دليل Wireshark الكامل

من إعداد: عبد الصمد بوركيبات

باحث في فقه الأمن السيبراني الأسري، ومتخصص في الأمن السيبراني

مقدمة في تحليل الشبكات

تعريف تحليل الشبكات

- عملية **فحص ومراقبة** حركة البيانات
- تحليل تدفق المعلومات بين الأجهزة
- تشخيص المشاكل وتحديد الأداء
- فهم سلوك الشبكة وتفاعلها

الأهمية في الأمن السيبراني

- **كشف التهديدات** والهجمات المحتملة
- مراقبة الأنشطة المشبوهة
- تحديد نقاط الضعف في الشبكة
- توفير أدلة للتحقيق في الحوادث

تطبيقات عملية

- **استكشاف الأخطاء** وإصلاحها
- تحسين أداء الشبكة
- تحليل سلوك التطبيقات
- مراقبة استخدام النطاق الترددي
- تدريب وتعليم مفاهيم الشبكات

أدوات التحليل الشائعة

- **Wireshark** - تحليل الحزم الشامل
- Tcpdump - أداة سطر الأوامر
- Nmap - مسح الشبكة واكتشاف الأجهزة
- PRTG - مراقبة الشبكة
- NetFlow - تحليل تدفق البيانات

ما هي Wireshark؟ ولماذا تُعد أداة استخباراتية؟

تعريف Wireshark

- **محلل بروتوكولات الشبكة** مفتوح المصدر
- أداة لالتقاط وتفحص حزم البيانات
- يدعم مئات البروتوكولات المختلفة
- متوافق مع أنظمة التشغيل المختلفة
- واجهة رسومية سهلة الاستخدام

قدرات Wireshark في تحليل البيانات

- **التقاط المباشر** لحركة البيانات
- عرض تفصيلي لطبقات الشبكة المختلفة
- تحليل البروتوكولات المعقدة
- إمكانية فلترة وتصنيف الحزم
- إعادة بناء الجلسات والتدفقات

الاستخدام كأداة استخباراتية

- **كشف الأنشطة المشبوهة** في الشبكة
- تحليل سلوك التطبيقات والبرمجيات
- مراقبة الاتصالات غير المصرح بها
- تحديد أنماط الهجمات السيبرانية
- تجميع الأدلة الرقمية للتحقيقات

أمثلة على المعلومات المستخلصة

- **بيانات الاعتماد** والمصادقة
- محتوى الرسائل والمحادثات
- عناوين IP والمنافذ المستخدمة
- الملفات المنقولة عبر الشبكة
- سجل التصفح والأنشطة الإلكترونية

التطور التاريخي لأداة Wireshark

بدايات Wireshark (Ethereal)

- تطويره في **1998** بواسطة **جيرالد كومبس**
- اسمه الأصلي **Ethereal**
- بدأ كأداة بسيطة لتحليل الشبكات
- دعم أساسي للبروتوكولات الشائعة
- واجهة رسومية بدائية

التطورات الرئيسية عبر الزمن

- **2006** تغيير الاسم إلى **Wireshark** بسبب مشاكل العلامة التجارية
- إضافة دعم لمئات البروتوكولات الجديدة
- تحسينات في أداء التقاط الحزم
- تطوير قدرات التشفير وفك التشفير
- تحسين واجهة المستخدم وإضافة الميزات المتقدمة

الإصدارات المهمة ومميزاتها

- **1.0** أول إصدار مستقر تحت اسم Wireshark
- **2.0** **واجهة مستخدم** محدثة بالكامل
- **3.0** دعم أفضل للتشفير والبروتوكولات الحديثة
- **4.0** تحسينات كبيرة في الأداء والاستقرار
- **4.4** إصلاحات أمنية وتحديثات البروتوكولات

Wireshark اليوم

- أداة **قياسية** في تحليل الشبكات
- يدعم آلاف البروتوكولات المختلفة
- مجتمع نشط من المطورين والمساهمين
- استخدام واسع في الأمن السيبراني
- تكامل مع أدوات تحليل وتصور البيانات
- تحديثات دورية لتحسين الأمان والأداء

المفاهيم الأساسية: Packets, Frames, Protocols

شرح الحزم (Packets)

- وحدة **بيانات** يتم نقلها عبر الشبكة
- تحتوي على **العنوان** والمحتوى
- تتضمن رأس (Header) وحمل (Payload)
- تختلف الحجم حسب البروتوكول المستخدم
- يمكن تقسيم البيانات الكبيرة إلى حزم متعددة

شرح الإطارات (Frames)

- وحدة بيانات في **طبقة وصلة البيانات**
- تغلف الحزم لإرسالها فعلياً
- تحتوي على عناوين **MAC** المصدر والوجهة
- تضيف معلومات للتحكم من الأخطاء
- تختلف حسب نوع الشبكة (إيثرنت، واي فاي، إلخ)

مفهوم البروتوكولات (Protocols)

- **قواعد** تنظم الاتصال بين الأجهزة
- تحدد هيكل البيانات وطريقة إرسالها
- تنظم عملية **المصافحة** وإنهاء الاتصال
- أمثلة: TCP, IP, HTTP, DNS, DHCP
- تعمل في طبقات مختلفة من نموذج OSI

العلاقة بين هذه المفاهيم

- البروتوكولات تحدد **هيكل** الحزم والإطارات
- البيانات تغلف في حزم وفقاً للبروتوكول
- الحزم تغلف في إطارات للنقل الفيزيائي
- Wireshark يحلل هذه العناصر **طبقة طبقة**

