الحل:

```
iptables -A INPUT -p tcp - -dport 993 -m conntrack - -ctstate  
NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -p tcp - -sport 993 -m conntrack - -ctstate  
ESTABLISHED -j ACCEPT
```

الأمر الثاني الذي يسمح بمرور بيانات التراسل الشبكي لاتصالات IMAP المنشأة (مطلوب فقط إذا لم تكن سياسة OUTPUT مضبوطة إلى ACCEPT

السماح لجميع اتصالات POP3 الواردة

للسماح لخادمك بالرد على اتصالات POP3 على المنفذ 110 ، فعليك تنفيذ الأمرين الاتيين

```
iptables -A INPUT -p tcp - -dport 110 -m conntrack - -ctstate  
NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -p tcp - -sport 110 -m conntrack - -ctstate  
ESTABLISHED -j ACCEPT
```

الأمر الثاني الذي يسمح بمرور بيانات التراسل الشبكي لاتصالات POP3 المنشأة (مطلوب فقط إذا لم تكن سياسة OUTPUT مضبوطة إلى ACCEPT

تمرين

السماح لجميع اتصالات POP3 الواردة

للسماح لخدمك بالرد على اتصالات POP3 على المنفذ 599 .

الحل:

```
iptables -A INPUT -p tcp - -dport 995 -m conntrack - -ctstate  
NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -p tcp - -sport 995 -m conntrack - -ctstate  
ESTABLISHED -j ACCEPT
```

الأمر الثاني الذي يسمح بمرور بيانات التراسل الشبكي لاتصالات POP3 المنشأة (مطلوب فقط إذا لم تكن سياسة OUTPUT مضبوطة إلى ACCEPT

بالنسبة لـ ipv6 ، يوجد جدول منفصل يمكننا بدئه او تعديله طالما احتجنا الى كيفية العمل مع حركة مرور ipv6 .

لعرض جدول ipv6 :

```
#ip6tables -L
```

إذا كنا نرغب في منع كل حركة المرور باستخدام ipv6 فسوف نسقط كل الحزم المتعلقة بـ ipv6 باستخدام الأمر الذي استخدمناه من قبل ولكن مع ipv6 هذه المرة:

```
#ip6tables -p INPUT DROP
```

```
#ip6tables -p FORWARD DROP
```

```
#ip6tables -p OUTPUT DROP
```

جدار الحماية غير المعقدة (ufw) uncomplicated firewall

يعد جدار الحماية غير المعقدة ufw بمثابة واجهة امامية للأجهزة iptables وهو مناسب بشكل خاص لجدارن الحماية القائمة على المضيف .يوفر ufw اطار عمل لإدارة netfilter بالإضافة الى واجهة سطر اوامر لمعالجة جدار الحماية .تهدف ufw الى توفير واجهة سهلة الاستخدام للأشخاص الذين ليسوا على دراية بمفاهيم جدار الحماية ، بينما في نفس الوقت تعمل على تبسيط اوامر iptables المعقدة لمساعدة المسؤول الذي يعرف ما يفعله ufw هو المنبع لتوزيعات اخرى وواجهات رسومية.

لتثبيت ufw :

#apt-get install ufw

في حال فشل التثبيت ، قم بتحديث قائمة الحزم :

#apt update

ثم نقم بمحاولة تثبيت ufw من جديد ، من خلال الامر install
في حال فشل التثبيت مرة اخرى ، قم بإدخال الامر التالي :

#apt update && apt full –upgrade -y

ثم قم بمحاولة تثبيت ufw من جديد ، من خلال الامر install
لفحص حالة ufw:

#ufw status

اذا كانت حالته غير مفعل inactive هذا يعني انه لم يتم اعداد اي تهيئة لجدار الحماية باستخدام ufw لتفعيل ufw :

#ufw enable

سيؤدي ذلك إلى تمكين ufw وسيعمل على إنشاء iptables باستخدام ufw استعلم عن حالة ufw مرة اخرى وستظهر انه تمت إضافة عدد من القواعد 80 لمنفذ http و443 لمنفذ https و53 على udp لقاعدة DNS و67 و68 لقاعدة DHCP .
لإظهار المزيد من المعلومات حول حالة UFW:

#ufw status verbose

لتحديث السياسة الافتراضية الخاصة بالواردة او الصادرة

#ufw default deny outgoing

لإضافة قاعدة محددة مثل ssh الصادرة

#ufw allow out 22

لحذف قاعدة معينه

#ufw delete allow out 22

لاضافة نطاق من القواعد او المنافذ

#ufw allow out 67:68/udp

لحذف قاعدة معينة عن طريق رقم القاعده

#ufw status numbered

ثم

#ufw delete 2

تمرين

باستخدام ال ufw في نظام الليونكس نفذ التالي :

*غير القاعدة الافتراضية لل incoming لكي يسمح لاي اتصال قادم الى الحاسوب

*اضف قاعدة جديدة لل dns 53 ليتم ترجمة النطاقات المطلوبة من قبل المستخدم

*اضف قاعدة جديدة للاتصال عبر بروتوكول http 80

*اضف قاعدة جديدة للسماح بالاتصال عن بعد على المنفذ 22

*اظهر التغييرات التي قمت بها على سلاسل ufw

Gufw

هناك بدائل لإدارة iptables و gufw هو واحد منهم وتم بنائه على ufw ولكن مع واجهة

مستخدم بسيطة لتثبيت gufw

#apt – get install gufw

#gufw&

مسح المنافذ (port scanning)

يعد فحص المنافذ احد اكثر اشكال الاستطلاع شيوعاً قبل الإختراق ، مما يساعد المهاجمين على تحديد المنافذ الأكثر عرضة للإصابة .يمكن أن يؤدي فحص المنفذ إلى دخول أحد المتطفلين إلى شبكتك واستغلال بياناتك ، فما هو فحص المنافذ؟

فحص المنافذ : هو عملية مسح مضيف معين للمنافذ المفتوحة وبالتالي معرفة الخدمات التي تعمل .

يوفر فحص المنافذ المعلومات التالية للمهاجمين :

- ماهي الخدمات قيد التشغيل (الخدمات العاملة حالياً).
- المستخدمين الذين يمتلكون الخدمات (المشغلين لتلك الخدمات).
- هل هناك أذن لتشغيل الخدمات من قبل مجهولين (غير مسجلين).
- ماهي خدمات الشبكة التي تتطلب المصادقة (مصادقة اثبات الهوية).

: NMAP

NMAP اختصار لـ network mapper وهو اداة مجانية ومفتوحة المصدر لاكتشاف الشبكة ويستخدمها محترفي الامن او المتسللون او اي شخص يريد ان يعرف عن اي جهاز متصل بشبكة معينة.

يستخدم nmap لاكتشاف المضيفين والخدمات على شبكة الكمبيوتر عن طريق ارسال الحزم وتحليل الردود.

فكر فيها كمهمة مراقبة ، للدخول الى منزل غريب يجب القاء نظرة على المنزل ومشاهدة عدد النوافذ والابواب المفتوحة او المعرضة للاختراق والتي يمكن استغلالها ، لذلك في ليست اداة قرصنة بل اداة لجمع المعلومات .

لرؤية اوامر المساعدة

#nmap - -help (or-h)

الامر الاساسي الذي يمكننا تجربته هو البحث عن ip لجهاز مستهدف :

#nmap 192.168.1.35

يمكنك محاولة مسح موقع الويب المعروض في الامثلة :

#nmap scanme.nmap.org

للبحث عن قائمة بالعناوين ، يمكنك استخدام الامر -iL ولكن عليك اولاً إنشاء ملف بالعناوين :

#nano targets.file

ثم اكتب العناوين التي تريدها في الملف ثم احفظها:

192.168.1.1-30

Scanme.nmap.org

ثم اكتب

#nmap -iL targets.file

سوف يبحث عن المنافذ المفتوحة على العناوين المدرجة في الملف سوف يقوم الامر -iR
بالبحث عن عدد عشوائي من المضيفين :

#nmap -iR 3 -vv

3: هو عدد المضيفين العشوائي

-v	المستوى 1 المطول : الذي سيظهر المزيد من المعلومات
-vv	المستوى الثاني المطول : سيظهر معلومات اكثر
-vvv	المستوى الثالث

من الامر ifconfig يمكنك التحقق من عنوان ip الخاص بك ثم مسحه لإظهار المنافذ
والمضيفات المفتوحة والموصولة على شبكتك .

حالة المنافذ :

مفتوح (open) هذا يعني ان المنفذ يقبل اتصالات tcp udp مما يعني ان هذا المنفذ يمكن
ان يتعرض لعمليات استغلال القرصنة .

مغلق (closed): يمكن الوصول الى المنفذ ويمكنك الاستماع اليه ، لكن لا يوجد تطبيق

يستخدمه فحص هذا المنفذ مفيد حتى تتمكن من معرفة ما اذا كان المضيف يعمل (شغال) ولكن لم يتم استخدام اي منافذ ، لذلك ربما تعود لاحقاً لمعرفة ما اذا كان اي شئى تغير.

مثال : اعرض جميع البورتات الخاصه بـ ip معين ؟

```
nmap -sS -sV 80.***.***.151
```

IP الهدف

ان هذا الامر سوف يساعدنا على عرض جميع البورتات المفتوحة الخاصة بعنوان الـ IP الهدف.

المرشح (filtered) هذا يعني ان nmap لا يمكنه تحديد ما اذا كان المنفذ مفتوحاً او مغلقاً بسبب تعذر الوصول اليه ، نظراً لعدم وصول حزم التصفية الى المنفذ ربما بسبب وجود جدار حماية او تطبيق مكافحة فيروسات او ببساطة ازدحام شبكة او اي شئى من شأنه اسقاط الحزم من الوصول الى منافذ المضيفين .

بدون تصفية (unfiltered) يمكن لـ nmap الوصول الى المنفذ ولكن لايمكن تحديد ما اذا كان مفتوحاً ام مغلقاً .

الإكتشاف : (Discovery)

ما يهمنا هنا هو المضيف يجب ان يكون عاملاً من اجل الاستفادة من المنافذ المفتوحة .

يمكنك رؤية خيارات المساعدة في عدد من الخيارات من nmap-help لاختبار خيارات الاكتشافات اذا قمت بكتابة nmap مع عنوان ip دون اضافة اي خيارات اكتشاف فسيقوم nmap بارسال الطلب التالي :

1.ICMP echo request(ping).

2.TCP SYN packet to port443.

3.TCP ACK packet to port 80.

4.ICMP timestamp request.

دعنا نرى تنفيذ الاوامر التالية

-sL	سيقوم بسرد الاهداف المطلوب مسحها
-sn	قم بطباعة الاجهزة المضيفة التي اكتشفت في الشبكة فقط
-Pn	تخطي مرحلة الاكتشاف والقيام بالمسح

دعنا نختبر الامر الاول لخيارات الاكتشاف التي سيقوم ببساطة بسرد الاهداف المطلوب مسحها.

`#nmap yahoo.com/24 -sL`

سوف يسرد عددا من الاهداف على العنوان الذي كتبتة (اخر 254 مضيفاً) ، من المفيد التحقق من خوادم اسماء DNS الاخرى ونوع الشبكات التي قد تكون لديهم.
قم بتعطيل فحص المنافذ وقم بطباعة الاجهزة المضيفة التي اكتشفت في الشبكة فقط

`#nmap [youraddress]/[subnetmask]-sn`

تخطي اكتشاف المضيف وتعامله مع كل المضيف على الانترنت (تخطي مرحلة الاكتشاف والقيام بالمسح).

`#nmap 192.168.1.1-5 -Pn -v`

تقنيات المسح

يمكنك البحث عن بروتوكول او منفذ معين باستخدام اداة تقنيات المسح ، والتي يمكنك رؤيتها من قائمة المساعدة الخاصة بـ nmap

`#nmap 192.168.1.35 -sU -sS -v`

سيبحث هذا الامر عن المنافذ التي تقوم بتشغيل خدمات فحص (-sS)SYN(UDP(sU) ضع في اعتبارك ان عمليات مسح TCP عادة ما تكون اسرع قليلاً من عمليات مسح UDP .

يعمل هذا عن طريق ارسال الـ nmap حزم UDP الى جميع المنافذ اي منفذ يستجيب مع حزمة udp سيعتبر منفذاً مفتوحاً اذا لم يكن هناك رد هذا المنفذ سيكون مفتوحاً | مرشح

Open| filtered

```
#nmap 192.168.1.35 -sO
```

سوف يتحقق من المنافذ المفتوحة لكل بروتوكول

```
#nmap 192.168.1.35 -sO -p 1,2,3,4,5,6,7
```

سوف يتحقق من وجود منفذ معين من خلال الرقم

مواصفات المنفذ port specifications

```
#nmap 192.168.1.35 -v -p U:1,2,3,4,5,6,7,T:21-25,8080
```

سوف يتحقق من وجود منفذ معين من خلال الرقم او يمكنك البحث عن قواعد البروتوكول او المنافذ عن طريق تحديد اسم المنفذ بدلا من الرقم

```
#nmap 192.168.1.35 -v -p http,https,ftp
```

تمرين:

ماذا تفعل هذه الاوامر ؟ اعطي مثال لكل واحد

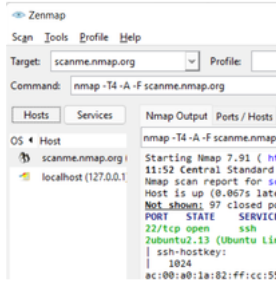
-A	
-O	
-T4	
-F	

Zenmap

هو واجهة المستخدم الرسومية لأداة Nmap ويمكن تثبيته على كل أنظمة التشغيل تقريبا لينوكس ويندوز وحتى mac os.

لتثبيته على نظام الويندوز ، يمكنك الذهاب الى الموقع الرسمي لـ zenmap والتوجه الى Downloads ومن ثم تحميل ملف التثبيت.

Microsoft Windows binaries



Please read the [Windows section](#) of the Install Guide for limitations and installation instructions for the Windows version of Nmap. You can choose from a self-installer (includes dependencies and also the Zenmap GUI) or the much smaller command-line zip file version. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 R2 and newer. We also maintain a [guide for users who must run Nmap on earlier Windows releases](#).

Note: The version of Npcap included in our installers may not always be the latest version. If you experience problems or just want the latest and greatest version, download and install [the latest Npcap release](#).

The Nmap **executable Windows installer** can handle Npcap installation, registry performance tweaks, and decompressing the executables and data files into your preferred location. It also includes the Zenmap graphical frontend. Skip all the complexity of the Windows zip files with a self-installer:

Latest **stable** release self-installer: [nmap-7.92-setup.exe](#)

Latest Npcap release self-installer: [npcap-1.60.exe](#)

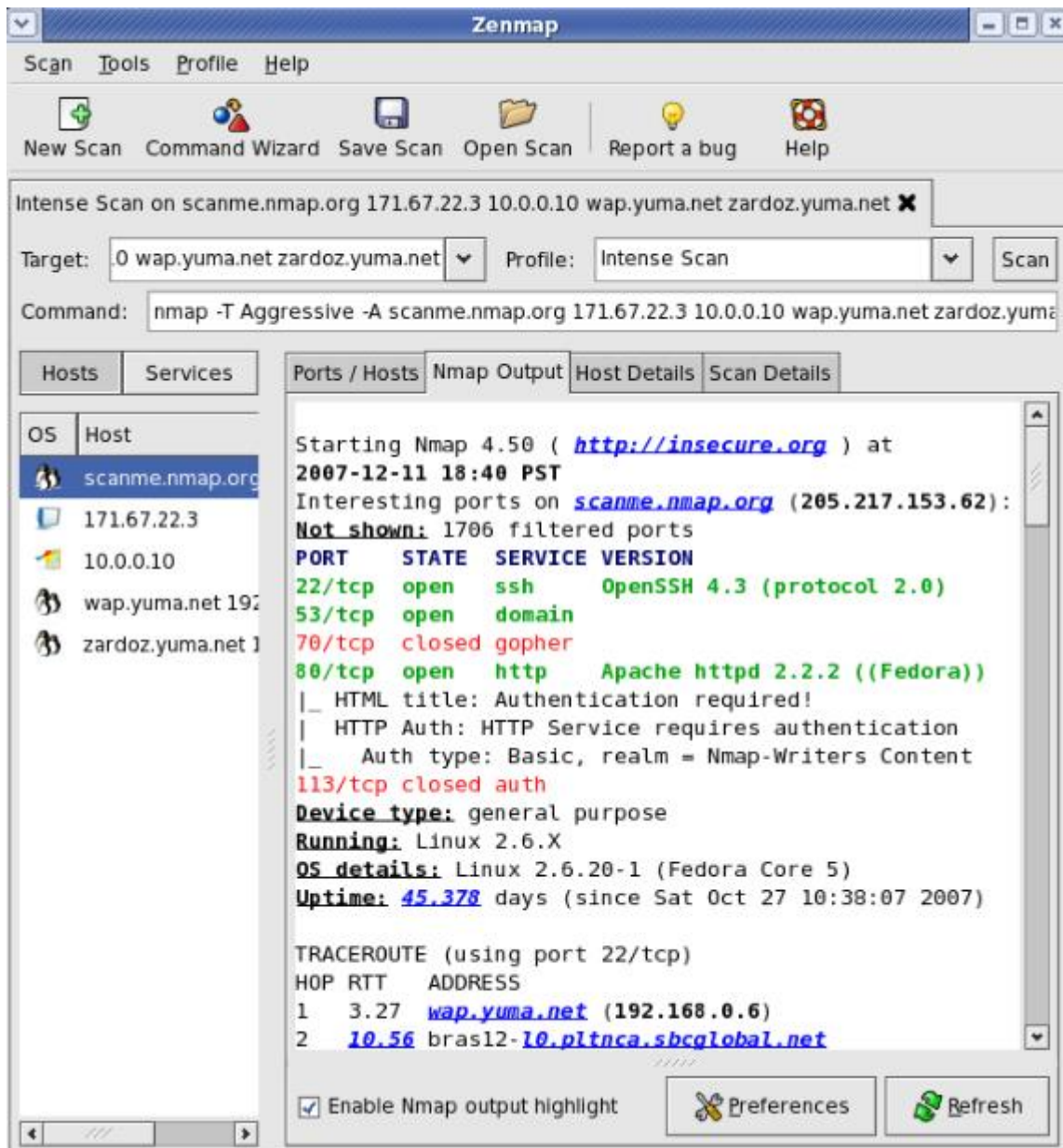
We have written [post-install usage instructions](#). Please [notify us](#) if you encounter any problems or have suggestions for the installer.

For those who prefer the command-line zip files ([Installation Instructions](#); [Usage Instructions](#)), they are still available. The Zenmap graphical interface is *not* included with these, so you need to run nmap.exe from a DOS/command window. Or you can download and install a superior command shell such as those included with the free [Cygwin system](#). Also, you need to run the [Npcap](#) and [Microsoft Visual C++ Redistributable Package](#) installers which are included in the zip file. The main advantage is that these zip files are a fraction of the size of the executable installer:

Latest **stable** command-line zipfile: [nmap-7.92-win32.zip](#)

بعد تحميل الملف ، نقوم بتنصيب البرنامج بخطوات بسيطة .

يمكنك وضع اي امر حاولنا باستخدام nmap في zenmap ولكن هنا يمكننا تحديد الاهداف بشكل منفصل عن شريط الاوامر لذلك من السهل فقط تغيير الهدف او الاهداف.

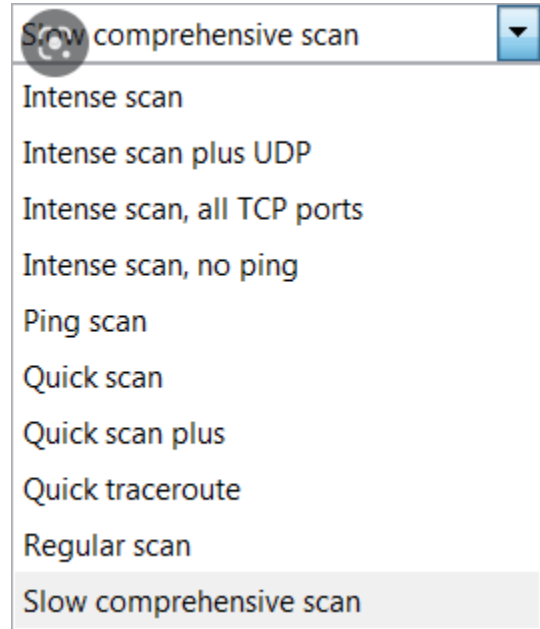


يمكننا في خانة target تحديد هدف او عدة اهداف من خلال ادخال مدى معين كما فعلنا بأوامر الـ nmap في الـ terminal .

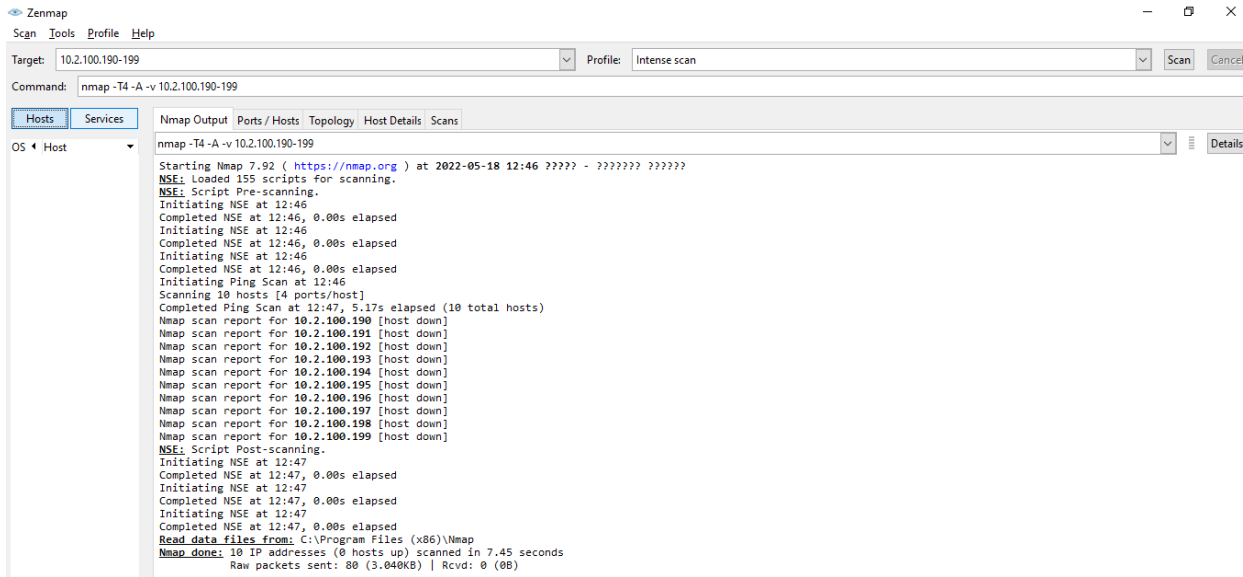
لاحظ عند كتابة الاهداف ان خانة الاوامر command قد تبديلت لتشغيل جملة كاملة يمكننا من خلالها ايضا تجربتها في الـ nmap ولكن ما هي الاوامر الموجودة بشكل افتراضي في خانة الامر (A,T4)؟

تم ادخال هذه الاوامر من خلال اختيار احد التعريفات المسبقة الموجودة على جهة اليمين من البرنامج profile .

يمكنك اختيار اي ملف تعريف مناسب من هذه القائمة.

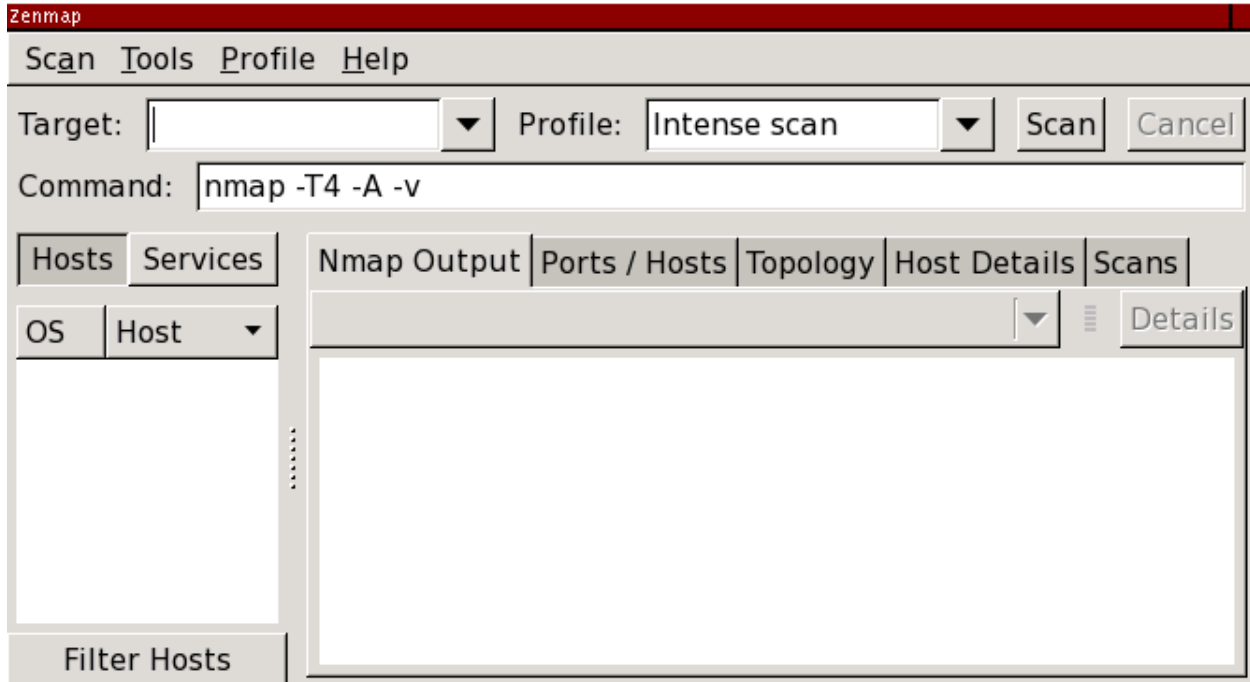


من القائمة الموجودة على جهة اليسار hosts يمكننا رؤية تفاصيل عن كل الأجهزة التي تم اكتشافها عن طريق البرنامج لعناوين الـ ip التي تم إدخالها كما في الشكل التالي :



في الشكل السابق تم البحث عن عن مدى من العناوين الـ ip من 190 الى 199

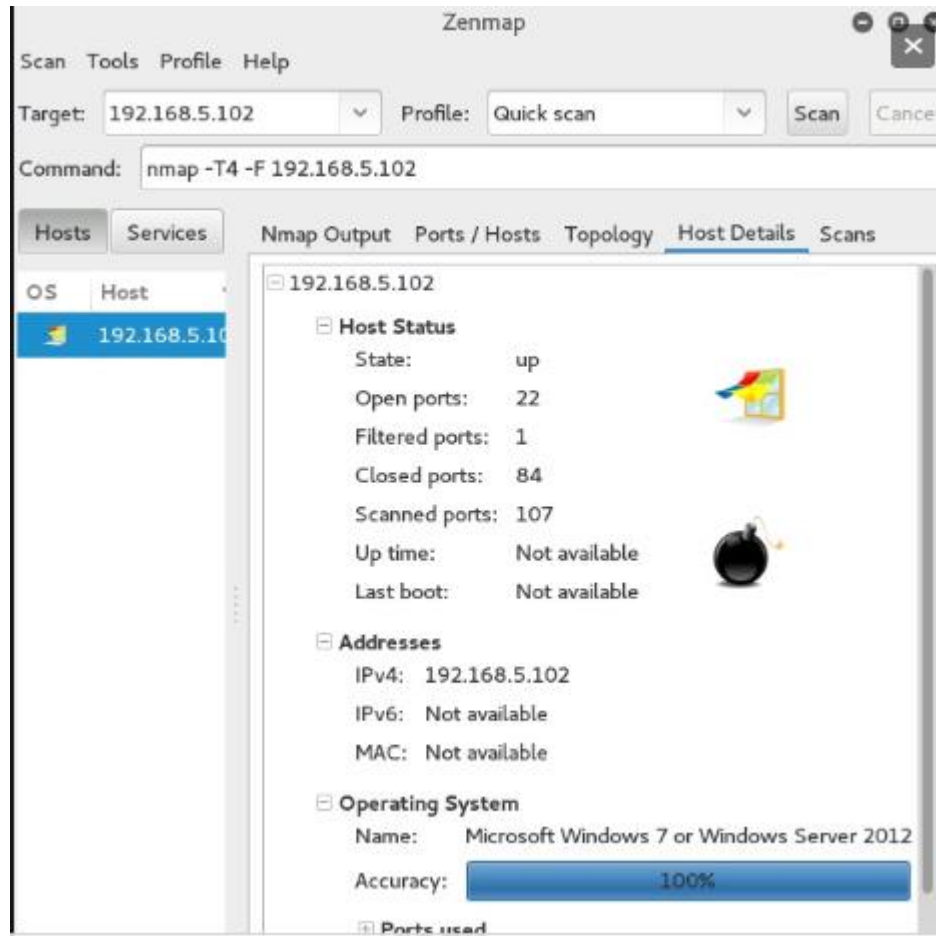
بجانب زر hosts هناك زر اخر باسم services والذي من خلاله يمكن معرفة جميع المنافذ العاملة والمكتشفة بالـ zenmap واي من المستخدمين يعمل على تلك الخدمة من خلال خيار (ports/hosts) مثل :



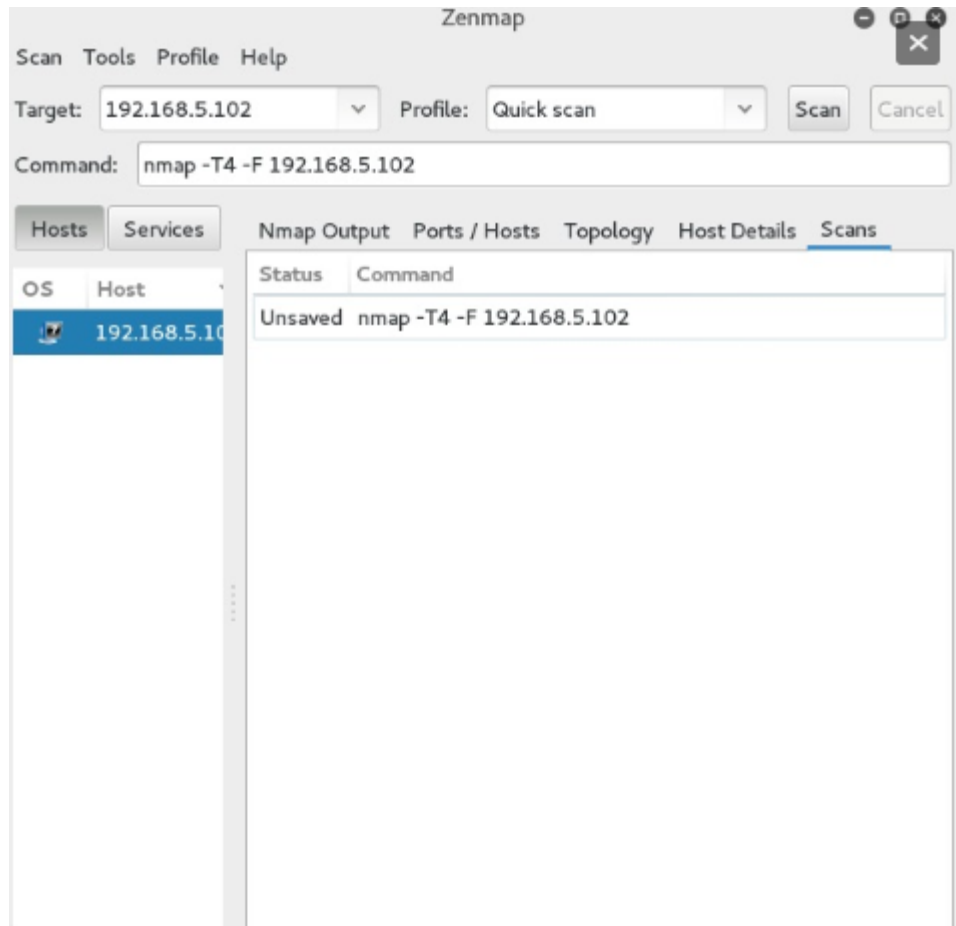
بإمكاننا أيضا استعراض شكل الشبكة المكتشفة عن طريق خيار **topology** والذي سيعرض شكل الشبكة بطريقة رسومية – مثال :



إذا ضغطت على زر legend سيظهر تفاصيل كل شكل في الخارطة الرسومية يمكننا معرفة المزيد عن جهاز المضيف بواسطة خيار الـ host details

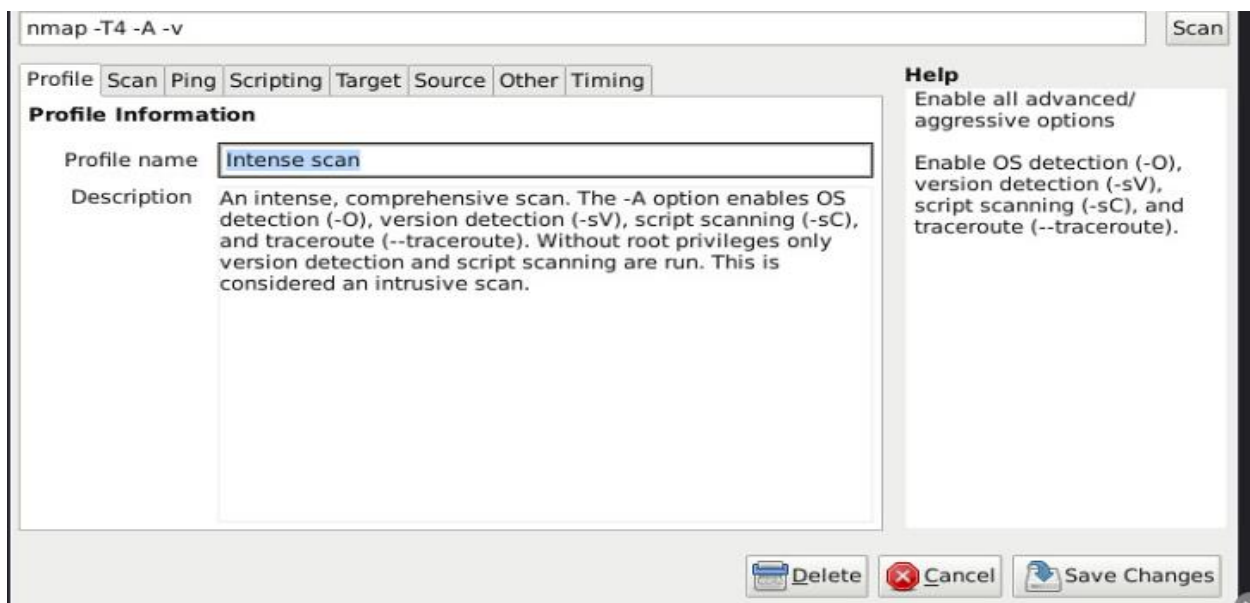


واخيرا يمكنك الاطلاع على قائمة بأوامر المسح التي قمت بها مؤخرا من خلال زر scans حيث يمكنك اضافة ، مسح او حفظ اي من الاوامر الموجودة في القائمة :



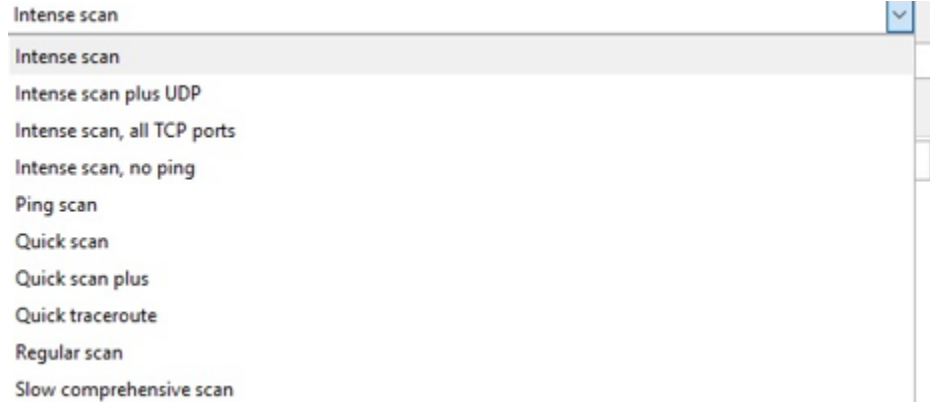
يمكنك اضافة اي تعريف اضافي لحفظه واستخدامه لاحقا عن طريق الاختيار من القائمة :

Profile>new profile or command



ويمكنك تعديل او اضافة اي امر من الاوامر الاضافيه للملف التعريفي الذي قمت بعمله ، مثل اوامر المسح الـ ping ، الاهداف والتوقيات.

بعد اعداد الملف التعريفي احفظ الملف (save changes) ثم ستراه من قائمة profile في الصفحة الرئيسية :



• يمكن فحص المنافذ على الشبكة من خلال الموقع التالي :

<https://www.yougetsignal.com/tools/open-ports/>

Port Forwarding Tester

your external address

open port finder

Remote Address Port Number

Port 80 is closed on 46.100.61.120

about

The open port checker is a tool you can use to check your external IP address and detect open ports on your connection. This tool is useful for finding out if your port forwarding is setup correctly or if your server applications are being blocked by a firewall. This tool may also be used as a port scanner to scan your network for ports that are commonly forwarded. It is important to note that some ports, such as port 25, are often blocked at the ISP level in an attempt to prevent malicious activity.

For more a comprehensive list of TCP and UDP ports, check out [this Wikipedia article](#).

If you are looking for a software solution to help you configure port forwarding on your network, try using this powerful [Port Forwarding Wizard](#).

If my tool has been helpful to you, check out my [desktop wallpaper](#) site or follow me on Twitter [@kirkouimet](#). Also, if your router is causing you massive grief try picking up a cheap Netgear N600 on [Amazon](#).

common ports

21 FTP
22 SSH
23 TELNET
25 SMTP
53 DNS
80 HTTP
110 POP3
115 SFTP
135 RPC
139 NetBIOS
143 IMAP
194 IRC
443 SSL
445 SMB
1433 MSSQL
3306 MySQL
3389 Remote Desktop
5632 PCAnywhere
5900 VNC
25565 Minecraft
Scan All Common Ports

مراقبة الشبكة من التهديدات الأمنية باستخدام برنامج Wireshark

كمسؤول عن امن الشبكة ، تعد مراقبة الشبكة امرأ ضرورياً للعمليات اليومية ، سواء كنت تحاول فهم بروتوكول ما او تصحيح عميل شبكة أو تحليل حركة البيانات ، تصبح أدوات مراقبة الشبكة من الأدوات المهمة التي يمكن الإستفادة منها مثل أدوات السنيفر network sniffer .