إعداد بيئة تحليل الشبكة

المتطلبات الأساسية

- جهاز كمبيوتر بمواصفات **مناسبة**
- مساحة تخزين كافية لملفات الالتقاط
- صلاحيات **المسؤول** للوصول للواجهات
- برنامج Wireshark مثبت بشكل صحيح
- برنامج تشغيل حزم البيانات `WinPcap/Npcap`

إعداد الواجهات الشبكية

- تحديد الواجهة **المناسبة** للاقتناص
- تكوين وضع `Promiscuous` عند الحاجة
- اختيار وضع الالتقاط المناسب `Monitor`
- ضبط إعدادات التصفية للواجهات
- اختبار الواجهة قبل بدء الالتقاط الفعلي

الاعتبارات الأمنية

- الحصول على **التصريحات** اللازمة
- عدم التقاط بيانات **حساسة** دون إذن
- تأمين ملفات الالتقاط بشكل جيد
- عدم مشاركة البيانات التي تحتوي على معلومات خاصة
- الالتزام بالقوانين واللوائح المحلية

أفضل الممارسات

- استخدام **فلاتر** لتحديد البيانات المطلوبة
- تحديد حجم ملفات الالتقاط لتجنب استهلاك المساحة
- توثيق إعدادات البيئة والفلاتر المستخدمة
- العمل على **بيئة معزولة** عند التعلم
- الاحتفاظ بنسخ احتياطية من ملفات الالتقاط المهمة

تثبيت Wireshark على جميع الأنظمة

القسم الثاني: التثبيت والتهيئة

التثبيت على Windows

- تحميل المثبت من **الموقع الرسمي**
- تشغيل المثبت كـ **مسؤول**
- اختيار المكونات المطلوبة `Npcap`
- السماح بتثبيت Npcap عند الطلب
- إعادة تشغيل الجهاز بعد التثبيت

التثبيت على Linux

- استخدام مدير الحزم `apt` أو `yum`
- أمر التثبيت: **sudo apt install wireshark**
- إضافة المستخدم لمجموعة **wireshark**
- تثبيت الحزم الإضافية لدعم البروتوكولات
- تسجيل الخروج وإعادة الدخول لتطبيق الصلاحيات

التثبيت على macOS

- تحميل ملف **.dmg** من الموقع الرسمي
- سحب Wireshark إلى مجلد التطبيقات
- تثبيت `ChmodBPF` للصلاحيات
- السماح بالوصول للواجهات من إعدادات الأمان
- إعادة تشغيل التطبيق بعد تثبيت الصلاحيات

المشاكل الشائعة وحلولها

- **عدم ظهور الواجهات**: تثبيت Npcap/ChmodBPF
- **صلاحيات غير كافية**: تشغيل كمسؤول
- مشاكل الاعتماديات: تثبيت الحزم المطلوبة
- تعارض مع برامج أخرى: إيقاف مؤقت للجدار الناري
- أخطاء التثبيت: تحميل إصدار متوافق مع النظام

الفرق بين Npcapg WinPcap

القسم الثاني: التثبيت والتهيئة

تعريف WinPcap

- **مكتبة التقاط الحزم** لنظام Windows
- تم تطويره في 1999 بواسطة فريق من الباحثين
- يدعم التقاط وإرسال حزم البيانات الخام
- يعمل في **وضع kernel** لتحسين الأداء
- لم يتم تحديثه بنشط منذ عام 2013

تعريف Npcap

- **النسخة الحديثة** من WinPcap
- تم تطويره بواسطة مطورو Wireshark
- يدعم أحدث إصدارات Windows
- يتضمن **تحسينات أمنية** وأداء أفضل
- يتم تحديثه بانتظام مع Wireshark

المقارنة بينهما

الميزة	WinPcap	Npcap
دعم Windows 10/11	✗	✓
الأداء	جيد	**ممتاز**
الأمان	متوسط	**محسن**
التحديثات	متوقفة	مستمرة

متى تستخدم كل منهما

- **Npcap**: الخيار الموصى به دائماً
- أنظمة Windows الحديثة 10/11
- عند الحاجة لأقصى أداء وأمان
- WinPcap: الأنظمة القديمة XP/7
- عند وجود تعارض مع Npcap
- للتوافق مع تطبيقات قديمة

إعداد الصلاحيات والتحكم في الواجهات

القسم الثاني: التثبيت والتهيئة

صلاحيات المسؤول

- تشغيل Wireshark كـ **مسؤول** للوصول الكامل
- في Linux: إضافة المستخدم لمجموعة `wireshark`
- في Windows: استخدام **Run as administrator**
- في macOS: تثبيت `ChmodBPF` للصلاحيات
- التحقق من الصلاحيات قبل بدء الالتقاط

التحكم في الواجهات الشبكية

- عرض الواجهات المتاحة في **شاشة الترحيب**
- تفعيل/تعطيل الواجهات حسب الحاجة
- اختيار وضع **Promiscuous** عند الضرورة
- إدارة واجهات `الشبكات اللاسلكية`
- تكوين واجهات `الشبكات الافتراضية`

إعدادات الأمان

- تقييد الوصول إلى **ملفات الالتقاط**
- تعطيل **تشغيل البرامج** تلقائياً
- تشفير ملفات الالتقاط الحساسة
- إعدادات `جدار الحماية` المناسبة
- التحكم في صلاحيات القراءة والكتابة

إدارة المستخدمين

- إنشاء **مجموعات مستخدمين** متخصصة
- تحديد صلاحيات مختلفة حسب الدور
- توزيع مهام الالتقاط والتحليل
- تتبع **نشاط المستخدمين**
- مراجعة الصلاحيات بشكل دوري