ماهو الـ sniffing ؟

أداة حزم الـ sniffing (ومعناها الحرفي من الإنجليزية الشم) هي أداة مساعدة ثم استخدامها منذ الإصدار الأصلي لشبكة إيثرنت ، تسمح عملية الـ sniffing للأفراد بالتقاط البيانات أثناء إرسالها عبر شبكة . يتم استخدام هذه التقنية من قبل محترفي الشبكات لتشخيص مشكلات الشبكة والمستخدمين الضارين لالتقاط بيانات غير مشفرة ، مثل كلمات المرور واسماء المستخدمين إذا تم التقاط هذه المعلومات خلال نقل المعلومات ، يمكن للمستخدم الوصول الى النظام او الشبكة ككل.

Wireshark

يعرف على نطاق واسع wireshark (المعرف سابقاً بإسم Ethereal) كأكثر أداة تستعمل لعمليات الـ sniffing شعبية في العالم. تطبيق مجاني مفتوح المصدر يعرض بيانات حركة المرور مع الترميز اللوني للإشارة إلى البروتوكول الذي تم استخدامه لنقله.

يستخدم wireshark مكتبات libpcap على linux أو winpcap على windows من اجل التقاط الحزم من الشبكة .إذا قام المستخدم بتطبيق أي عوامل فلترة (filtering) لالتقاط الحزم عبر wireshark .يتم إسقاط الحزم المفلترة ويتم تمرير البيانات ذات الصلة فقط إلى محرك الالتقاط.

يقوم محرك الالتقاط بتشريح الحزم الواردة ، ويحللها ، ثم يطبق أي فلاتر إضافية للعرض قبل إظهار النتيجة للمستخدم . يكمن سر استخدام أدوات الشبكة مثل wireshark في استخدام ادوات الفلترة لالتقاط وعرض المعلومات المهمة فقط.

Capturing from wireshark.fifo [Wireshark 1.8.10 (SVN Rev. Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

802.11 Channel: Channel Offset: FCS Filter: All Frames None

No.	Time	Source	Destination	Protocol	Length	Frame check sequence	Info
1	0.000000000	9f:1f:c7:a4:9d:e1	09:3f:0e:b6:28:bb	LLC	8561	0xbe42713a	I, N(R)=84, N(S)=60; DSAP 0xb6 Individual, SSAP 0xc8 Response
2	0.000000000	f3:1f:5d:15:f8:7c	2a:0e:fd:3d:fa:00	LLC	7204	0x94ef4d0b	I, N(R)=9, N(S)=29; DSAP 0xc1 Individual, SSAP 0x94 Command
3	0.000000000	49:3c:f4:81:9a:2d	24:43:4b:e9:90:f0	LLC	2874	0xe44b9e48	I, N(R)=81, N(S)=51; DSAP 0xe4 Individual, SSAP LLC Sub-Layer Management
4	0.000000000	12:7e:bc:2c:f0:57	e7:d5:49:09:8d:8b	LLC	8614	0xb644e168	I, N(R)=37, N(S)=50; DSAP 0xb6 Group, SSAP 0xd8 Command
5	0.000000000	1b:29:23:5a:cb:61	3e:1a:1e:f3:f7:89	LLC	2963	0xce9fb421	S F, func=RE3, N(R)=99; DSAP 0x36 Individual, SSAP 0xc0 Response
6	0.000000000	1a:57:45:58:04:84	aa:09:be:e5:a0:96	LLC	2959	0xce023f09	I, N(R)=97, N(S)=32; DSAP 0xb4 Group, SSAP EIA RS-511 Manufacturing Messe
7	0.000000000	19:63:90:dc:6e:1f	65:23:2c:54:a0:7f	LLC	2373	0xdc611451	S, func=RR, N(R)=110; DSAP 0xd4 Group, SSAP 0xa6 Command
8	0.000000000	20:8b:b4:8f:64:71	3c:a3:e4:7b:e3:6f	LLC	3415	0x633c7f98	U, func=SAPP; DSAP 0xa4 Individual, SSAP 0xd8 Command
9	0.000000000	0e:01:99:28:6a:ae	a1:9f:e4:ca:01:41	LLC	4346	0xc9d27ca6	U P, func=Unknown; DSAP 0xde Group, SSAP ISO Network Layer (unofficial?)
10	0.000000000	02:ae:51:51:5c:fb	29:31:48:14:52:52	LLC	1948	0x9d26d846	I P, N(R)=10, N(S)=110; DSAP 0x54 Individual, SSAP 0x88 Command
11	0.000000000	e7:1e:14:63:3a:0c	ee:24:ff:fd:79:b3	LLC	3327	0x0ba826c6	S P, func=RR, N(R)=104; DSAP 0x1e Group, SSAP 0x9e Command
12	0.000000000	75:2b:0c:38:c6:14	8c:e9:ed:7c:14:d7	LLC	7585	0x81224933	S, func=RR, N(R)=67; DSAP 0xc2 Group, SSAP ISO Network Layer (unofficial?)

Frame 1: 8561 bytes on wire (68488 bits), 8561 bytes captured (68488 bits) on interface 0

Ethernet II, Src: 9f:1f:c7:a4:9d:e1 (9f:1f:c7:a4:9d:e1), Dst: 09:3f:0e:b6:28:bb (09:3f:0e:b6:28:bb)

Destination: 09:3f:0e:b6:28:bb (09:3f:0e:b6:28:bb)

Source: 9f:1f:c7:a4:9d:e1 (9f:1f:c7:a4:9d:e1)

[Expert Info (Marr/Protocol): Source MAC must not be a group address: IEEE 802.3-2002, Section 3.2.3(b)]

Address: 9f:1f:c7:a4:9d:e1 (9f:1f:c7:a4:9d:e1)

....1. = Locally administered address (this is NOT the factory default)

....3. = IG bit: Group address (multicast/broadcast)

Type: Jumbo LLC (0x8870)

Frame check sequence: 0xbe42713a [correct]

Logical-Link Control

Data (8539 bytes)

Data: a0b9c323bf8e91bdf5a58f7bda7bcca04a2435a38ef913a...

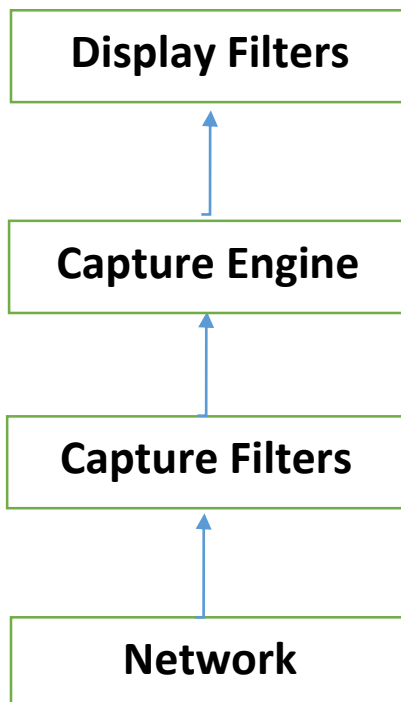
[Length: 8539]

```

2100 99 af 29 38 98 ec 7e fc 8a 17 30 71 ae 67 5d 4e ..l8.,.,. .8q.g]N
2110 8a 66 8a 3c 08 3e 7d 17 79 d3 90 da 38 b4 b0 c2 jf.<.>. y..B...
2120 f0 75 a4 45 b6 7a f9 ce 2b 7c a9 2f 58 e8 9f 90 .e.E.2.. +./X...
2130 95 3b 0f c8 b3 6f fa 1a eb e9 0b 63 97 96 c1 c4 .B..0...C...
2140 ad e6 7a 5b 1b de 6f 18 d7 54 83 ed 01 4e ef 2e ..2[.0..T...N..
2150 45 0d 42 54 58 0a 02 aa 51 25 49 d1 ac b5 49 e5 E.BTX...Q!...I.
2160 88 e3 c9 7d 2e 89 df 0b 97 3e 95 cc 93 de 42 71 ...).....>...B
2170

```

Ethernet checksum (eth.fcs), 4 bytes P... Profile: Default




Wireshark متوفر على انظمة الـ windows وعلى انظمة الـ mac وعلى انظمة linux
يمكنك استخدام برنامج wireshark على نظام الـ kali مباشرة.
يمكنك ايضا تنزيل برنامج wireshark على اي نظام تستخدمه من خلال الموقع التالي :

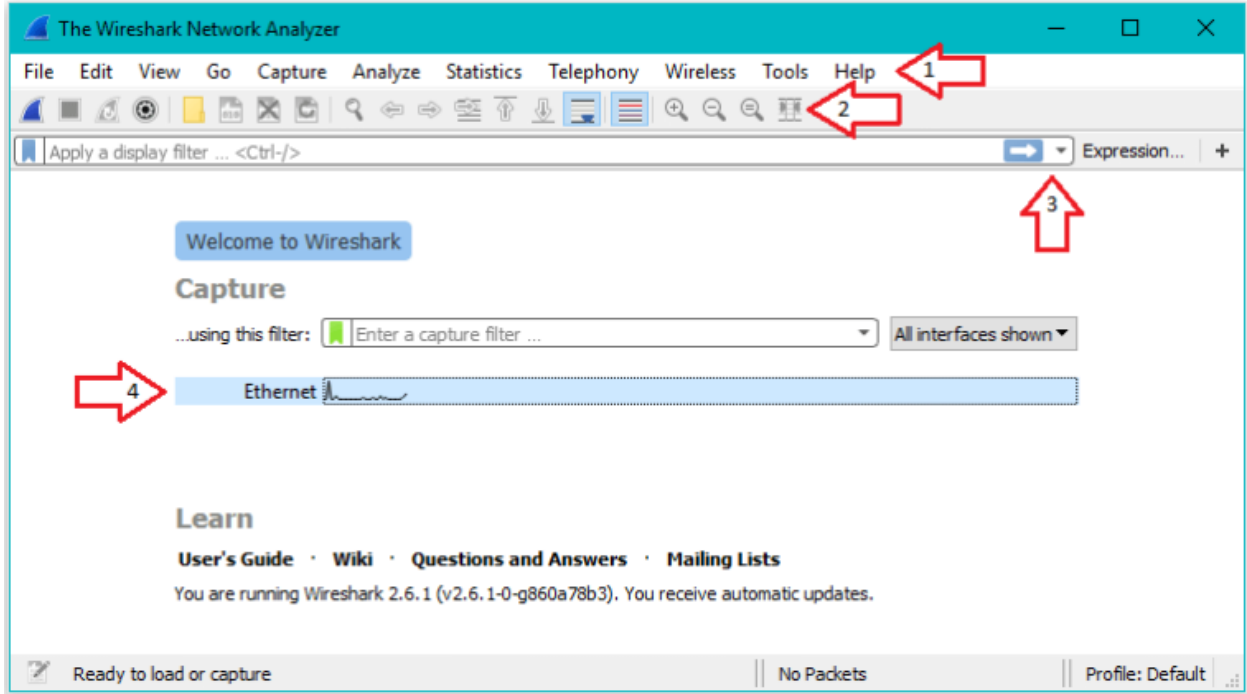
<https://www.wireshark.org/download.html>

Download Wireshark

The current stable release of Wireshark is 3.6.5. It supersedes all previous releases. You can also download the latest development release (3.7.0) and documentation.

Stable Release (3.6.5)	^
 Windows Installer (64-bit) Windows Installer (32-bit) Windows PortableApps® (64-bit) Windows PortableApps® (32-bit) macOS Arm 64-bit .dmg macOS Intel 64-bit .dmg Source Code	
Old Stable Release (3.4.14)	^
Development Release (3.7.0)	^
Documentation	^

قم بفتح برنامج الـ wireshark بعد ان قمت بتهيئته وستظهر لك في النافذة الرئيسية كل واجهات الشبكة الموجودة على جهازك :



Primary Areas of the Wireshark Start Screen

المناطق الأساسية لشاشة بدء Wireshark

1. The Menu - القائمة (القوائم)
2. The Main Toolbar - شريط الأدوات الرئيسي
3. The Filter Toolbar - شريط أدوات التصفية
4. The Interface List - قائمة الواجهة

The Menu

Wireshark's main menu, "The Menu," is located at the top of the window when run on Windows and Linux and the top of the screen when run on macOS.

في هذه القائمة عند تشغيلها على نظامي التشغيل windows و linux و اعلى الشاشة عند تشغيلها على نظام MacOS.

The Menu displays 11 different items : تعرض القائمة 11 عنصراً مختلفاً :

File

Open/Merge capture files, save, print, export, and quit Wireshark.

فتح / دمج ملفات الالتقاط وحفظها وطباعتها وتصديرها وإنهاء Wireshark

Edit

Find, time reference, or mark a packet. Handle configuration profiles. Set preferences.

ابحث عن حزمة أو مرجع زمني أو ضع علامة عليها. ملف تعريف تكوين المعالج. حدد التفضيلات.

View

Change display of capture data such as colorization of packets, showing packet in another window, zooming font, and collapsing and expanding trees.

تغيير عرض بيانات الالتقاط مثل تلوين الحزم ، وإظهار الحزمة في نافذة أخرى ، وتكبير الخط ، وانهيار وتوسيع الأشجار.

Go

Options to go to a specific packet

خيارات للذهاب إلى حزمة معينة

Capture

Edit capture filters and start and stop captures.

قم بتحرير فلاتر الالتقاط وابدأ وأوقف اللقطات.

Analyze

Alter display filters, configure user specific decodes, enable or disable dissection of protocols, and follow TCP streams

قم بتعديل عوامل تصفية العرض ، وتكوين فك الشفرات الخاصة بالمستخدم ، وتمكين تشريح البروتوكولات أو تعطيله ، واتباع تدفقات TCP

Statistics

Display statistic windows, summary of captured packets, protocol hierarchy stats, and more

عرض الإطارات الإحصائية وملخص الحزم الملتقطة وإحصائيات التسلسل الهرمي للبروتوكول والمزيد

Telephony

Display telephony related stats such as media analysis, flow diagrams, protocol hierarchy stats

عرض الإحصائيات المتعلقة بالاتصالات الهاتفية مثل تحليل الوسائط ومخططات التدفق وإحصائيات التسلسل الهرمي للبروتوكول.

Wireless

Display IEEE 802.11 wireless and Bluetooth statistics

عرض إحصاءات IEEE 802.11 اللاسلكية والبلوتوث

Tools

Various tools such as creating Firewall ACL rules

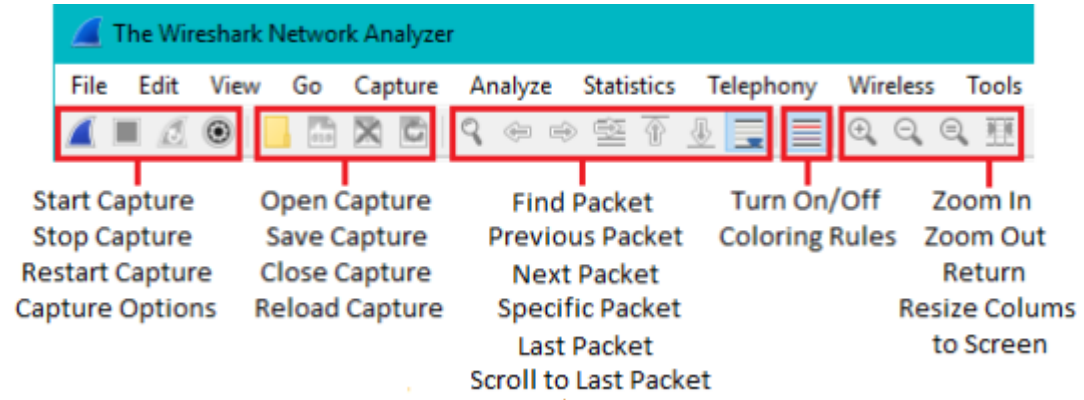
أدوات متنوعة مثل إنشاء قواعد قائمة التحكم في الوصول لجدار الحماية

Help

View basic help, manuals of command line tools, etc..

عرض التعليمات الأساسية ، كتيبات أدوات سطر الأوامر ، إلخ.

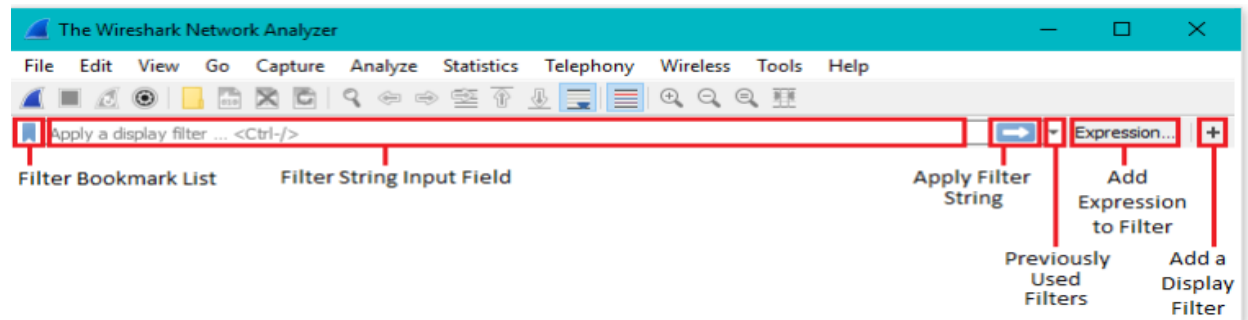
شريط أدوات Wireshark الرئيسي : Wireshark Main Toolbar



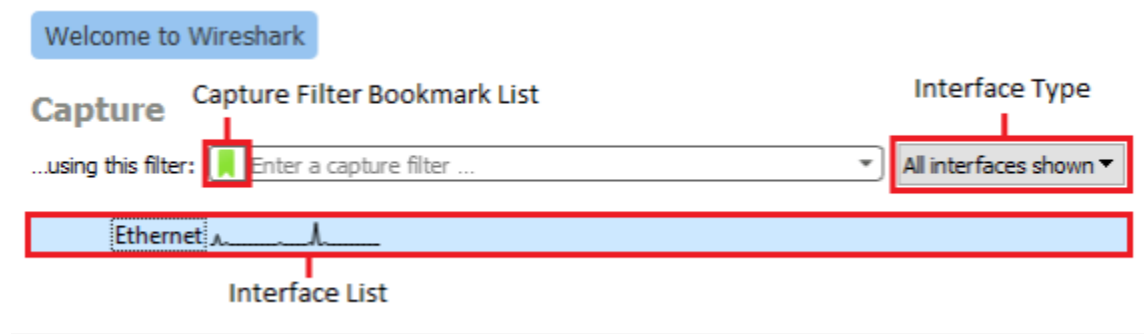
هذا شريط أدوات وصول سريع يوفر أزرارًا سهلة الاستخدام للوظائف الأكثر شيوعًا في القائمة الرئيسية. تصبح معظم هذه الأزرار نشطة فقط بعد تحديد واجهة للمراقبة.

Wireshark Filter Toolbar

يتيح لك شريط الأدوات هذا إمكانية تعديل عوامل تصفية العرض وتطبيقها بسرعة على ما تلتقطه. يتيح لك عوامل تصفية العرض تضيق نطاق الحزم التي التقطتها لتقتصر فقط على الحزم ذات الصلة بما تحاول رؤيته مثل مصادر عناوين IP والوجهات المحددة والبروتوكولات وعناوين MAC وما إلى ذلك .