واجهة Wireshark الرسومية: شرح تفصيلي

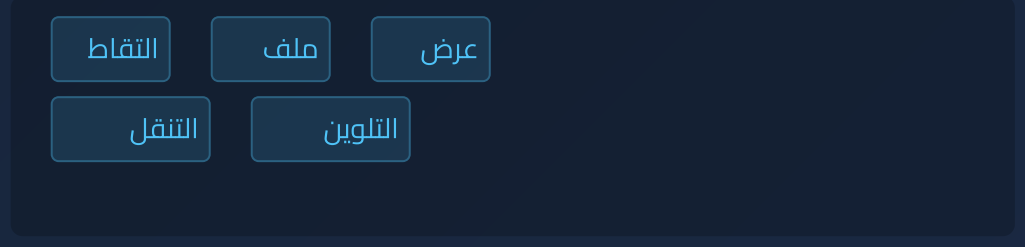
القسم الثاني: التثبيت والتهيئة

القوائم الرئيسية

- **ملف** File : فتح وحفظ ملفات الالتقاط
- **تحرير** Edit : نسخ، بحث، وإعدادات
- **عرض** View : تخصيص واجهة العرض
- **التقاط** Capture : بدء وإيقاف الالتقاط
- **تحليل** Analyze : تتبع الجلسات والفلاتر

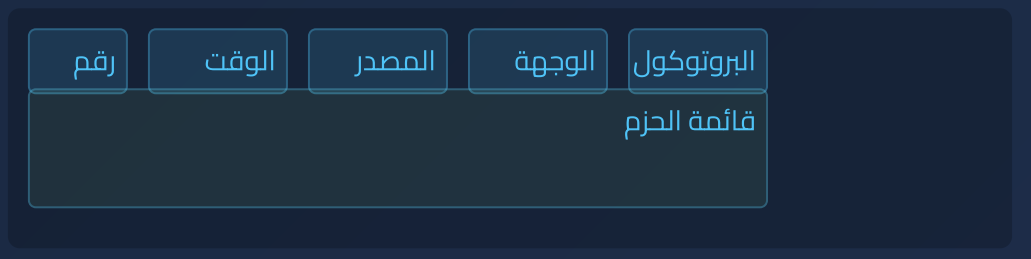
شريط الأدوات

- أزرار **الالتقاط**: بدء، إيقاف، وإعادة التشغيل
- أزرار **الملفات**: فتح، حفظ، وطباعة
- أزرار **التنقل**: الانتقال بين الحزم
- أزرار **العرض**: تكبير وتصغير
- أزرار **التلوين**: تفعيل وإيقاف التلوين



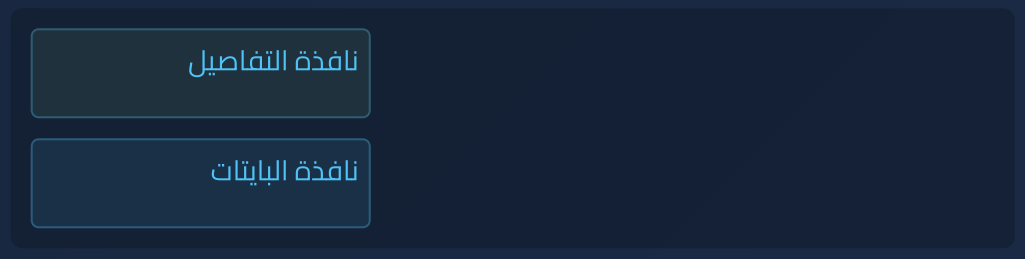
نافذة عرض الحزم

- عرض **قائمة الحزم** الملتقطة
- أعمدة: رقم الحزمة، الوقت، المصدر، الوجهة
- عرض **البروتوكول** والمعلومات
- إمكانية **الفرز** حسب الأعمدة
- تلوين الحزم حسب البروتوكولات



نوافذ التفاصيل والبايتات

- **نافذة التفاصيل**: تحليل طبقات الحزمة
- عرض **البروتوكولات** المتداخلة
- **نافذة البايتات**: عرض البيانات الخام
- عرض **النص** والسداسي عشري
- إبراز الجزء المحدد من الحزمة



التحكم في الأداء وإعدادات الفلترة التلقائية

القسم الثاني: التثبيت والتهيئة

تحسين أداء Wireshark

- تعطيل **تحليل البروتوكولات** غير الضرورية
- استخدام **فلاتر الالتقاط** لتقليل البيانات
- إغلاق النوافذ غير المستخدمة
- تحديث Wireshark لأحدث إصدار
- زيادة ذاكرة التخزين المؤقت Cache

إعدادات الفلترة التلقائية

- تفعيل **الفلاتر التلقائية** للبروتوكولات
- إنشاء **قوائم فلترة** مخصصة
- إعدادات الفلترة حسب IP أو MAC
- فلترة حسب **نوع الحزمة** أو المحتوى
- حفظ الفلاتر الشائعة للاستخدام السريع

إدارة الذاكرة

- تحديد **حجم الذاكرة** المخصص لـ Wireshark
- ضبط **عدد الحزم** المعروضة في القائمة
- تفريغ الذاكرة بعد كل عملية تحليل
- استخدام Garbage Collection بشكل دوري
- مراقبة استخدام الذاكرة أثناء التشغيل

التعامل مع ملفات التتبع الكبيرة

- **تقسيم الملفات** الكبيرة إلى أجزاء أصغر
- استخدام **ملفات متعددة** للتقاط طويل
- تحميل أجزاء محددة من الملف
- تصدير البيانات المطلوبة فقط
- استخدام أدوات خارجية لمعالجة الملفات الضخمة

التقاط البيانات من الواجهات الصحيحة

القسم الثالث: التقاط البيانات الحية

تحديد الواجهات الشبكية المناسبة

- فهم **طوبولوجيا الشبكة** الحالية
- اختيار الواجهة **الأقرب** للهدف
- التحقق من حالة الواجهات النشطة
- استخدام `ifconfig` أو `ipconfig` للتحقق
- اختيار الواجهة ذات **حركة المرور** المطلوبة

التقاط البيانات في أوضاع مختلفة

- وضع **Promiscuous** لرؤية كل الحزم
- وضع **Monitor** للشبكات اللاسلكية
- التقاط `الحزم الواردة` فقط
- التقاط `الحزم الصادرة` فقط
- التقاط في وضع **الجسر** للشبكات المعقدة

التقاط البيانات من الشبكات اللاسلكية

- اختيار **بطاقة لاسلكية** تدعم وضع المراقبة
- التحقق من **توافق** البطاقة مع Wireshark
- استخدام `Monitor Mode` لرؤية جميع الحزم
- تحديد **القناة** الصحيحة للشبكة المستهدفة
- مراعاة **قيود التشفير** في الشبكات اللاسلكية

مشاكل وحلول شائعة

- **عدم ظهور الواجهات**: تثبيت برامج التشغيل
- **صلاحيات غير كافية**: تشغيل كمسؤول
- مشاكل `الشبكات اللاسلكية` : بطاقات غير متوافقة
- **فقدان الحزم**: زيادة حجم المخزن المؤقت
- أخطاء **التعارض**: إيقاف برامج الجدار الناري

Capture Filters: الصياغة والتطبيق

القسم الثالث: التقاط البيانات الحية

أساسيات فلاتر الالتقاط

- تعمل على **مستوى kernel** قبل المعالجة
- تستخدم **صيغة BPF** Berkeley Packet Filter
- تقلل من **حجم البيانات** الملتقطة
- تحسن **أداء** Wireshark بشكل كبير
- تطبق قبل حفظ الحزم في الذاكرة

صياغة فلاتر فعالة

- استخدام **عوامل المقارنة**: `==` `!=` `<` `>`
- الربط بين الشروط بـ **AND** و **OR**
- فلترة حسب **البروتوكول**: tcp, udp, icmp
- فلترة حسب **المنفذ**: port 80, port 443
- فلترة حسب **عنوان IP**: host 192.168.1.1

```
tcp port 80 and host 192.168.1.1
```

أمثلة عملية

- **HTTP traffic**: tcp port 80 or tcp port 8080
- **HTTPS traffic**: tcp port 443
- **DNS traffic**: udp port 53
- **ARP traffic**: arp
- **ICMP traffic**: icmp

```
tcp portrange 1-1024 and not host
192.168.1.100
```

نصائح متقدمة

- استخدام **الأقواس** لتحديد أولوية العمليات
- فلترة حسب **نطاق المنافذ**: portrange 20-80
- فلترة حسب **حجم الحزمة**: less 100, greater 500
- استبعاد **عناوين محددة**: not host 192.168.1.1
- فلترة حسب **اتجاه البيانات**: src, dst

```
(tcp src port 80) and (tcp dst port 1024-
5000)
```

تسجيل البيانات التلقائي والمجدول

القسم الثالث: التقاط البيانات الحية

إعداد التسجيل التلقائي

- تفعيل **ملفات متعددة** في إعدادات الالتقاط
- تحديد **حجم الملف** الأقصى لكل ملف
- اختيار **تنسيق الملف** المناسب `pcapng`
- إعداد **تسمية تلقائية** للملفات
- تفعيل **الاستمرارية** بين الملفات

التقاط مجدول

- استخدام **مهام مجدولة** في نظام التشغيل
- أوامر **tshark** للاستخدام في السكربتات
- تحديد **الفترات الزمنية** للاقتناص
- دمج مع `cron` في Linux أو `Task Scheduler` في Windows
- إعداد **الإشعارات** عند انتهاء الالتقاط

إدارة مساحة التخزين

- تحديد **عدد الملفات** الأقصى
- تفعيل **الحلقة التلقائية** `ring buffer`
- إعداد **الضغط التلقائي** للملفات القديمة
- نقل الملفات إلى **تخزين خارجي**
- حذف الملفات **القديمة** تلقائياً

أفضل الممارسات

- استخدام **فلاتر الالتقاط** لتقليل البيانات
- توثيق **إعدادات الالتقاط** المستخدمة
- مراقبة **مساحة التخزين** بانتظام
- حماية **الملفات الحساسة** بتشفيرها
- عمل **نسخ احتياطية** للملفات المهمة

قراءة الحزم المشفرة وغير المشفرة

القسم الثالث: التقاط البيانات الحية

التعرف على الحزم المشفرة

- بحث عن **بروتوكولات التشفير** TLS/SSL
- تحليل **مصافحة TLS** في بداية الاتصال
- التعرف على **المنافذ المشفرة** الشائعة
- فحص **رؤوس الحزم** للإشارات المشفرة
- مراقبة **شهادات SSL** المتبادلة

تحليل الحزم غير المشفرة

- استعراض **المحتوى النصي** مباشرة
- تحليل **بروتوكولات HTTP** و FTP
- استخراج **المعلومات الحساسة** غير المحمية
- فحص **البيانات الوصفية** للحزم
- استخدام **ميزة Follow Stream** لإعادة بناء الجلسات

التحديات في تحليل الحزم المشفرة

- **عدم القدرة** على رؤية المحتوى الفعلي
- صعوبة **فك التشفير** بدون مفاتيح
- تعقيد **خوارزميات التشفير** الحديثة
- مشاكل **الأداء** عند محاولة فك التشفير
- قيود **قانونية وأخلاقية** في فك التشفير