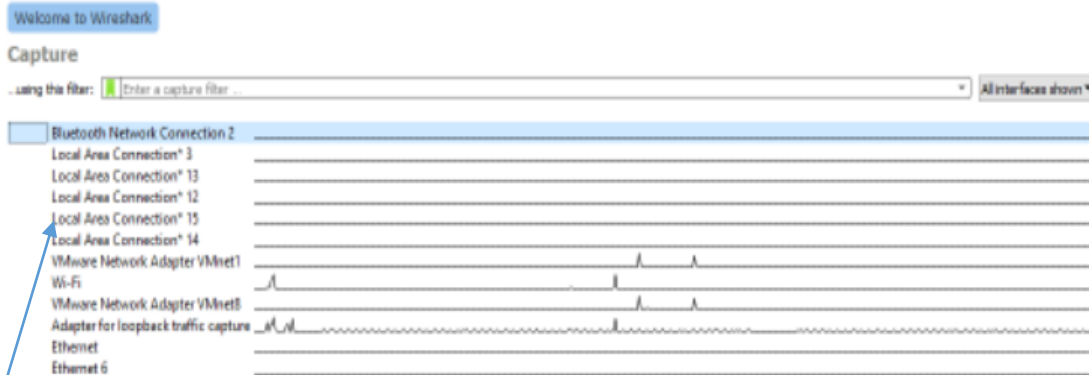
Wireshark Interface List



قائمة الواجهة هي المنطقة التي ستظهر فيها الواجهات التي قام جهازك بتثبيتها. قبل أن تتمكن من رؤية حزم البيانات ، تحتاج إلى اختيار إحدى الواجهات من خلال النقر عليها. يمكنك اختيار مرشح الالتقاط ونوع الواجهة لتظهر في قوائم الواجهات في هذه الشاشة أيضًا.

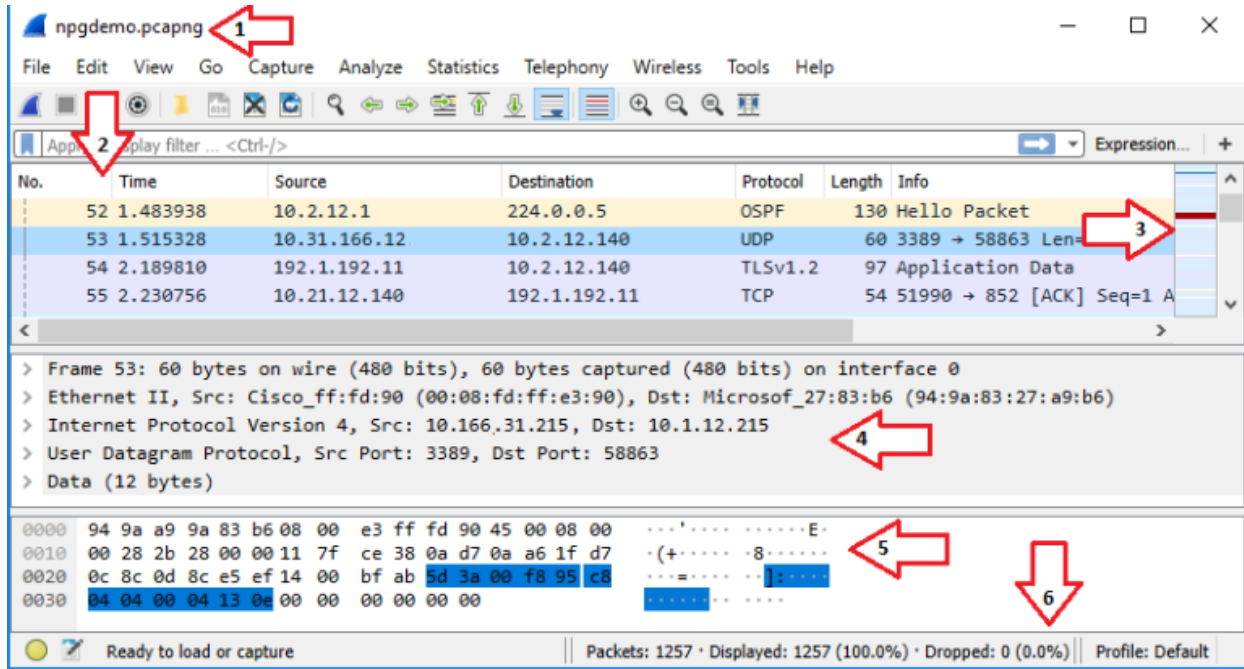
يؤدي النقر فوق ملف الالتقاط الموجود والواجهة أو فتحه إلى نقلك إلى شاشة العمل: ما يهمنا هنا واجهة الشبكة المستخدمة في الاتصال على الانترنت نختار طريقه الاتصال في الشبكة .

على فرض طريقة الاتصال هي wifi



نختار wifi اي طريقة الاتصال

ثم على الفحص ثم يبدأ بتحليل البيانات للشبكة ككل



Primary Areas of the Wireshark Working Screen:

Wireshark: المجالات الأساسية لشاشة عمل

1. Title Bar
2. Packet List Pane
3. Intelligent Scrollbar
4. Packet Details Pane
5. Packet Bytes Pane
6. The Statusbar

Wireshark Title Bar (Wireshark) شريط العنوان

يعرض هذا الشريط اسم الواجهة التي تلتقطها حتى تحفظ اللقطة. ثم سيظهر اسم ملف تفرغ الالتقاط. إذا قمت بفتح ملف التقاط محفوظ فسيتم عرض اسمه هنا.

Wireshark Packet List Pane

No.	Time	Source	Destination	Protocol	Length	Info
4	0.234943	10.2.0.3	10.2.0.255	UDP	305	54915 → 54915 Len=26
5	0.273809	10.2.0.4	239.255.255.250	SSDP	164	M-SEARCH * HTTP/1.1
6	0.377621	10.2.0.4	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
7	0.753440	34.17.21.139	10.2.0.3	TLSv1.2	121	Application Data
8	0.757435	10.2.0.3	34.17.21.139	TLSv1.2	1134	Application Data
9	0.806247	34.17.21.139	10.2.0.3	TCP	60	443 → 56237 [ACK] Seq=
10	0.807766	34.17.21.139	10.2.0.3	TLSv1.2	607	Application Data
11	0.851638	10.2.0.3	34.17.21.139	TCP	54	56237 → 443 [ACK] Seq=

يمثل كل سطر في هذا الجزء حزمة واحدة. بشكل افتراضي ، يتم تقسيم الجزء إلى 7 أعمدة ، يوفر كل منها بيانات تعريف مفيدة لكل حزمة ويمكن فرزها لمساعدتك على تشريح البيانات بشكل أفضل. يمكنك إزالة وإضافة وإعادة ترتيب الأعمدة لتناسب احتياجاتك. سيؤدي تحديد حزمة إلى إظهار المزيد من التفاصيل في جزء تفاصيل الحزمة وجزء حزم بايت.

يخصص العمود **No** "رقم" رقمًا فريدًا لكل حزمة. يمكنه أيضًا عرض رمز للمساعدة في تحديد العلاقة بين الحزم إذا نقرت على حزمة.

يعرض **Time** الطابع الزمني لوقت التقاط الحزمة. تنسيق هذا الطابع الزمني قابل للتخصيص.

Source يعرض عنوان IP أو عنوان MAC المصدر الذي نشأت منه الحزمة.

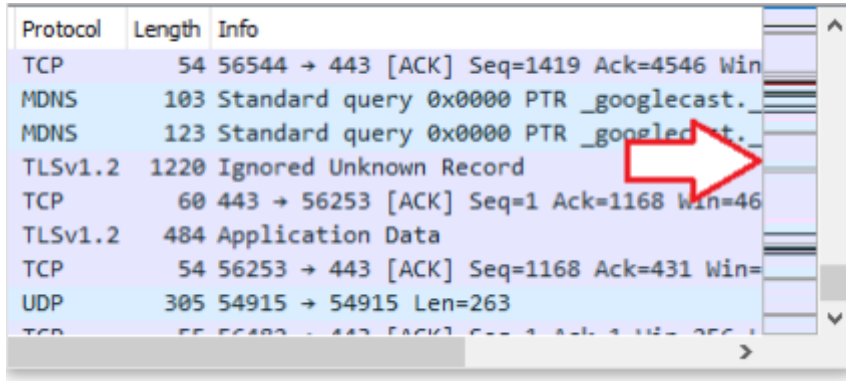
Destination يعرض عنوان IP أو عنوان MAC الوجهة الذي كانت الحزمة تتجه إليه.

Protocol يعرض معلومات البروتوكول المختصرة للحزمة.

Displays the packet length. **Length**

يعرض معلومات إضافية متعلقة بالحزمة. **Info**

Wireshark Intelligent Scrollbar (شريط التمرير الذكي Wireshark)



يوجد على يمين جزء قائمة الحزم شريط ملون يسمى شريط التمرير الذكي وهو عبارة عن خريطة مصغرة للحزم. كل سطر من شريط التمرير الذكي عبارة عن خط نقطي يمثل حزمة واحدة. يعتمد عدد الحزم المعروضة على ارتفاع القائمة ومواصفات شاشة العرض الفعلية.

تسهل هذه القائمة الانتقال إلى الحزم بناءً على التلوين. كما أنه يجعل من السهل تحديد مجموعات من أنواع معينة من الحزم خاصة إذا كنت تستخدم قواعد تلوين مخصصة.

Wireshark Packet Details Pane(جزء تفاصيل حزمة Wireshark)

```
> Frame 12: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interface 0
> Ethernet II, Src: Giga-Byt_39:72:72 (90:2b:34:2b:72:72), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.2.0.3 , Dst: 10.2.0.255
> User Datagram Protocol, Src Port: 54915, Dst Port: 54915
▼ Data (263 bytes)
  Data: 0047495200000000d00f5a53ad01000040b90f712f000000...
  [Length: 263]
```

عند النقر فوق حزمة في جزء قائمة الحزم ، يتم تحميل بيانات حول تلك الحزمة في جزء تفاصيل الحزمة. يعرض هذا الجزء بروتوكولات الحزمة المختلفة وحقول البروتوكول. يتم عرض هذه القائمة كشجرة يمكن توسيعها لإظهار المزيد من التفاصيل

يمكن أن تتضمن التفاصيل أيضًا حقلين خاصين ينشئهما Wireshark بمفرده من خلال تحليل الحزم. الحقلين هما الحقول والارتباطات التي تم إنشاؤها.

Generated Fields (تم إنشاء الحقول)

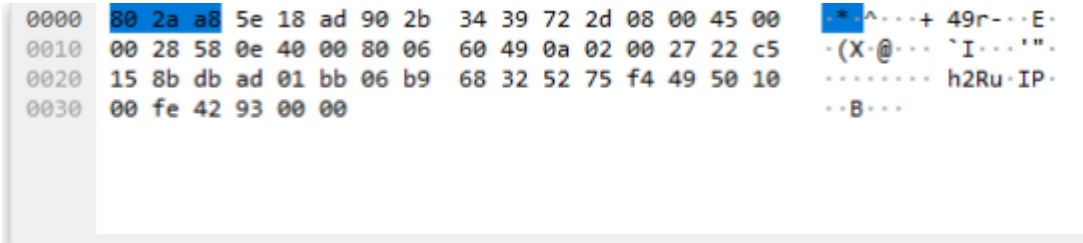
يتم وضع هذه المعلومات بين قوسين ([]) وتحتوي على معلومات مثل تحليل TCP ووقت الاستجابة والتحقق من صحة المجموع الاختباري وتحديد الموقع الجغرافي لـ IP.

Links (الروابط)

سيقوم Wireshark

بإنشاء ارتباط إذا اكتشف العلاقات بين الحزم. سيتم تنسيق هذه الروابط باللون الأزرق مع تسطير. سيؤدي النقر المزدوج على الرابط إلى الانتقال بك إلى الحزمة ذات الصلة هناك أيضًا قائمة سياق يمكنك الوصول إليها بالنقر بزر الماوس الأيمن داخل الجزء.

Wireshark Packet Bytes Pane (جزء حزم بايت Wireshark)



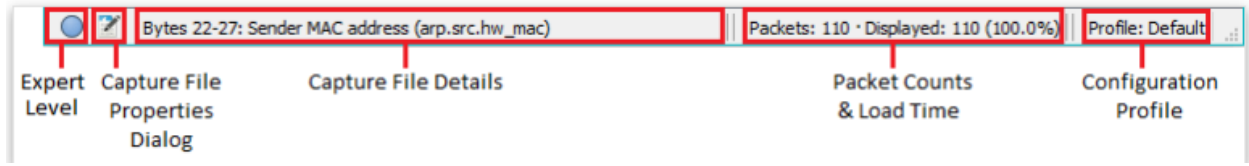
عند النقر فوق حزمة في جزء قائمة الحزم ، يتم تحميل بيانات حول الحزمة في جزء حزم البايت أيضًا. هذه البيانات في نمط تفريغ سداسي حيث يعرض كل سطر إزاحة تمثل الفترات بايت غير قابلة ASCII. البايتات ، 16 بايت سداسي عشري ، و 16 بايت للطباعة.

بتمييز البيانات Wireshark إذا حركت الماوس فوق جزء معين من البيانات ، فسيقوم المقابلة التي تراها في المثال أعلاه باللون الأزرق حيث يتم تمييز البايت السداسي مع وحدات المرتبطة ASCII بايت

تجميع بعض الحزم في جزء واحد أو يفك تشفير Wireshark من حين لآخر ، عندما يعيد البيانات ، سيكون هناك عدة صفحات مبنية أسفل جزء حزم البايت

هناك أيضًا قائمة سياق يمكنك الوصول إليها بالنقر بزر الماوس الأيمن داخل الجزء.

Wireshark Statusbar(شريط حالة البرنامج)



يحتوي شريط الحالة على رسائل إعلامية.

The Colorized Bullet

في أقصى يسار شريط الحالة يوجد رمز نقطي ملون يمثل أعلى مستوى خبير. عند وضع الماوس فوقه يعرض مربع معلومات الخبراء.

The Capture File Properties Button

على يمين الرمز النقطي الملون يوجد زر حوار خصائص ملف الالتقاط.

The Left Side

في معظم الحالات ، سيعرض الجانب الأيسر معلومات سياقية حول ملف الالتقاط مثل حجمه واسمه والوقت المنقضي. سيؤدي التمرير فوق تفاصيل ملف الالتقاط إلى إظهار المسار إلى الملف.

The Middle

سيعرض الوسط المعلومات المتعلقة بملف الالتقاط الحالي مثل عدد الحزم ووقت التحميل.

The Right Side

سيظهر اليمين ملف تعريف التكوين الحالي قيد الاستخدام.

إذا كنت تستخدم مرشح عرض به مشكلة ، فسيتم عرضه أيضًا في حقل تفاصيل ملف الالتقاط في شريط الحالة .

نأمل أن يكون هذا البرنامج التعليمي لواجهة Wireshark سهل الفهم وقد جعل Wireshark أسهل كثيرًا لفهمها والعمل معها. أوصي بتحميل Wireshark ، واختيار

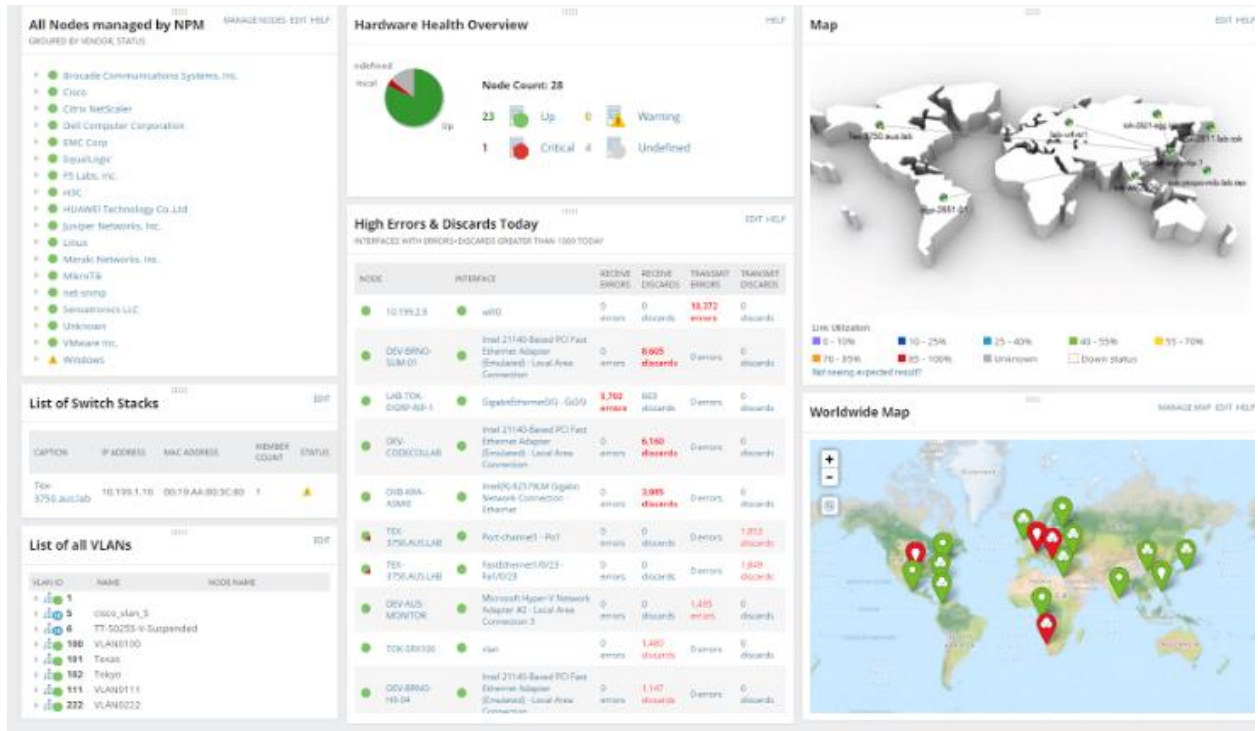
واجهة على جهاز الكمبيوتر الخاص بك ، والبحث فقط حول الواجهة والحزم. ستندهش من نوع البيانات التي سترأها تتقاطع.

Recommended for You: Solarwinds Network Performance Monitor (NPM)

هل تعرف صحة معدات الشبكات الخاصة بك؟ هل تعرف متى يحدث شيء ما قبل أن يبلغ المستخدم عن المشاكل؟ تعرف إلى أين يذهب عرض النطاق الترددي الخاص بك أو أين تفقد الحزم الخاصة بك؟

Solarwinds قم بأتمتة جمع البيانات والتنبيه للبنية التحتية للشبكات الخاصة بك باستخدام حتى تعرف بالضبط ما يجري في شبكتك ويمكنك النوم بسهولة NPM

على عكس الأدوات الأخرى ، فإن NPM جاهزة للخروج من منطقة الجراء مع معظم الماركات والنماذج الشائعة لمعدات الشبكات. لا تعبث بالقوالب المخصصة أو ملفات xml أو التعليمات البرمجية لاستخراج المعلومات المهمة.