حلول عملية

- استخدام **مفتاح فك التشفير** SSLKEYLOGFILE
- تحليل **البيانات الوصفية** بدلاً من المحتوى
- التركيز على **أنماط الاتصال** وسلوكها
- استخدام **وسيط TLS** لفك تشفير الاتصالات
- التحليل **قبل وبعد** مرحلة التشفير

اكتشاف الأنشطة الغريبة في الوقت الفعلي

القسم الثالث: التقاط البيانات الحية

مراقبة الشبكة المباشرة

- استخدام **واجهة المراقبة** المباشرة
- تفعيل **التحديث التلقائي** للحزم
- مراقبة **معدل الحزم** في الوقت الفعلي
- استخدام I/O Graph لرصد الأنماط
- مراقبة **الاستخدام غير الطبيعي** للنطاق

مؤشرات الأنشطة المشبوهة

- **زيادة مفاجئة** في حركة المرور
- اتصالات من **عناوين غريبة**
- محاولات **مسح المنافذ** Port Scanning
- تبادل **بيانات غير معتادة** بين الأجهزة
- استخدام **بروتوكولات نادرة** أو غير معروفة

إعداد التنبيهات

- استخدام **فلاتر العرض** للأنشطة المشبوهة
- تكوين **إشعارات ملونة** للمخاطر
- ربط Wireshark مع أنظمة SIEM
- إعداد **تنبيهات عبر البريد** أو الرسائل
- تخصيص **قواعد التنبيه** حسب سياسة الشبكة

الاستجابة السريعة

- **عزل الأجهزة** المصابة فوراً
- حظر **عناوين IP** المشبوهة
- إغلاق **المنافذ** المستهدفة
- توثيق **الأدلة الرقمية** للتحقيق
- تنفيذ **خطة الطوارئ** الأمنية

تفسير الطبقات: Ethernet > IP > TCP > HTTP

القسم الرابع: تحليل الحزم البروتوكولية

نموذج OSI/TCP-IP

- **نموذج OSI**: 7 طبقات هرمية
- **نموذج TCP/IP**: 4 طبقات عملية
- كل طبقة **تغلف** البيانات من الطبقة الأعلى
- Wireshark يعرض **التفكيك** الكامل للطبقات
- تحليل الطبقات يساعد في **تشخيص المشاكل**

التطبيق (HTTP, FTP, DNS)

النقل (TCP, UDP)

الشبكة (IP, ICMP)

الوصلة (Ethernet)

تحليل طبقة Ethernet

- الطبقة **الأدنى** في نموذج TCP/IP
- تحتوي على **عناوين MAC** المصدر والوجهة
- تحديد **نوع البروتوكول** في الطبقة الأعلى
- تحليل EtherType لتحديد البروتوكول التالي
- كشف **الإطارات التالفة** أو غير الصالحة

تحليل طبقة IP

- تحتوي على **عناوين IP** المصدر والوجهة
- تحديد **إصدار البروتوكول** IPv4/IPv6
- تحليل **حقل TTL** (Time To Live)
- فحص **تجزئة الحزم** وإعادة تجميعها
- تحديد **البروتوكول** في الطبقة الأعلى

تحليل طبقة TCP

- تحليل **مصافحة TCP** الثلاثية
- فحص **أرقام المنافذ** المصدر والوجهة
- مراقبة **أرقام التسلسل** والإقرارات
- كشف **إعادة الإرسال** وفقدان الحزم
- تحليل **إشارات التحكم** SYN, ACK, FIN, RST

تحليل طبقة HTTP

- تحليل **طلبات HTTP** (GET, POST, PUT)
- فحص **رؤوس HTTP** والمعلومات الوصفية
- استعراض **محتوى الرسائل** والبيانات
- تحليل **كودات الحالة** 200, 404, 500
- استخدام **Follow TCP Stream** لإعادة بناء المحادثة

تحليل TCP Handshake

القسم الرابع: تحليل الحزم البروتوكولية

مراحل TCP Handshake

- **SYN**: العميل يبدأ الاتصال
- **SYN-ACK**: الخادم يستجيب ويوافق
- **ACK**: العميل يؤكد الاستلام
- بعد اكتمال المصافحة، يبدأ **نقل البيانات**

SYN 1 | SYN-ACK 2 | ACK 3

تفسير الحزم

- حزمة **SYN**: علم SYN=1، ACK=0
- حزمة **SYN-ACK**: علم SYN=1، ACK=1
- حزمة **ACK**: علم SYN=0، ACK=1
- مراقبة **أرقام التسلسل** الأولية ISN
- تحليل **حجم النافذة** Window Size

مشاكل شائعة في TCP Handshake

- **فشل المصافحة**: عدم استجابة الخادم
- **إعادة الإرسال**: فقدان حزم SYN/ACK
- **انتهاء المهلة** Timeout
- **رفض الاتصال** Connection Refused
- **ازدحام الشبكة** وتأخير الاستجابة

تطبيقات عملية

- **تشخيص مشاكل الاتصال** بالخوادم
- كشف **جدار الحماية** الذي يحجب المنافذ
- تحليل **أداء الشبكة** وسرعة الاستجابة
- مراقبة **محاولات الاختراق** والمسح الضوئي
- تحسين **إعدادات TCP** للأداء الأفضل

تحليل DNS و DHCP و TLS

القسم الرابع: تحليل الحزم البروتوكولية

تحليل حزم DNS

- تحليل **طلبات الاستعلام** Query
- فحص **الإجابات** Response
- مراقبة **أنواع السجلات** A, AAAA, MX, CNAME
- كشف **محاولات التسمية** غير الصالحة
- تحليل **زمن الاستجابة** للخوادم