بعد شرح البرنامج نأخذ امثله :

نرجع للصفحة الرئيسية ثم نختار كرت الشبكة الذي نعمل عليه ثم نعمل فحص

The image shows a Wireshark interface with a list of network packets. The selected packet (No. 1299) is a TLSv1.2 Application Data packet. Below the list, the packet details pane shows the following layers:

- Frame 1299: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface 0
- Ethernet II, Src: dc:a6:32:7e:e8:f7, Dst: 5c:1a:6f:d6:a3:40
- Internet Protocol Version 4, Src: 192.168.1.8, Dst: 34.231.253.113
- Transmission Control Protocol, Src Port: 36260, Dst Port: 8883, Seq: 98, Ack: 1, Len: 97
- Secure Sockets Layer
 - TLsv1.2 Record Layer: Application Data Protocol: mqtt

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 5c 1a 6f d6 a3 40 dc a6 32 7e e8 f7 08 00 45 00  \o: @ 2... E.  
0010 00 95 ec 55 40 00 40 06 6c 04 c0 a8 01 08 22 e7  ...U@ 1...."
```

سنرى كم كبير من البروتوكولات المرسله عبر الشبكة مثل ARP ,UDP ,TCP وغيرها لإيقاف عملية الالتقاط والرجوع الى الصفحة الرئيسية نضغط على زر الإيقاف stop ثم من قائمة file نضغط على close .

يمكننا استخدام عوامل الفلتره الموجوده في اعلى الصفحة لالتقاط حزم بروتوكول معينه مثلاً لالتقاط حزم ال ping يمكننا إضافة بروتوكول ICMP للفلتر وتطبيقه على واجهه الشبكة كما في المثال التالي :

ابدأ عملية التقاط جديدة ثم اكتب icmp في عامل الفلتره ثم ابدأ البحث بالنقر مرتين على واجهه الشبكة .

بإستخدام الcmd اكتب ping على موقع جوجل لتجربة ال ping

```

Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. All rights reserved.

C:\Users\belal>ping google.com

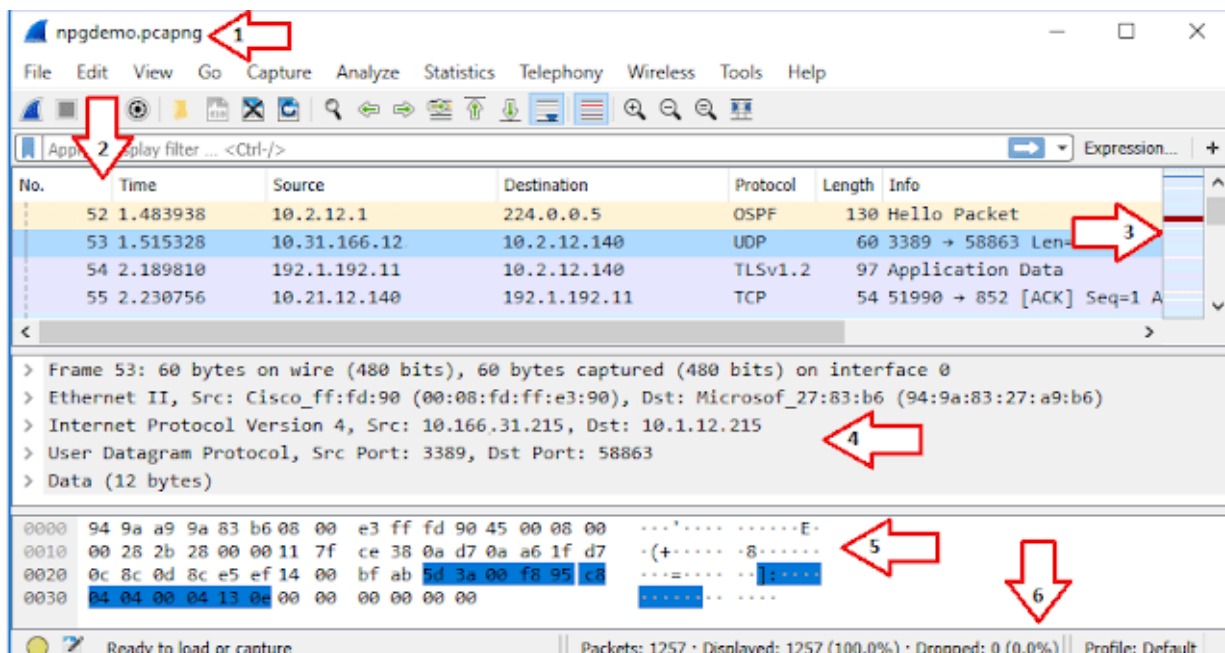
Pinging google.com [142.250.185.238] with 32 bytes of data:
Reply from 142.250.185.238: bytes=32 time=79ms TTL=57
Reply from 142.250.185.238: bytes=32 time=74ms TTL=57
Reply from 142.250.185.238: bytes=32 time=91ms TTL=57
Reply from 142.250.185.238: bytes=32 time=74ms TTL=57

Ping statistics for 142.250.185.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 74ms, Maximum = 91ms, Average = 79ms

C:\Users\belal>

```

ثم راقب حركة البيانات التي ستبدأ بالظهور في واجهة برنامج wireshark.



ستلاحظ حركة البيانات في الشاشة الرئيسية من المصدر الى الوجهة في كل حزمة تم ارسالها باستخدام بروتوكول icmp.

المثير للاهتمام ايضاً الخانة الوسطى في الشاشة الرئيسية والتي تحتوي على اربع اسطر في حالة البحث الأخيرة .

فعند التقاط حركة البيانات سيقوم wireshark بالتقاط ال header لكل الحزم ، هذه الاسطر تمثل ال header لكل طبقة من طبقات نقل البيانات وستحصل على معلومات كبيرة عن كل حزمة خطوة بخطوة من لحظة ارسال الحزمة حتى استلامها في كل طبقة. في الخانة الأخيرة في الصفحة الرئيسية يمكننا رؤية البيانات الفعلية المرسله والمستقبله لكل حزمة وبياناتها المشفرة.

يمكننا رؤية مثال اوضح عن رؤية تلك البيانات عند ارسال طلب GET عبر بروتوكول ال http، مثلاً، وسترى البيانات المجابة من الخادم الذي طلبت منه تلك الصفحة.

تمرين :

1 : حاول التقاط حزم ICMP المرسله والمستقبله على الموقع yahoo.com ؟

2 : حاول التقاط حزم HTTP من خلال زيارة احد العناوين التي تدعم التصفح عبر بروتوكول ال HTTP ماذا تلاحظ ؟ ما المعلومات التي تستطيع الاطلاع عليها من خلال استماعك لهذه الحزم؟

التقاط حزم HTTP

ابدأ عملية التقاط جديدة ثم اكتب http في عامل الفلترة ثم ابدأ البحث بالنقر مرتين على واجهة الشبكة .

ثم دعنا نجرب الدخول الى أي من المواقع التي تعمل بروتوكول http مثل :

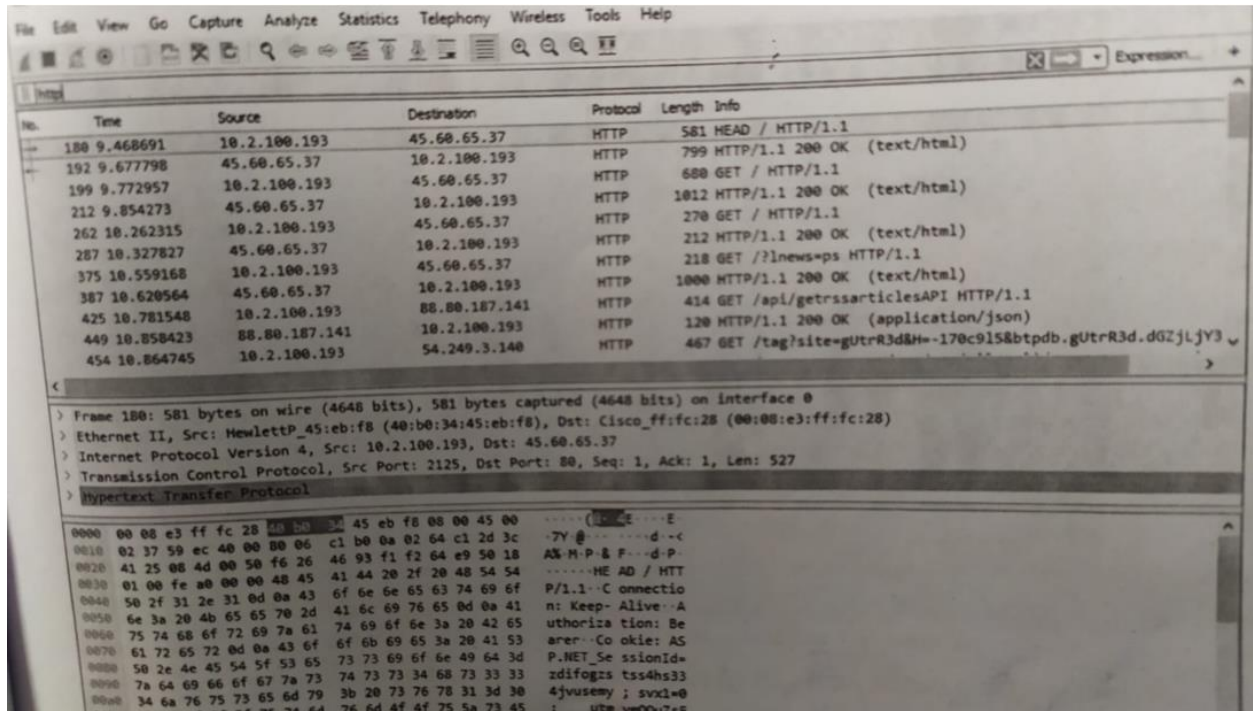
<http://site.moh.ps>

<http://social.ipoke.co/social-pages/websites>

http://www.pcbs.gov.ps/site/lang_ar/632/default.aspx

<http://www.pmd.ps>

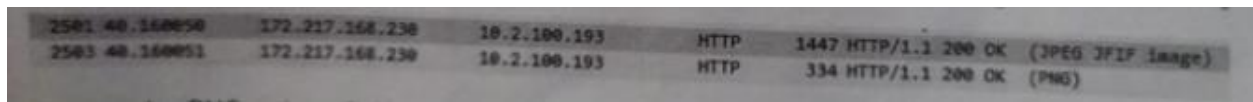
انظر الى صفحة الموقع الذي قمت بفتحه ثم ارجع الى برنامج ال wireshark



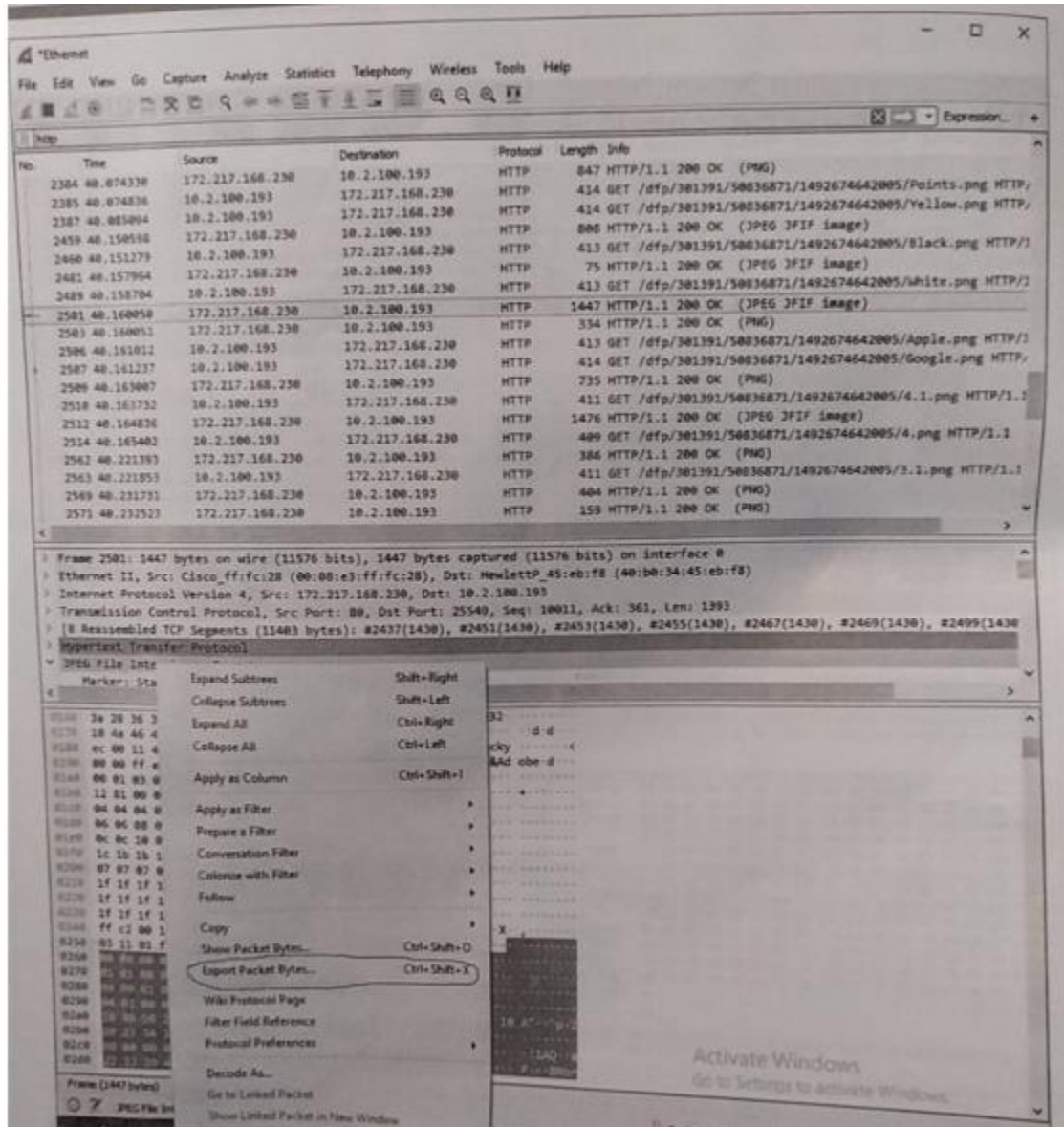
يمكنك الاطلاع على تفاصيل كثيرة من خلال تفحص الحزم المستقبلية والمرسلة الى الموقع ، كما يمكننا استغلال معلومات حساسة يتم نقلها عبر بروتوكول الـ http فيمكننا الاطلاع على رد الصفحات والمعلومات المرسلة الحساسة مثل اسم المستخدم وكلمة المرور وايضا الى جميع الكائنات او الملفات التي تم ارجاعها من الموقع .

في المثال السابق ستلاحظ وجود كم كبير من المعلومات التي ترجعها الصفحة مثل الصور والملفات التي تظهر في الموقع .

يمكنك ملاحظة نوع الملف المرجع من خلال نوع الملف ونوعية الرد مثل :



من الصورة السابقة ستدرك انها صورتان : صورة من نوع JPEG وصورة اخرى من نوع PNG هل بإمكاننا التقاط تلك الصورة وحفظها ؟ نعم ، يمكننا الضغط على الحزمة من نوع الصورة او الملف المراد تخزينه ثم اضغط بالزر الايمن على JPEG file interchange format ثم اختر من القائمة المنسدلة Export packet bytes ثم احفظه باسم الملف ونوعه في المكان المراد حفظه.

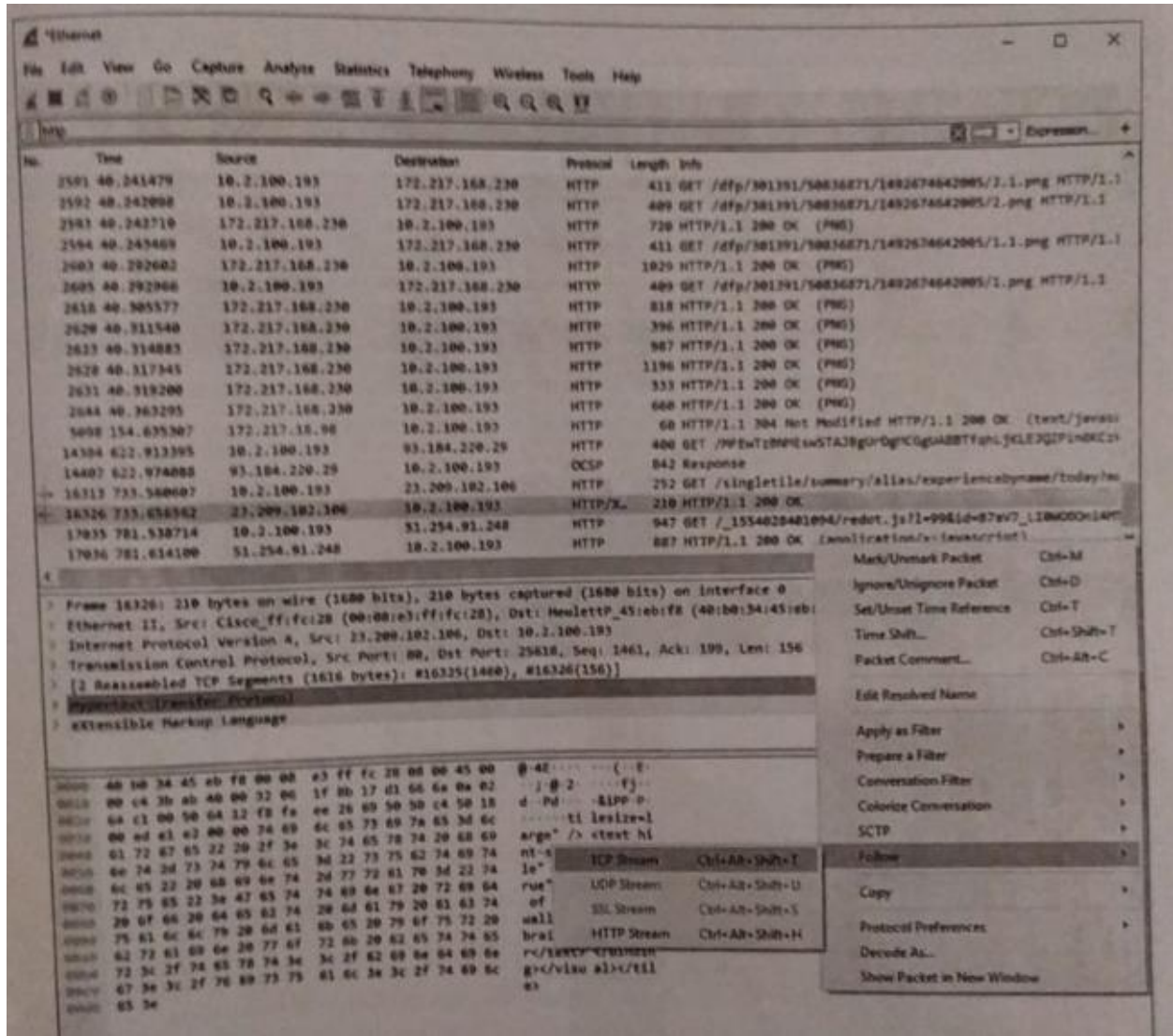


اذهب الى الموقع الذي حفظت فيه الملف (الصور مثلا) وافتح الصورة للتأكد بانه تم حفظ الصورة بنجاح.

يمكنك ايضا الاطلاع على ال tcp stream لصفحات الويب الملتقطة.

اختر أيا من الحزم الملتقطة http ثم اضغط بالزر اليمين على الحزمة ثم اختر :

Follow->TCP Stream



وستظهر لك صفحة جديدة تعرض لك سيل المعلومات من كل طلب تم طلبه وتمت الإجابة عليه.

يمكنك معرفة الكثير من المعلومات من خلال تصفح تلك الصفحات من الـ TCP Stream

التقاط معلومات عند تسجيل دخول المستخدم :

باستخدام خاصية التقاط الحزم وفلتره حزم الـ http يمكننا معرفة معلومات حساسة مثل تفاصيل تسجيل مستخدم الى اي موقع يستخدم بروتوكول الـ http كما في المثال التالي :

ابدأ جلسة wireshark جديدة واضف عامل تصفية الـ http ثم اذهب الى العنوان التالي :

<http://testphp.vulnweb.com/login.php>

قم بادخال معلومات الدخول الى الموقع (يمكنك ادخال معلومات غير حقيقية فهدفنا رؤية معلومات التسجيل) ثم اضغط على زر الارسال submit .

انتقل الى شاشة wireshark وابحث عن الحزمة التي تشير الى ارسال معلومات المستخدم الى السيرفر، يمكنك ملاحظة الحزمة التي تم ارسالها عبر البروتوكول واسلوب الارسال ، فغالبا ما يتم ارسال معلومات التسجيل عبر post :

اضغط بالزر اليمين على تلك الحزمة ثم اختر follow: TCP Stream ، ستظهر شاشة مشابهة للتالي :