تحليل حزم DHCP

- مراقبة **عملية الاكتشاف** DORA
- تحليل **الرسائل**: Discover, Offer, Request, Ack
- فحص **عناوين MAC** و IP المخصصة
- مراقبة **تجديد الإيجار** Lease Renewal
- كشف **الخوادم غير المصرح بها**

تحليل حزم TLS

- فحص **مصافحة TLS** Handshake
- تحليل **تبادل الشهادات** Certificate Exchange
- مراقبة **خوارزميات التشفير** المستخدمة
- فحص **إصدارات TLS** 1.2, 1.3
- تحليل **تغيير تشفير** Change Cipher Spec

العلاقة بين هذه البروتوكولات

- **DHCP** يوفر IP للجهاز للاتصال بالشبكة
- **DNS** يحول أسماء النطاقات إلى عناوين IP
- **TLS** يؤمن الاتصال بعد إنشائه
- تعمل **معاً** لتمكين الاتصال الآمن
- مشاكل في أي منها **تؤثر** على تجربة المستخدم

DHCP | DNS | TLS

تتبع الجلسات: Follow Stream

القسم الرابع: تحليل الحزم البروتوكولية

مفهوم تتبع الجلسات

- إعادة **بناء المحادثات** الكاملة
- تجميع **الحزم المتعلقة** بنفس الجلسة
- عرض **تسلسل البيانات** المتبادلة
- فصل **اتجاهات التدفق** المرسل/المستقبل
- تحويل **البيانات الثنائية** إلى نص مقروء

استخدام ميزة Follow Stream

- النقر **الأيمن** على حزمة TCP
- اختيار **Follow** > **TCP Stream**
- عرض **المحتوى الكامل** للجلسة
- إمكانية **التصفية** حسب المحتوى
- حفظ **الجلسة** كملف منفصل

تطبيقات عملية

- استخراج **المحتوى النصي** للمحادثات
- تحليل **بروتوكولات التطبيق** HTTP, FTP, SMTP
- كشف **بيانات الاعتماد** المنقولة
- فحص **محتوى الملفات** المنقولة
- تشخيص **مشاكل التطبيقات** عبر الشبكة

نصائح متقدمة

- استخدام **فلاتر العرض** قبل التتبع
- تفعيل **تمييز الألوان** للاتجاهات المختلفة
- تحويل **البيانات المشفرة** Base64
- دمج **عدة جلسات** متصلة
- استخدام **النسخ الاحتياطي** للجلسات المهمة

تحليل الجلسات المشفرة ومحاولات فك التشفير

القسم الرابع: تحليل الحزم البروتوكولية

تحليل جلسات SSL/TLS

- فحص **مصافحة TLS** Handshake
- تحليل **شهادات SSL** المتبادلة
- مراقبة **خوارزميات التشفير** المستخدمة
- فحص **إصدارات البروتوكول** TLS 1.2/1.3
- تحليل **تغيير تشفير** Change Cipher Spec

محاولات فك التشفير

- استخدام **ملفات المفاتيح** Key Log
- محاولة **كسر التشفير** بالقوة الغاشمة
- استغلال **ثغرات البروتوكول**
- استخدام **وسيط TLS** TLS Proxy
- تحليل **البيانات الوصفية** بدلاً من المحتوى

استخدام مفتاح فك التشفير

- إعداد **متغير البيئة** SSLKEYLOGFILE
- استيراد **ملفات المفاتيح** في Wireshark
- تكوين **إعدادات TLS** لفك التشفير
- استخدام **مفاتيح ما قبل التوزيع** Pre-Shared Keys
- فك تشفير **جلسات HTTPS** و FTPS

بيانات مشفرة ← مفتاح فك التشفير ← بيانات مفكوكة

تحديات وحلول

- **تعقيد التشفير** الحديث AES-256
- صعوبة **الحصول على المفاتيح** الصحيحة
- مشاكل **الأداء** عند فك التشفير
- قيود **قانونية وأخلاقية** في فك التشفير
- استخدام **بدائل** مثل تحليل البيانات الوصفية

الفرق بين Display Filtersg Capture

القسم الخامس: الفلاتر والتحكم في العرض

تعريف فلاتر الالتقاط

- تعمل على **مستوى kernel** قبل المعالجة
- تستخدم **صيغة BPF** Berkeley Packet Filter
- تمنع **وصول الحزم** إلى Wireshark
- تحسن **الأداء** وتقلل استخدام الموارد
- محدودة في **التعقيد** والقدرات

```
tcp port 80 and host 192.168.1.1
```

تعريف فلاتر العرض

- تعمل على **مستوى التطبيق** بعد الالتقاط
- تستخدم **صيغة Wireshark** الخاصة
- تخفي **عرض الحزم** غير المطابقة
- لا تؤثر على **الأداء** أثناء الالتقاط
- مرنة جداً و **قوية** في التحليل

```
tcp.port == 80 && ip.addr == 192.168.1.1
```

متى تستخدم كل نوع

- **فلاتر الالتقاط**:
- عند وجود **حركة مرور كثيفة**
- لالتقاط **بيانات محددة** فقط
- عند العمل على **موارد محدودة**
- **فلاتر العرض**:
- لتحليل **بيانات ملتقطة** بالفعل
- للبحث عن **أنماط معقدة**
- عند الحاجة لـ **مرونة** في التحليل

مقارنة وأمثلة عملية

الغرض	فلتر الالتقاط	فلتر العرض
HTTP traffic	tcp port 80	tcp.port == 80
IP address	host 192.168.1.1	ip.addr == 192.168.1.1
Protocol	icmp	icmp