```
Follow TCP Stream (tcp.stream eq 15)
Stream Content
GET / HTTP/1.1
Host: www.wireshark.org
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/35.0.1916.153 Safari/537.36
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Cookie: __cfduid=dd903204a3f4e4c45f81c3d0d156356551401056698086;
__utma=87653150.1222912745.1401056681.1404072442.1404077419.15; __utmb=87653150.5.10.1404077419;
__utmc=87653150; __utmz=87653150.1403815183.9.6.utmcsr=google|utmccn=(organic)|utmcmd=organic|
utmctr=(not%20provided)

HTTP/1.1 200 OK
Server: cloudflare-nginx
Date: Sun, 29 Jun 2014 22:16:11 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
X-Mod-Pagespeed: 1.7.30.5-3847
Vary: Accept-Encoding
X-Slogan: Be good. You never know who's running Wireshark nearby.
Cache-control: max-age=0, no-cache, no-store
CF-RAY: 14257cb0d5fb0d1f-ATL
Content-Encoding: gzip

2af
.....LS..6.)..B..%.En..A.v.....h..X0...."Yr".0.]y.....9C.....^L.....}
{3...U4AZ..V--..g.....|H...S.....l...h.D $1..V'.s5...4.
{.V:).w.7.1e....Z=xw01.....)!;}....FH...e...|-
.zY..DeMrb..V...L.6.US...Q...gM.
Y.qv...u....X..SmEE..w....Z...jU.U..).m...W...0st...m...g$.ws...b...V..E...t...
{X...</1...NK54k...S...&...xAZ...rt...u.Bm.#.../
J...<.1...:."M3...~?..wfy..r..a...'.D...9...%...0.....6.0..f2
[.Zn3' |...V...8.....6...t...5[.....B.....i..].M...7.g.H...m.Q...Q-^..Q.
t..e...i.....w.....
```

انظر الى المكتوب بالخط الاحمر وستجد غالبا المعلومات التي ادخلتها بنفسك في معلومات التسجيل امامك.

من الامثلة على المواقع التي تستخدم بروتوكول ال- http

<http://www.bbc.com/arabic>

<http://www.arabcoders.ae/>

<http://www.baheth.info/>

<http://www.arabic-keyboard.org/photoshop-arabic/>

<http://www.techpanda.org/>

تدريبات

قبل التدرّب على ملفات عملية الالتقاط حزم حقيقية موجودة على موقع wireshark قم بزيارة المواقع التالية المفيدة التي يمكنك التدرّب من خلالها على wireshark .

<http://www.malware-traffic-analysis.net/>

<https://unit42.paloaltonetworks.com/unit42-customizing-wireshark-changing-column-display/>

يمكنك تجربة عمليات التقاط لحزم من كل الانواع من خلال عينات الالتقاط :

<https://wiki.Wireshark.org/SampleCaptures>

اطلع على العينات التالية :

Telnet

Viruses and worms

Lightweight directory access protocol(LDAP)

SNMP

Routing Protocols

تمرين

باستخدام Wireshark وال- virtual box

قم بالتقاط كلمة المرور التي تستخدمها في الدخول الى خادم Ubuntu عبر برنامج ال-puTTY وبروتوكول ال-Telnet وقم بتصوير النوافذ المتعلقة بالتقاط الحزم وبشاشة الاتصال واكتب ملاحظاتك.

التتبع tracking

هناك العديد من الطرق لتتبعك على شبكة الانترنت طرق مختلفه واسباب مختلفه

عند زياره موقع محدد سواء كان فيه معلومات دخول ام لا قد يتتبعك ذلك الموقع **مثال**: اذا زرت موقعا ووجدت فيه زر الإعجاب الخاص بفيسبوك: توقع ان فيسبوك يتتبعك والمواقع مثل جوجل وياهو يتتبعوك ايضا اذا استخدمت اي موقع يستخدم الخدمات المقدمه مثلا من جوجل.

يجب ان تعلم ايضا ان مزود بريدك الالكتروني بطبيعته قادر على قراءه رسائلك وبريدك الالكتروني وسيكون قادرا على تتبع المواقع التي تقوم بزيارتها (ان كان هناك رابط يربط الموقع رجوعا الى البريد الالكتروني) نخص بالذكر خدمه Gmail

من جوجل والتي تقوم بقراءه وتحليل معلوماتك الشخصيه ورسائلك لاطهار الاعلانات المناسبه لك.

لا حاجه ايضا للقول ان مزود خدمه الانترنت ايضا قادر على تتبعك ومعرفه كل استعلام DNS يقوم به جهازك للولوج الى موقع انترنت بعض الحكومات تجبر مزودي الانترنت بتسجيل كل العناوين التي يقوم المستخدم بزيارتها.

العمل ,الجامعه, المدرسه.....الخ كل تلك الجهات على الأغلب تقوم بتسجيل كل عناوين المواقع التي تقوم بزيارتها في عمالك او جامعتك حتى انها تسجل محتويات تلك المواقع بقيامك بزياره مواقع تستخدم بروتوكولات تشفير مثل https او TLS

مثل قد يصعب ذلك المهمه ولكن باستخدام الادوات المناسبه لن يجعل ذلك مستحيلاوفي حال وجود برنامج مراقبه عن بعد مثبت على جهازك فلن يشكل ذلك فرقا (استخدام بروتوكولات تشفير) فسوف يتمكنون من الاطلاع على المعلومات على جهازك مثلما تنظر اليها انت.

لا حاجه ايضا لذكر ان كل معلوماتك التي ترسلها او تستقبلها من خلال شبكه Wi-Fi عامه ستراقب وسيتم تتبع عناوين الانترنت التي قمت بزيارتها وتسجيلها.

Man-in-the-Middle هو مثال واضح عن عمليه التتبع فاي شخص بإمكانه ان يكون في منتصف الاتصال بإمكانه تتبع وتسجيل المعلومات التي يتم تبادلها عبر تلك الشبكه.

عناوين الـ IP

الشيء الأساسي الذي يمكن التعرف عليك من خلاله على الإنترنت هو عنوانك المنطقي IP- Address. فإي اتصال تقوم به على الإنترنت يتطلب وجود IP Address في حال إجابته الطلبات التي تقوم بها عناوين أخرى على الإنترنت وهو جزء من عملية الـ TCP (طلب وإجابته) البروتوكول الذي يعمل عليه الإنترنت.

قم بزيارته الموقع التالي :

<https://whatismyipaddress.com/>

وسيفيظهر لك عنوان IP مخالف عما كنا نراه من خلال الأمر ipconfig (على الويندوز)

The screenshot displays the website's interface with the following information:

- My IP Address is:**
 - IPv4: 41.25.36.103
 - IPv6: Not detected
- My IP Information:**
 - ISP: Mada AlArab Ltd
 - City: Ramallah
 - Region: Ramallah
 - Country: Palestine, State of
- Warning:** Your private information is exposed!
- Buttons:** HIDE MY IP ADDRESS NOW, Show Complete IP Details
- Map:** A map showing the location in Ramallah, Palestine, with a red pin and a tooltip that says "Click for more details about".
- Map Legend:** Location not accurate? Update My IP Location

سيظهر لك الموقع عنوانك الجغرافي اسم الدولة والمدينة بالإضافة إلى خريطة تحتوي موقعك الجغرافي التقريبي هل لاحظت ذلك من الإعلانات تبدو كأنها تعرف تماماً أين تقيم؟ تلك المعلومات كلها يمكن معرفتها من خلال عنوانك المنطقي IP Address

عنوان الـ IP في الحقيقة ينتمي إلى الـ Router الخاص بك والذي تم تزويده من قبل الـ ISP الخاص بك هذا العنوان يتغير بشكل ديناميكي كل فترة معناه وعادة ما يبقى العنوان بدون تغيير حتى يتم فصل موجهك وإعادة تشغيله.

لا تخط بين عنوانك المنطقي المحلي Local or enteral IP Address مع العنوان

المنطقي العام Public or external IP Address العنوان المنطقي العام هو العنوان

الذي سيعرفك على الانترنت .

فصل العناوين داخلي وخارجي هل هو شيء جيد ؟

نعم بهذه الطريقة لن يتمكن اي جهاز خارج شبكتك من الوصول اليك الا من خلال ال-Router (من خلال بروتوكول ال-NAT) والذي يضيف طبقة حماية اضافية.

اتصالات الطرف الثالث:

عند طلب موقع معين لا يتوقف الامر عن عنوان او مصدر واحد ذلك الموقع سيطلب عدد من الطلبات الاضافيه عبر عدد من الروابط الى مواقع اخرى.

يمكننا رؤيه ذلك بشكل واضح اذا استخدمنا اداة Burp Suite والمتوفره على اللينكس كالي بشكل افتراضي وعلى ويندوز اذا ذهبت الى موقع البرنامج لتحميله.

ما هي اداة BURP Suite

اداة Burp Suite وهي اداة اختراق وحمايه متاحه لكل نظام اللينكس، ال-Mac OS

وايضا الويندوز تم تطويرها من طرف شركة Portswigger وهي برمجية متاحة بـ 3

نسخ منها ال- Professional وال- Enterprise و ال- Community ، كل من نسخة

Pro و Enterprise مدفوعتين ويمكن تجربتهما بالمجان لفترة محدودة ، ونسخة

Community متاحة بشكل مجاني مع نقص في بعض البرمجيات والخصائص.

في الغالب نجد نسخة ال- Community في أنظمة مختلفة جاهزة كنظام kali Linux.

أداة Burp Suite هي أداة إختراق لتطبيقات الويب وتعتمد على عدة تقنيات تؤهلها لتصير

كذلك وتعتبر واحدة من أشهر أدوات الإختراق في العالم لذلك.

استخدامات اداة ال- Burp Suite :

تاتي اداة الاختراق Burp Suite محمله بمجموعه من التقنيات الثانويه التي تؤهلك لهدف

واحد ووحيد وهو اختبار اختراق تطبيقات الويب والمواقع بالدرجه الاولى تستطيع هذه الاداه

كشف اي لبس في المواقع او اي مشكله في الاتصال والوصول للموقع من طرف المستخدم.

تستطيع اداة Burp Suite التنصت واعتراض اي اتصالات عابره للموقع ويمكنها عمل

فحص شامل لاي موقع او تطبيق ويب واستخراج اهم نقاط الضعف الخاصه به (مثل شهادات

الأمان SSL تقنيات الكوكيز ان كانت تسبب اي ضرر للمستخدم...)

حتى انها تكشف الثغرات الموجودة في المواقع ايضا وتستطيع اداة Burp Suite محاكاة هجوم على مواقع وتطبيقات الويب عبر عدة تقنيات من اجل كشف قوه مواقع الويب بل والاداه اكثر تطورا وذكاء ايضا اذ انه يمكن استخراج كل الملفات الموجوده في اي تطبيق ويب من صور ,فيديوهات,ملفات ميديا او حتى سكريتات (ملفات كتابيه سواء كانت كود او اي نوع اخر من الملفات).

ولأنه في تطبيقات الويب يتم الاعتماد على التشفير كثيرا يوجد تقنيات في الـ Burp Suite تمكنك بشكل اكبر من فك تشفير هذه الاكواد (صوصا اكواد الجافاسكريت) كما يمكنها استخراج ملفات الـ Session و Cookies احيانا في المواقع التي تطبق عليها برمجيه . Burp Suite

اهم الادوات المكونه لبرمجه Burp Suite واستخداماتها:

ما يجعل اداة الـ Burp Suite اداة قويه حقا هو مجموعه الادوات والتقنيات الثانويه الموجوده مسبقا في الاداه نفسها الادوات التي تفرق بين النسخه المجانيه والنسخ المدفوعه من الاداه كذلك معظم هذه الادوات قد تجدها مسبقا في النسخه المجانيه والبعض الاخر متاح فقط في النسخ المدفوعه.

اداه Scanner وسط الـ Burp Suite وتعتبر الاكثر فتكا في اداة Burp Suite بشكل عام غير متوفره في النسخه المجانيه تسمح لك هذه الاداه بالبحث الشامل في الموقع عن اي نوع من الاخطاء والثغرات التي يمكن استخدامها ويبقى الفحص لمدته طويله حسب نوع وتفرع الموقع.

اداه Burp Intruder من الادوات التي ستعجبك كذلك هذه الاداه تقوم بتنفيذ هجمات محتمله على الموقع من هجمات ...لتخمين كلمات السر الى هجمات الـ Sql Injection على روابط تطبيق الويب وتعمل الاداه بشكل ادق في تغيير تكوينيه الـ Http Request بحيث تقوم باضافه والتعديل على روابط الـ Http Requests الى حين ايجاد نوع محدد من الاخطاء او الثغرات.

اداه Target هي اداة متاحه في النسخه التجريبيه من البرمجيه وتوفر لك هذه الاداه كل المعلومات التي تحتاج حول تطبيق الويب او الموقع الذي تريد استهدافه بحيث تجلب لك كل المعلومات التي تحتاج من خوادم الـ DNS معلومات حول النطاق معلومات حول المنصه المستخدمه في تطبيق الويب ومعلومات كثيره يمكننا تعريف هذه الاداه كأداة جمع المعلومات حول هدف محدد.

اداه Decoder وكما يشير الاسم الخاص بها فالهدف منها هو فك تشفير النتائج او ال Burp Suite التي يتم تحصيلها اثناء ارسال الطلب (Request) محدد والتوصل بالنتائج بشكل مشفر لا تتعب نفسك في محاوله فك تشفيرها فقط قم باستخدام اداة Decoder الموجوده مسبقا في ال- Burp Suite وستؤدي العمل.

اداه Proxy وتعتبر اشهر اداة في ال- Burp Suite بصفه عامه يمكننا تعريفها كبرمجيه Man in the Middle بين المتصفح والخادم بحيث تقوم بالتجسس على كل البيانات التي يتم ارسالها واستقبالها وتبادلها بين كل من المتصفح والخادم اي عندما تنقر عبر الدخول لموقع معين يتم ارسال واستقبال طلبات تقوم اداة Proxy باظهارها لك كلها في البرمجيه.

اداه Repeater هي اداة تسمح لك بالتلاعب بالقيم الموجوده في الروابط الخاصه بالمواقع عند القيام بعمليات ال- GET مثلا بافتراض ان رابط موقع مثلا website.com/user/1 يجلب لنا المستخدم رقم 1 فان هذه الاداه ستبدأ بالتلاعب بالارقام الى ان تصل مثلا الى نتيجته محدده مثلاوهنا نعرف ان عدد المستخدمين هو 256 مستخدم في الموقع يمكن بالطبع التلاعب بها بميزات هائله وكثيره.

اداه Click bandit تعتمد هذه التقنيه على توليد اكواد يمكن ادراجها في الموقع من اجل تحصيل عمليات ال... ان لم تكن لديك فكره عن ال- Clickjacking فهي اضافات يتم اضافتها في موقع محدد بشكل خفي بحيث تتبع تحركات المستخدم وعندما ينقر في الصفحه تقوم بعمل محدد اشتهرت كثيرا بين مستخدمي المواقع لجلب اعجابات لصفحاتهم على فيسبوك بحيث يتم اضافه زر لايك للصفحه بشكل خفي يلاحق سهم الفأره وفور النقر سقوم المستخدم بعمل اعجاب للصفحه دون ان يدري.

اداه Extender تسمح لك ببساطه باضافه ادوات جديده واطافات جديده للبرنامج بحيث تقوم الشركه المطوره بنشر برمجيات بين الحين والآخر يمكن ادراجها للبرنامج عبر ال- Extender اعتبارها مثل اطافات المتصفح (Extensions).

من يمكنه استخدام Burp Suite؟ وكيف؟