كتابة فلاتر متقدمة

القسم الخامس: الفلاتر والتحكم في العرض

صياغة الفلاتر المتقدمة

- استخدام **النقاط** للوصول للحقول الفرعية
- تحديد **البروتوكولات** المتداخلة
- الوصول إلى **الحقول المخفية**
- فلترة حسب **القيم العددية**
- استخدام **النطاقات** والقيم النسبية

```
tcp.flags.syn == 1 && tcp.flags.ack == 0
```

استخدام العوامل المنطقية

- **AND** `&&` : تحقيق جميع الشروط
- **OR** `||` : تحقيق أي شرط
- **NOT** `!` : نفي الشرط
- **XOR** `^^` : تحقيق شرط واحد فقط
- استخدام **الأقواس** لتحديد الأولوية

(AND) &&	(OR) ||
(NOT) !	(XOR) ^^

فلاتر قائمة على المحتوى

- البحث عن **نصوص محددة** في الحزم
- فلترة حسب **القيم السداسية عشر**
- استخدام **التعبيرات النمطية** Regex
- فلترة حسب **الأحجام** والأطوال
- مقارنة **البايتات** والبتات

```
http contains "password" || frame contains
"00:11:22"
```

أمثلة معقدة

- فلترة **الاتصالات المشبوهة**:

```
tcp.port > 1024 && !tcp.analysis.flags
```

- كشف **محاولات الاختراق**:

```
http.request.method == "POST" &&
http.file_data
```

- تحليل **الأخطاء** في الشبكة:

```
tcp.analysis.retransmission ||
tcp.analysis.duplicate_ack
```

فلاتر خاصة بالبروتوكولات

القسم الخامس: الفلاتر والتحكم في العرض

فلاتر بروتوكول TCP/IP

- فلترة حسب **عناوين IP** المصدر والوجهة
- فلترة حسب **المنافذ** Ports
- فلترة حسب **أعلام TCP** Flags
- فلترة حسب **حجم النافذة** Window Size
- فلترة حسب **أرقام التسلسل** Sequence Numbers

```
ip.addr == 192.168.1.1 && tcp.port == 80
```

فلاتر بروتوكول HTTP

- فلترة حسب **نوع الطلب** GET, POST
- فلترة حسب **رمز الحالة** Status Code
- فلترة حسب **نوع المحتوى** Content-Type
- فلترة حسب **عنوان URL** أو المسار
- فلترة حسب **المضيف** Host

```
http.request.method == "POST" &&
http.content_type == "application/json"
```

فلاتر بروتوكول DNS

- فلترة حسب **نوع الاستعلام** Query Type
- فلترة حسب **نوع السجل** Record Type
- فلترة حسب **اسم النطاق** Domain Name
- فلترة حسب **رمز الاستجابة** Response Code
- فلترة حسب **خوادم DNS** المستخدمة

```
dns.qry.name contains "example.com" &&
dns.resp.code == 0
```

فلاتر بروتوكولات أخرى

- **DHCP**: فلترة حسب نوع الرسالة
- **ARP**: فلترة حسب عناوين MAC
- **ICMP**: فلترة حسب نوع الرسالة
- **TLS/SSL**: فلترة حسب إصدار التشفير
- **FTP**: فلترة حسب أوامر الملفات

```
dhcp.option.type == 53 || arp.src.hw_mac ==
00:11:22:33:44:55
```

الفلاتر المركبة AND / OR

القسم الخامس: الفلاتر والتحكم في العرض

استخدام العوامل AND/OR

- **AND (&&)**: تحقيق جميع الشروط معاً
- **OR (||)**: تحقيق أي شرط من الشروط
- دمج **شروط متعددة** في فلتر واحد
- تضييق **نطاق البحث** بشكل دقيق
- زيادة **فعالية** الفلترة

(&&) AND | **(||) OR**

ترتيب الأولويات

- **الأقواس** لها الأسبقية القصوى
- ثم **NOT (!)** ثم **AND (&&)**
- أخيراً **OR (||)** الأقل أولوية
- استخدام الأقواس لـ **تحديد الأولوية**
- تجنب **التباس** في النتائج

1. ( ) الأقواس
2. ! NOT
3. && AND
4. || OR

أمثلة عملية

- فلترة **HTTP** و **HTTPS** معاً:

```
tcp.port == 80 || tcp.port == 443
```

- فلترة **عنوان IP** و**منفذ** محددين:

```
ip.addr == 192.168.1.1 && tcp.port == 80
```

- فلترة **بروتوكولات متعددة**:

```
(tcp || udp) && ip.src == 10.0.0.1
```

نصائح للفلاتر الفعالة

- استخدام **الأقواس دائماً** للوضوح
- تجنب **التعقيد الزائد** في الفلتر
- اختبار **كل شرط** على حدة أولاً
- استخدام **التعليقات** للفلاتر المعقدة
- حفظ **الفلاتر الشائعة** للاستخدام المستقبلي

```
(tcp.port == 80 || tcp.port == 443) &&
!ip.src == 192.168.1.100
```

تخصيص الألوان لتتبع الحزم بسهولة

القسم الخامس: الفلاتر والتحكم في العرض

إعداد قواعد التلوين

- الوصول إلى **قائمة التلوين** من View > Coloring Rules
- إنشاء **قواعد جديدة** أو تعديل الموجودة
- تحديد **اسم القاعدة** والفلتر المرتبط
- اختيار **لون الخلفية** ولون النص
- تحديد **ترتيب الأولوية** للقواعد

تخصيص الألوان للبروتوكولات

- تمييز **بروتوكولات TCP** باللون الأزرق
- تمييز **بروتوكولات UDP** باللون الأخضر
- تمييز **بروتوكول HTTP** باللون البرتقالي
- تمييز **بروتوكول DNS** باللون الأصفر
- تمييز **بروتوكولات التشفير** باللون البنفسجي