منصه Burp Suite بالرغم من وجود نسخ مدفوعه فيها الا انه يمكن للجميع الوصول للنسخه المجانيه التي توفر مجموعه من الادوات القويه وهذا يعني انه يمكن لاي شخص استخدام Burp Suite الا ان الاداه شهيره اكثر بين صفوف مختصي الحمايه في الشركات الكبرى والشركه المطوره لمواقع الويب بحيث يتوجب على فريق الفحص التقني تمريراي

برمجية ويب من اداه Burp Suite للتأكد من صلابتهما وصعوبه اختراق او اظهار اي معلومات عن ضعف تطبيق الويب.

يحتاج اي فريق مطور لموقع من الصفر تمرير موقعه من Burp Suite حتى لا يتعرض للاختراق مستقبلا على الكفه المقابلة يمكن ايضا للمخترقين استخدام الاداه من اجل كشف اي لبس /خطأ/ثغره/Exploit/Glitch في تطبيق ويب معين فاي اختلال يمكن استخدامه اما للبدئ في استخدام Burp Suite فيكفي التوجه للموقع الرسمي وتحميل الاداه بما يتوافق مع نظامك الخاص والبدئ في استخدامها.

لإعداد Burp للعمل على متصفح الـ Firefox إذهب الى الرابط التالي واتبع التعليمات:

<https://support.portswigger.net/customer/en/portal/articles/1783>

[066-configuring-firefox-to-work-with-burp](https://support.portswigger.net/customer/en/portal/articles/1783)

<https://portswigger.net/burp/documentation/desktop/external-browser-config/browser-config-firefox>

or

<https://portswigger.net/burp/documentation/desktop/penetration-testing-configuration-your-browser>

Http Referrer

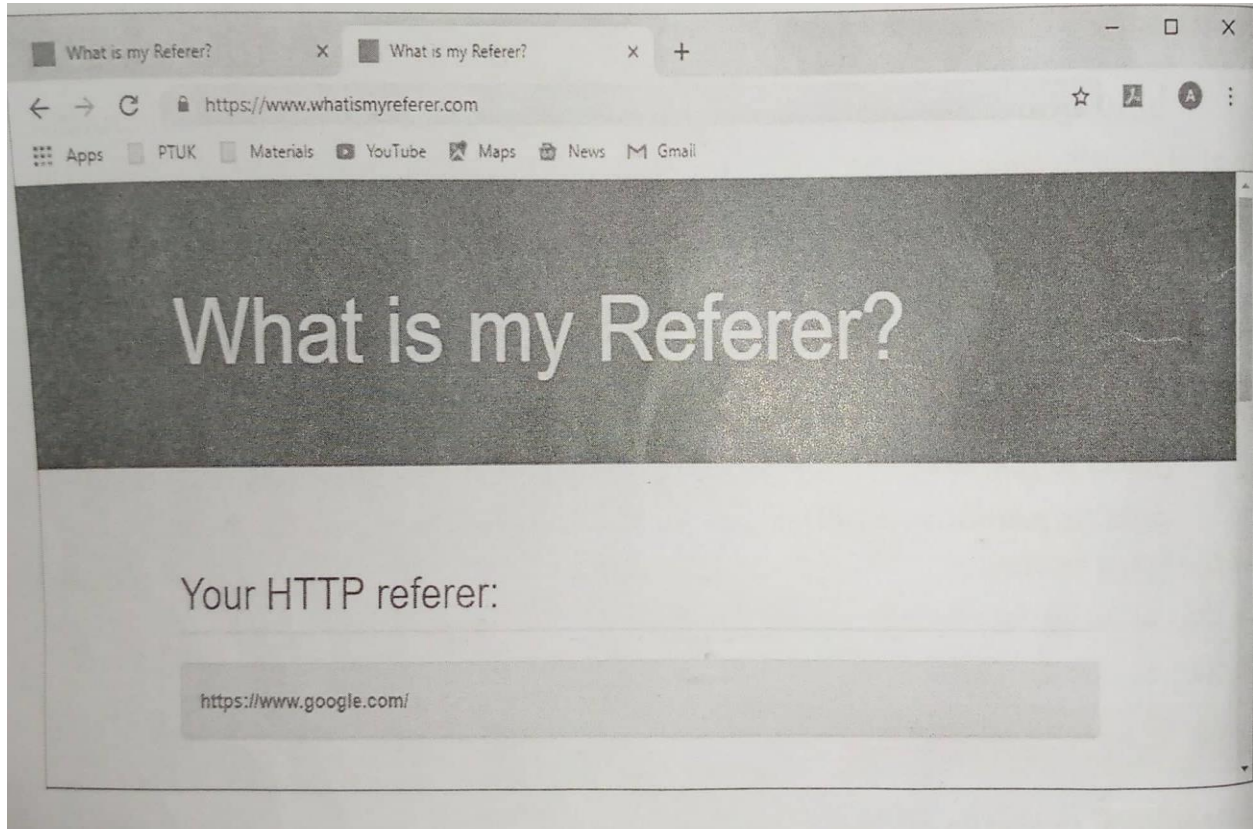
يمكن تتبع الصفحات التي ترسلك من موقع معين الى اي موقع اخر من خلال المعلومات التي يرسلها الموقع الذي ارسلك هناك او من خلال الـ Cookies

فعند بحثك عن شئ معين من خلال موقع البحث من جوجل عند اختيارك لأي نتيجة بحث وارده في بحثك سيعلم الموقع الذي ذهبت اليه من خلال اي موقع وصلت اليه مثال :

ابحث عن ... من خلال جوجل ثم اضغط على اول نتيجة بحث

Whatismyreferer.com

عند وصولك للموقع ستري بشكل واضح في اي موقع وصلت اليه



تمرين

قم بالبحث باستخدام اي موقع بحيث غير جوجل مثل موقع البحث :.bing.com او
Yahoo.com عن "what is my referrer" ثم ادخل نتيجة الموقع :

Whatismyreferer.com

واطبع صورته الموقع الذي يظهر الموقع الذي اتيت منه .

المصادقه وتشفير البيانات

الكلمات السريه Passwords

الكلمات السريه مصدر قلق للعديد من المستخدمين فالمفترض عمل كلمات سريه
للبريد, الالكتروني, انظمه التشغيل, المواقع الاجتماعيه وغيرها ان كانت الخدمه موصوله

بالانترنت ام تعمل محليا بدون الاتصال بالانترنت فان المحافظه على كلمات المرور وتذكرها جميعا وتغييرها كل فتره والاخرى وحمايتها من الاختراق والسرقة عوامل ازعاج للكثير من الناس.

بما ان الكلمات السريه نقطه ضعف في الامان على الانترنت يجب عليك ان تستخدم كلمات سريه معقده وطويله تعقيد الكلمه السريه وتشفيرها مهم جدا على الانترنت فعند حصول المخترق على كلمتك السريه ومن ثم حصول المخترق على قاعده بيانات LinkedIn.com يكون عاده من خلال اختراق موقع معين مثلا مهوله لكل المستخدمين الذين يدخلون في حساباتهم عن طريق الكلمات السريه .

[الموقع التالي:](#)

<https://haveibeenpwned.com>

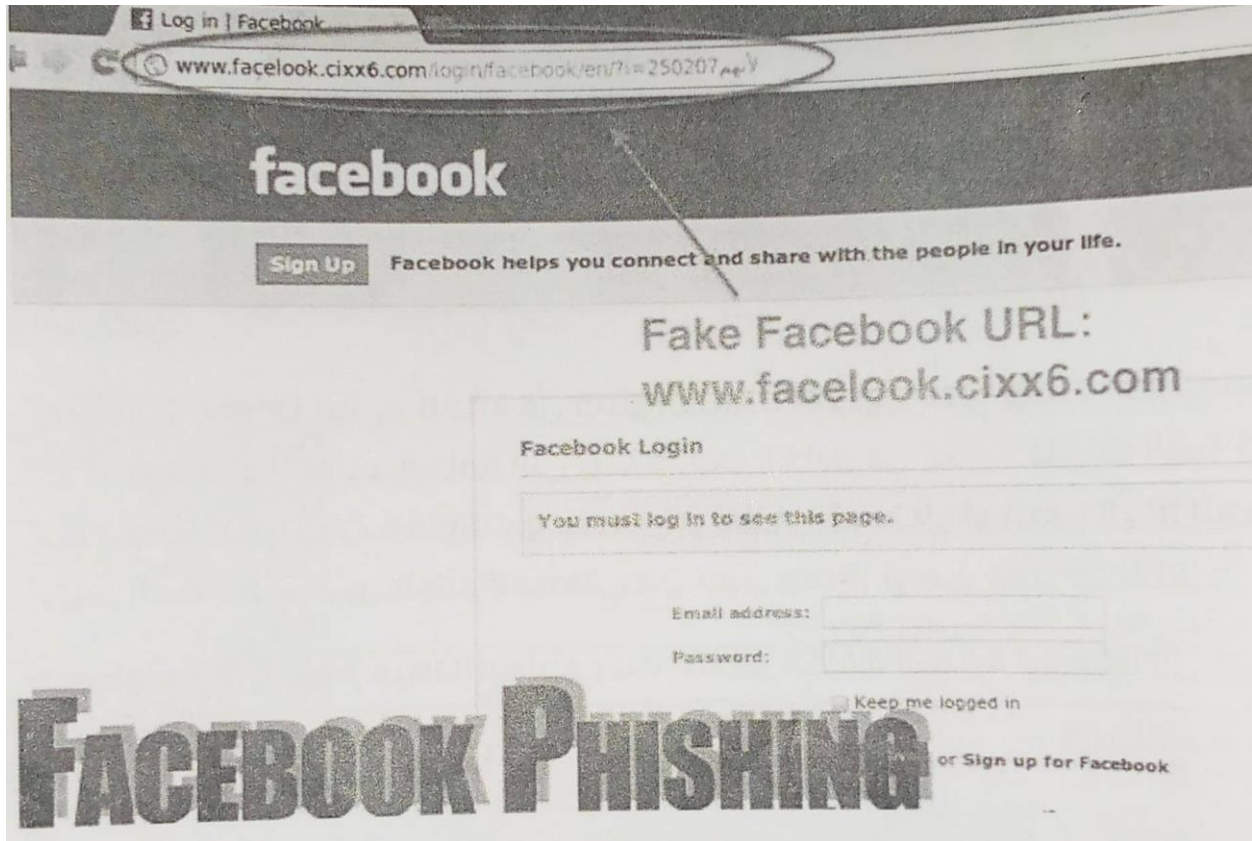
يوفر طريقه بحث عن حسابك من خلال عدد من المواقع ليفحص اذا كان حسابك تم اختراقه (معرفة كلمته السريه) ام لا

الشركات الكبيرة اكبر عرضه للاختراق نظرا لكبر الجائزه في حال نجاح ذلك الاختراق لذلك تصرف الشركات الكبيره العديد من التمويلات على تحسين البنيه التحتيه للامان على شبكتها

بالنسبه للشركات الصغيره فان استخدام وسائل الامن على شبكتها يعتبر من المهام الثانويه نظرا لارتفاع كلفه الحمايه على الشبكه في حال اختراق شبكتها معلوماتك كلها التي استخدمتها في الولوج الى موقع الشركه الصغيره ستكون في يد المخترق وهذا اهم سبب يجعلك تستخدم كلمات سر مختلفه لكل موقع تستخدمه فقد يكون المخترق بتجربه كلمتك السريه في مواقع اخرى اذا كنت تستخدم نفس الكلمه السريه فالتبع سيدخل المخترق الى حساباتك الاخرى بكل سهوله

من اكثر الوسائل ايضا شيوعا في اتلحصول على كلمتك السريه هو phishing attack

والذي من خلاله يدعي المخترق انه الموقع الرسمي لمؤسسه معينه ويطلب مثلا تحديث المعلومات ورؤيه رساله سريه والذي قد يقع بها المثير من الناس فعند ادخال الكلمه السريه ومعلومات الحساب سترسل تلك المعلومات للمخترق ببساطه بدلا من الموقع الرسمي .



يمكن بالطبع الحصول على كلمتك السريه عبر عده طرق اخر مثلاو ببساطه شخص ما يسترق اليك النظر وانت تدخل كلمتك السريه والعديد من الوسائل التي من الممكن الاطلاع على كلمتك السريه من خلالها لذلك من المهم جدا استخدام التشفير عند التعامل مع معلومات حساسه مثل الكلمه السريه .

كسر كلمة المرور – Password Cracking

هناك 3 طرق اساسيه لكسر الكلمات السريه :

1. هجوم القاموس Password Cracking

فيه يستخدم المهاجم قاموسا يحتوي على معظم الكلمات الشائعه التي يستخدمها الناس ليستخدمها الولوج الى حسابك.

2- هجوم القوة الغاشمه Brute Force Attack

فيه يستخدم المهاجم كل تركيب كلمه سريه ممكن من خلال تجربه كل حرف في الكلمه السريه

3- هجوم هجين- Hybrid Attack

يستخدم فيه المهاجم كلمات مرور من القاموس مع تجربه تغيير كل حرف من الكلمه السريه هجوم الكلمه السريه يمكن ان يكون:

- Online
- Offline

Online Cracking يستخدم في الهجوم على كل خدمه تستخدم فيه الولوج الى خدمه معينه مثل موقع ماftb او غيرها.

من اشهر الادوات التي تستخدم في الـ online cracking هو : hydra والموجود في كالي بشكل افتراضي.

Online cracking بطيء للغاية في كسر الكلمات السريه نظرا لوقت الاستجابه في الخادم في حمايه كلمات السر كحد العدد الاقصى للمحاولات مثل ثلاث محاولات وعندها يتم اغلاق التسجيل او حجب الـ ip. للجهاز المهاجم عندها قد يقوم المهاجم بتغيير عنوانه المنطقي من خلال Proxy او من خلال الـ vpn .

Offline attack يقوم فيها المهاجم بفك تشفير الكلمه السريه ليحولها الى كلمه المرور الاصليه ثم يقوم باستخدامها في الدخول الى النظام او الموقع .

الفرق بين الهاش والتشفير

التشفير : التشفير هو عمليه تغيير شكل المعلومات الى شكل اخر باستخدام المعادلات الرياضيه التي تتطلب وجود قيم معينه وهذه القيم هي المفتاح المستخدم في عمليه التشفير الناتج النهائي من عمليه التشفير هو نص غير مقروء للشخص الذي يحمل المفتاح او الشخص الذي حاول ونجح في كسر التشفير

الهاش : الهاش ومعناها الحرفي هو المزيج او الخلط هو عباره عن اجراء العديد من العمليات التي تتعلق بتغيير مكان الحروف او الارقام مع تطبيق بعض المعادلات الرياضيه عليها للحصول على نص اخر ولكن من الصعب جدا ان يتم عكس العمليه يعني استخراج النص الاصلي من الناتج ومن الملاحظ ان عمليه الهاش عندما يتم استخدام نفس الخوارزميه ونفس النص يكون الناتج هو نفس الهاش على الدوام ومن الملاحظ ايضا ان الهاش لا تتطلب وجود مفتاح لانجاز العمليه وعاده ما يكون الهاش الناتج اطول من النص الاصلي .

هناك العديد من الخوارزميات المتخصصه في الهاش مثل SHA2,SHA1,MD5

يمكنك تجربته هاش كلمه معينه من خلال الموقع التالي :

<http://www.shal-online.com/>

<https://www.freecodeformat.com/pbkdf2.php>

مثال : استخدم اداة hashcat

نفذ الامر التالي :

Hashcat -force -m 0 hashes.txt dics.txt -o result.txt

--force	في حال ظهور مشكله تتعلق بالGPU
-m 0	Md5
Hashes.txt	ملف يحتوي على كم كبير من الهاش
Dics.txt	ملف يحتوي على عدد كبير من الكلمات غير مشفره
-o	output
Result.txt	الملف الذي سيكتب بنتيجته

حفظ كلمات المرور

لا شك ان عمليه حفظ كلمات المرور لكل موقع او برنامج يحتفظ بمعلوماتك الشخصيه امر مرهق ان لم يكن صعبا توفر العديد من البرامج ان كانت مثبتة على جهازك او كانت تعتمد على تخزين تلك المعلومات في خادم على الانترنت ميزه حفظ تلك الكلمات السريه بشكل جيد وانيق ولكن لكل شئ حسناته وسيئاته :في حين انها توفر عليك عناء حفظ تلك الكلمات السريه في عقلك او على جهازك او ببساطه على ورقه فانها توفر نقطه اختراق واحده يمكن ان تستغل وهي الكلمه السريه الرئيسييه للاختراق :فان كل معلوماتك الحساسه الموجوده في ذلك الحساب ستعرض بكل بساطه للمخترق.

Masterpassworddapp.com

والمتوفر على اكثر من منصه يمكنك تحميلها ايضا :

keepass

والذي يمثل هذه النوعيه من البرامج التي تكون مثبتة على جهازك ولا حاجه للاتصال بالانترنت

من الادوات ايضا التي يمكن استخدامها من خلال تالمتصفح اداه

Lastpass

تمرين

باستخدام اداه الـ hashcat نفذ ما يلي :

بفرض وجود ملفين (انشئ الملفين في حال عدم وجودهم):الملف الاول يحتوي على عدد من الهاش بصيغه الـ md5 والملف الثاني يحتوي على عدد من كلمات المرور الشائعه.

قم بتنفيذ امر المقارنه لتقوم الاداه بكتابه ناتج العمليه في ملف result.txt

حمایه الخوادم

هجوم الـ STP MANIPULATION

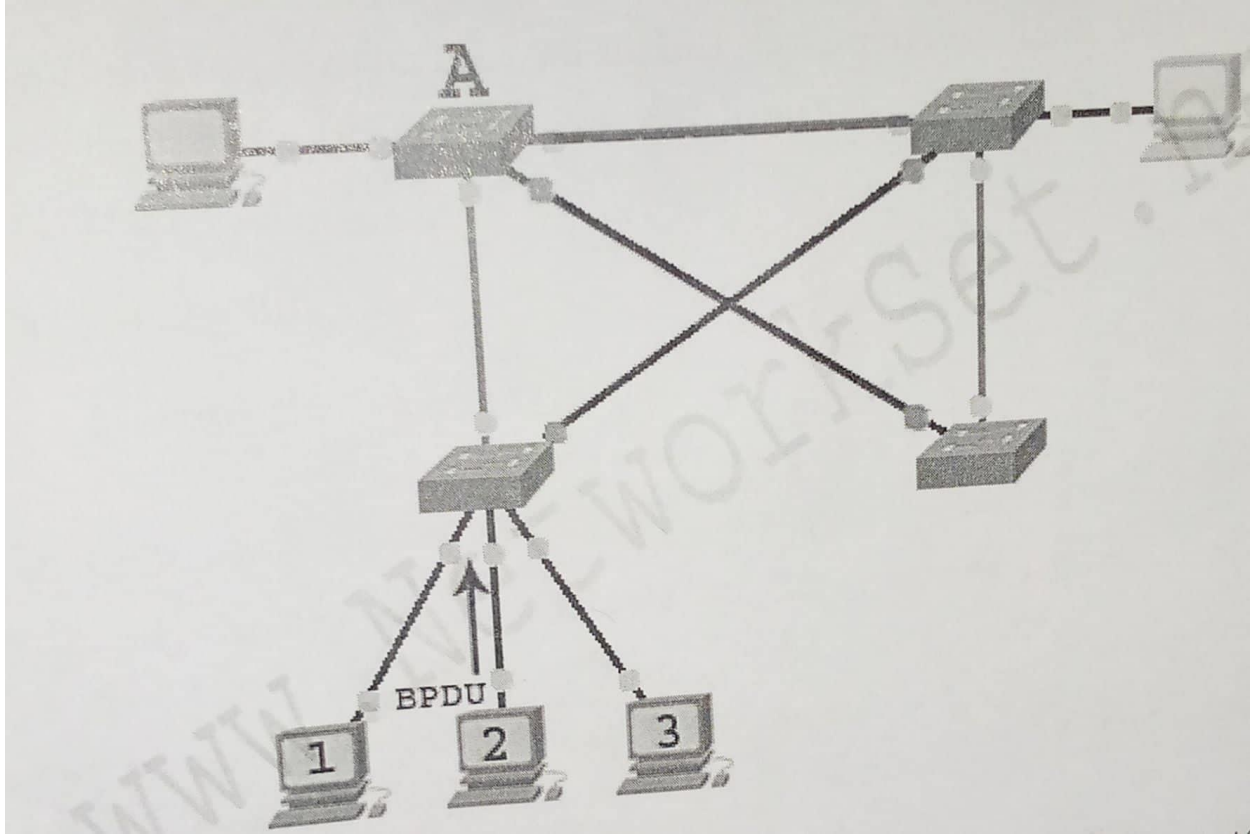
هذا الهجوم يعد خطير جدا وذلك بسبب قدرته على تخريب الشبكة بشكل كامل بالاضافه الى امكانيه المهاجم في التنصت على كل ما يجري في الشبكة واقصد بهذا ليس فقط المفتاح الذي ينتمي اليه المهاجم بل كل المفاتيح الموجوده على الشبكة ويمكن ان تطلق عليه STP MANIPULATION او BPDU ATTACK .

بروتوكول الـ SPANNING TREE

كما هو معروف ان برو توكول الـ STP يلعب دور كبير في الشبكة في منع ما يعرف بال LOOP او BROADCAST STORM ويتم ذلك عن طريق مفتاح واحد ليكون ROOT BRIDGE ويتم الاختبار حسب اقل BRIDGE ID موجود على الشبكة وبعدها يتم اختيار المنافذ التي يجب ان تعمل او تتوقف اعتمادا على الـ COST او التكلفة للوصول لـ ROOT BRIDGE وكل هذه الامور تتم عن طريق ما يعرف بـ BPDU .

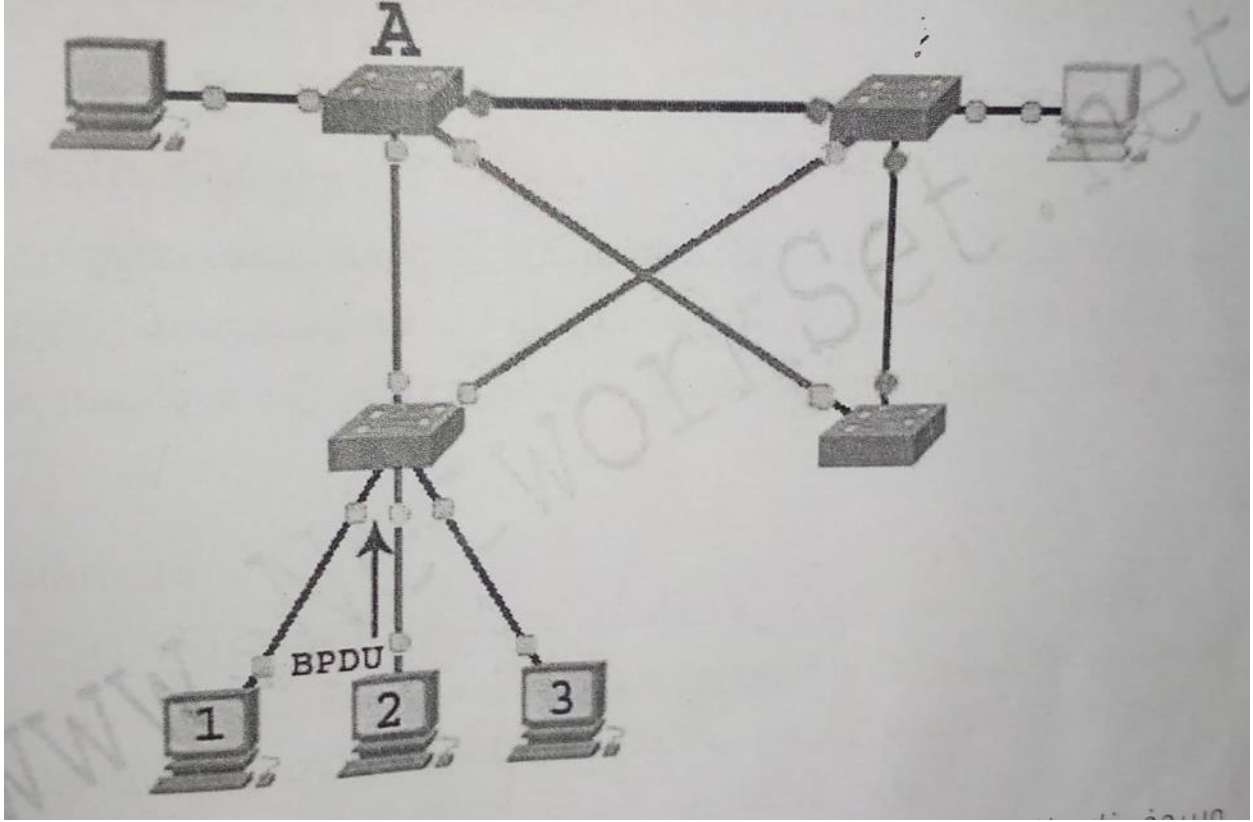
كيف يتم هذا النوع من الهجوم ؟

الهجوم كغيره فكرته لسيطه وتأثيره كبير جدا وهو يتم عن طريق ارسال BPDU مزور يخبر فيه المهاجم المفتاح الذي يرتبط معه بأنه يملك اقل BRIDGE ID على الشبكة وبأنه يجب ان يكون هو الـ ROOT BRIDGE وبالتالي سوف تتم اعاده توزيع المنافذ على كل المفاتيح
مثال :



في الشكل اعلاه نرى فيها التوزيع الطبيعي للشبكة ونرى ايضا ان المفاتيح A هو الـ ROOT BRIDGE على الشبكة والخطوط الحمراء خاصه ب الـ STP ونرى ان المهاجم الموجود على الجهاز رقم 2 يقوم بارسال BPDU مرور الى المفتاح.

في الشكل التالي سوف نشاهد ماذا سوف يحدث عن بعد ان يقوم المهاجم بتغيير المخطط:



وسوف نلاحظ ان كل شئ قد تغيير واصبح كل حركة البيانات التي تعبر عن الشبكة تمر عبر الشخص المهاجم وبالتالي اصبح عندنا الهجوم الذي يعرف بـ MITP او MAN IN THE MIDDLE .

كيف احمي شبكتي من هذا النوع من الهجوم؟

سيكسو تقترح عليك 3 طرق للحمايه من هذا الهجوم الاولى

1. BPDU GUARD خاصيه تخبر فيها المنفذ ان لا يستقبل اي نوع من رسائل الBPDU وفي حال استلام البورت لأيBPDU سوف يقوم بتحويل حاله البورت الى ERRDISABLE اي سوف يتم اغلاق المنفذ بشكل كامل

طريقه الاعداد تتم على الشكل التالي:

ادخل اولاً على المنفذ غير الامن واكتب فيه الامر التالي:

`Switch(config)#spanning-tree bpduguard enable`

وإذا اردت ان تقوم بتفعيل هذه الخاصيه على كل المنافذ التي تكون في حاله ...اكتب الامر التالي:

Switch(config)#spanning-tree portfast bpduguard default

2. BPDU ROOT في هذه الخاصية اخبر المفتاح بأن المنفذ لن يكون ابدا
ROOT BRIDGE وتتم من خلال هذا الامر:

Switch(config-if)# spanning-tree guard root

3. BPDU FILTERING هذه الخاصية هي نفس الخاصية الاولى والفرق الوحيد هو ان
هذه الخاصية تتيح لك ان تحدد ماذا تريد للمنفذ ان يفعل في حال استلم BPDU بعكس
ال BPDU GUARD الذي سوف يقوم باغلاق المنفذ بشكل مباشر وطريقه الاعداد هي
كالتالي :

Switch(config-if)# spanning-tree bpduguard enable

وإذا اردت ان تقوم بتفعيل هذه الخاصية على كل المنافذ التي تكون في حاله...اكتب
الامر التالي:

Switch(config-if)# spanning-tree portfast bpduguard default

DHCP STARVATION هجوم

ما هو هجوم DHCP STARVATION. ؟

يشكل هذا النوع من الهجوم خطرا كبيرا على الشبكة لانه يقوم ببساطه بحجز كل العناوين
الموجودة في خادم ال DHCP وفيها يقوم المهاجم بارسال عدد غير محدود من الرسائل الى
خادم ال DHCP يطلب فيها تزويده بعنوان منطقي للجهاز الخاص فيه وعندما يتم استلام
الاعدادات من الخادم وحجز عنوان له يقوم بارسال طلب جديد الى السيرفر لكن هذه المرة
MAC ADDRESS مختلف وهكذا حتى يقوم المهاجم بحجز كل العناوين المتاحة على
السيرفر وحتى لو كان 10000 عنوان لان هذه العملية تتم بسرعه كبيره والتي قد لا تستغرق
بضع دقائق وبالتالي اي محاوله من اي جهاز اخر موجود على الشبكة للحصول على عنوان
من الخادم سوف تباء بالفشل.

طرق الحماية من هذا النوع من الهجوم

طريقه الحماية تتم من خلال امن المنفذ PORT SECURITY وذلك بتحديد عدد معين من عناوين الماك المسموح لها بالدخول من خلال هذا المنفذ والوامر طبعا سوف تطبق على المفتاح بالشكل التالي:

```
Switch# conf t
```

```
Switch(config) # interface fastethernet 0/1
```

```
Switch(config-if)# Switchport mode access
```

```
Switch(config-if)# Switchport port-security
```

تطبيق هذه الاعدادات سوف تسمح لعنوان ماك واحد للدخول ورده الفعل التي سوف يقوم بها المفتاح هي اغلاق المنفذ بشكل كامل في حال تخطي هذا العدد وتستطيع ان تقوم بتحديد العدد ورده الفعل كما تريد.

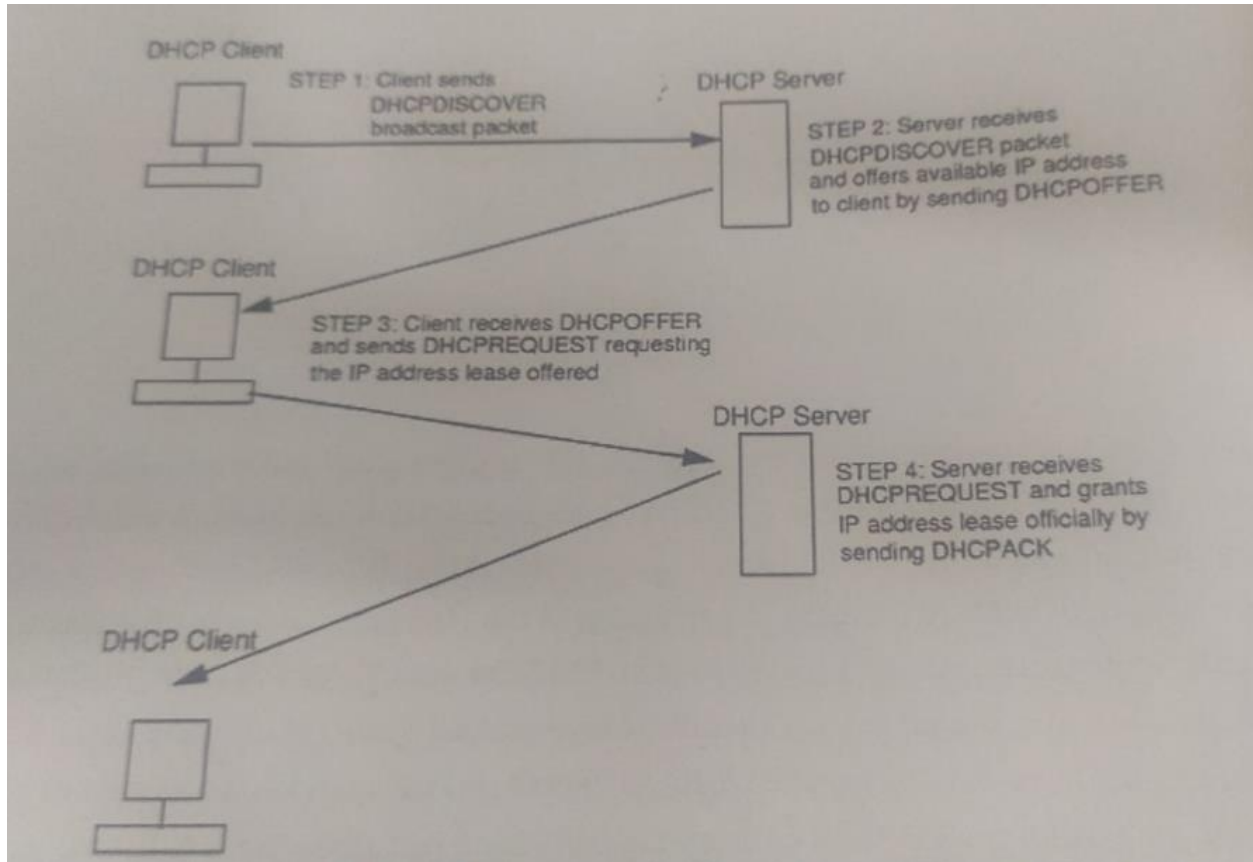
هجوم الـ DHCP SPOOFING

ما هو هجوم الـ DHCP SPOOFING؟ وكيف يتم؟

يعد هذا الهجوم احد الهجمات الخطيره على الشبكة والحمايه منه امر مهم جدا على الشبكة وفكرته بسيطه جدا وتنفيذها اسهل وهي ببساطه تقوم من خلال قيام المخترق بتشغيل خادم DHCP على جهازه يملك نفس المعلومات التي يقوم الخادم الرئيسي بتزويدها للاجهزة لكن مع اختلاف بسيط جدا وهو الـ GATEWAY للشبكة فهو يقوم بتغييره بحيث يقوم هو جهازه نفسه ومن خلال احد البرامج مثل الـ ETTERCAP يقوم بتحويل حركه مرور البيانات الماره عبر جهازه الى الـ GATEWAY الحقيقي للشبكة وبهذا كل ما يتم ترسالة من خلال الاجهزة الموجودة على الشبكة سوف تعبر من خلال جهاز المخترق ومن خلال احد برامج تحليل البيانات مثل الـ WIRESHARK سوف يشاهد كل تفاصيل حركه مرور البيانات وطبعا هذه تعد كارته كبيره للشبكة وخصوصا اي هجمه تدرج تحت هجمات الـ MITM. ولو اراد المهاجم ان يكون المهاجم كاملا فهو سوف يقوم اولا بتنفيذ هجوم الـ DHCP STARVATION على السيرفر الرئيسي ويقوم بحجز كل العناوين الموجوده عنده وعندها سوف يضمن بان كل الاجهزة الموجوده على الشبكة وعلى مفاتيح اخرى سوف تلجأ اليه للحصول على المعلومات اللازمه للاتصال بالشبكة مما يزيد من كميته المعلومات الماره عبر جهاز المخترق وبالتالي دمار اكبر للشبكة.

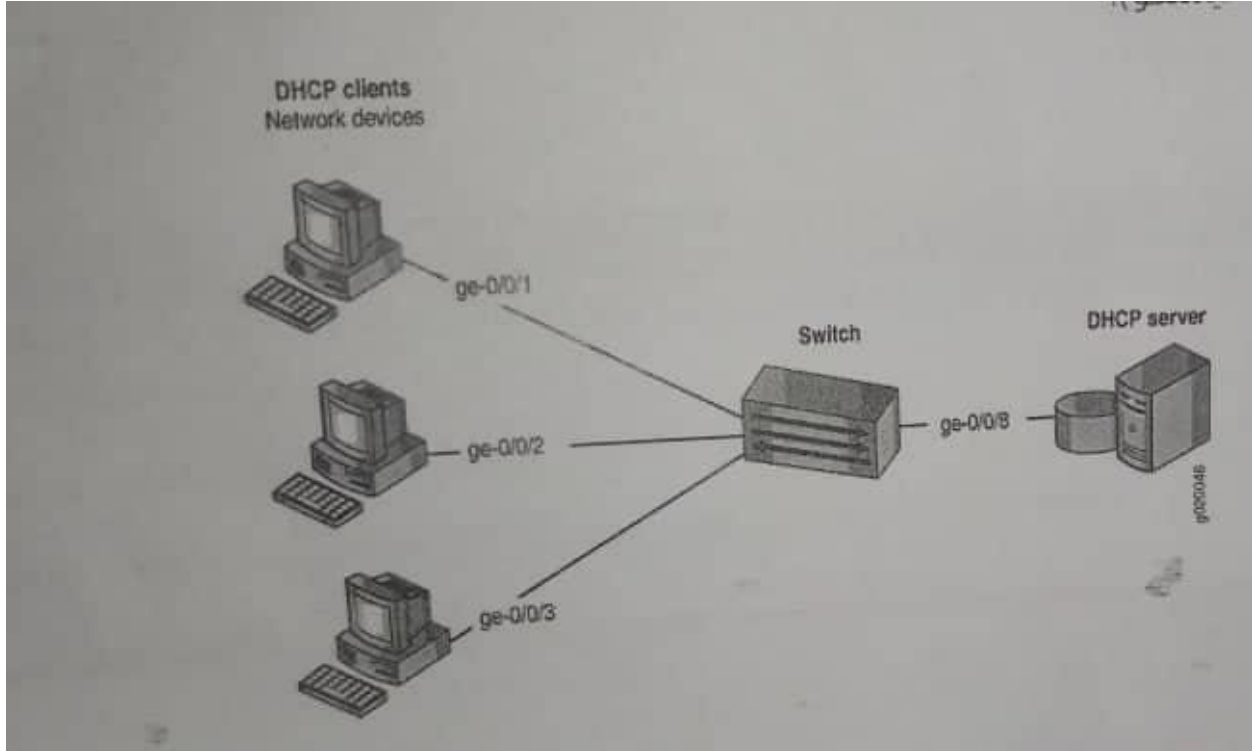
كيفيه الحماية من هذا النوع من الهجمات ؟

الحل الذي قدمته سيسكو كان عبارته عم خاصيه تدعى DHCP Snooping هذه الخاصيه ببساطه تعرف المفتاح ما هي المنافذ الموثوقه وما هي المنافذ الغير موثوقه وبكلام اخر تعرف ما هي المنافذ التي يسمح لها بتوزيع طلبات الdhcp فنحن نعلم ان عمليه طلب المعلومات من الdhcp تمر بعده خطوات تبدا بقيام جهاز العميل بارسال broadcast الى الشبكه يسال فيه عن خادم الdhcp وبعدها يرد عليه الخادم بعنوان الip الخاص فيه وعندها تاتي خطوه الطلب من العميل الى الخادم (طلب الاعدادات) وبعد وصول الطلب الى السيرفر يقوم بارسال المعلومات اللازمه له من ip و subnet mask و dns وطبعاً ال gateway وهذه صورته توضيحيه لسير العمليه:



من خلال فهمك لهذه العمليه سوف تستنتج بان هذه الخاصيه تقوم باخبار المفتاح من هو المنفذ الموثوق والذي يسمح له بالرد على طلبات الdhcp التي تتم من خلال المستخدمين الموجودين على الشبكه ومن هنا اتت كلمه snooping والتي تعني تفتيش الطلبات ومن اين وصلت والنخ...

طريقه الاعداد (سيسكو)



```
Switch(config) # ip dhcp snooping
```

```
Switch(config) # ip dhcp snooping vlan 10,32,104
```

```
Switch(config) # interface range gigabitethernet 0/0/10 – 0/0/3
```

```
Switch(config-if)#ip dhcp snooping limit rate 3
```

```
Switch(config-if) # interface gigabitethernet 0/0/8
```

```
switch(config-if)#ip dhcp snooping trust
```

اول امر اعتقد بانه واضح للجميع وهو من اجل تفعيل الـ dhcp snooping على المفتاح مجرد تفعيلك لهذه الخاصيه على المفتاح يقوم هو بشكل تلقائي بوضع كل المنافذ على شكل untrusted غير موثوقه اما في الامر الثاني فنحن نقوم بتحديد الـ vlan التي نريد ان نقوم بتفتيشها وهذا شئ مهم ايضا واساسي ومن خلال هذا الامر نستطيع ان نكتب كل الـ vlan التي نريدها وقد قمنا في هذا المثال باضافه 3 vlan وهم: 10,32,104 الامر الثالث من اجل تحديد مجموعه من المنافذ وقد اختلنا 3 منافذ والتي تشكل اجهزة العملاء لدينا في الشبكه وبعدها

نقوم بتحديد عدد الطلبات التي يسمح له بطلبها وهي تحسب بعدد الpacket كل ثانيه
ppsويمكننا زياده هذا الرقم كما نشاء لكن لا ينصح بهذا كثيرا واخيرا ندخل على المنفذ
المرتبط مع خادم ال...ونخبر المفتاح بان هذا المنفذ موثوق به trusted
لمشاهده تفاصيل عن حاله الdhcp snoopingنستخدم الاوامر التاليه :

```
Switch# show ip dhcp snooping
```

```
Switch# show ip dhcp snooping binding
```

تمرين

اكتب الاوامر المطلوبه لحمايه الخادم من المفتاح ضد هجمات dhcp spoofing مع العلم
بالمعطيات التاليه

هناك شبكه ظاهريه واحده VLAN1

هناك واجهتان في المفتاح والتي ستفعل فيها الحمايه وهما fa0/0 و fa0/1

عدد الطلبات المسموح طلبها هو 5

المشاريع:

يقدم الطالب مشروعه خلال اسبوع الى اسبوعين للتقديم والمناقشه مع تلخيص للمشروع
(من ورقتين الى 5اوراق) على ان تتم المناقشه في نهايه المده المحدده يمكن لطالب اختيار
اي مشروع ملائم ضمن ماده امن وحمايه الشبكات بشرط تغطيه ماده لم نغطيها في هذا
المساق وعدم تكرار موضوع الشروع مع طالب اخر.

مشاريع مقترحة :

- خوارزميات التشفير
- برامج الـ antivirus
- الهندسة الإجتماعية
- حماية شبكة wi fi
- تطبيق عملي (برنامج يعمل كأداة تصيد مثلا، او برنامج يقوم بعمل تشفير وفك تشفير)