TCP UDP HTTP DNS TLS

تخصيص الألوان للمحتوى

- تلوين **الحزم المشبوهة** باللون الأحمر
- تلوين **الأخطاء** باللون الأحمر الفاتح
- تلوين **إعادة الإرسال** باللون الأصفر
- تلوين **حزم التحكم** باللون الرمادي
- تلوين **المحتوى الحساس** باللون الأحمر الداكن

خطأ إعادة إرسال تحكم حساس

أفضل الممارسات

- استخدام **ألوان محايدة** لمعظم الحزم
- تخصيص **ألوان زاهية** للحزم المهمة
- تجنب **الألوان المتشابهة** للبروتوكولات المختلفة
- حفظ **قواعد التلوين** للاستخدام المستقبلي
- تفعيل **التلوين التلقائي** عند بدء Wireshark

عادي آمن خطر مهم تنبيه

حفظ الملفات بصيغ مختلفة (pcap, csv, json)

القسم السادس: التصدير والتقارير

صيغ الملفات المدعومة

- **pcap/pcapng**: الصيغة القياسية لحزم الشبكة
- **csv**: بيانات جدولية للتحليل الإحصائي
- **json**: بيانات منظمة للتطبيقات البرمجية
- **txt**: نص عادي للقراءة المباشرة
- **psml**: صيغة Wireshark للبيانات الوصفية

pcap | csv | json

متى تستخدم كل صيغة

- **pcap/pcapng**: للحفظ الكامل للبيانات الخام
- **csv**: للتحليل في Excel أو أدوات البيانات
- **json**: للتكامل مع تطبيقات الويب والبرمجة
- **txt**: للتقارير النصية البسيطة
- **psml**: للاستيراد مرة أخرى في Wireshark

حفظ الملفات بطرق مختلفة

- **File > Save**: حفظ جميع الحزم
- **File > Export Specified Packets**: حفظ مختار
- **File > Export Packet Dissections**: حفظ التفاصيل
- **File > Export Objects**: استخراج الملفات
- استخدام **سطر الأوامر tshark** للتصدير الآلي

مشاكل وحلول شائعة

- **ملفات كبيرة جداً**: تقسيمها إلى أجزاء أصغر
- **فقدان البيانات**: التأكد من اختيار الصيغة المناسبة
- **مشاكل التوافق**: استخدام pcapng بدلاً من pcap
- **صلاحيات الكتابة**: التحقق من صلاحيات المجلد
- **تلف الملفات**: التحقق من سلامة الملف قبل الحفظ

تحليل ملفات ضخمة وتجزئتها

القسم السادس: التصدير والتقارير

التعامل مع الملفات الكبيرة

- زيادة **ذاكرة النظام** المخصصة لـ Wireshark
- استخدام **فلاتر العرض** لتقليل البيانات المعروضة
- تفعيل **التحميل التدريجي** للملفات
- إغلاق **النوافذ غير الضرورية** أثناء التحميل
- استخدام **أجهزة قوية** للمعالجة

تقسيم الملفات

- استخدام **File > Export Specified Packets**
- التقسيم حسب **الزمن** أو عدد الحزم
- استخدام أدوات **سطر الأوامر** مثل `editcap`
- التقسيم حسب **عناوين IP** أو البروتوكولات
- حفظ الأجزاء في **ملفات منفصلة**

ملف كبير ← أجزاء أصغر

تحليل مقاطع محددة

- استخدام **فلاتر دقيقة** لتحديد المقاطع المطلوبة
- التركيز على **الفترات الزمنية** المهمة
- تحليل **الجلسات المحددة** فقط
- استخراج **الحزم ذات الصلة** بالحدث
- استخدام **الإشارات المرجعية** `Bookmarks`

تحسين الأداء

- تعطيل **تحليل البروتوكولات** غير الضرورية
- تقليل **عدد الحزم المعروضة**
- استخدام **الذاكرة المؤقتة** بكفاءة
- تفادي **العمليات المعقدة** على الملفات الكبيرة
- استخدام **أدوات خارجية** للمعالجة المسبقة

تصدير الحزم المحددة فقط

القسم السادس: التصدير والتقارير

تحديد الحزم المطلوبة

- استخدام **التحديد اليدوي** مع Ctrl/Cmd
- تطبيق **فلاتر العرض** لتحديد الحزم
- التحديد حسب **النطاق الزمني**
- التحديد حسب **البروتوكول** أو النوع
- استخدام **الإشارات المرجعية** Bookmarks

خيارات التصدير

- **File > Export Specified Packets**
- اختيار **نطاق الحزم** المطلوب تصديرها
- تحديد **صيغة الملف** المناسبة
- اختيار **تضمين** أو استبعاد معلومات معينة
- إمكانية **الضغط** للملفات الكبيرة

المحددة فقط | بعد الفلترة | حسب النطاق الزمني

تصدير البيانات الوصفية

- تصدير **معلومات الحزم** الأساسية
- استخراج **تفاصيل البروتوكولات**
- تصدير **البيانات الخام** Raw Data
- تضمين **الطوابع الزمنية** والمعلومات الإضافية
- حفظ **معلومات الواجهة** والالتقاط

أمثلة عملية

- تصدير **جلسة TCP** كاملة
- استخراج **حزم HTTP** فقط
- تصدير **محادثة DNS** محددة
- فصل **حزم التحكم** عن حزم البيانات
- إنشاء **تقرير** من حزم محددة

مشاركة ملفات التحليل مع فريق التحقيق

القسم السادس: التصدير والتقارير

إعداد الملفات للمشاركة

- تصدير **الحزم ذات الصلة** فقط
- تنظيم الملفات حسب **التصنيف**
- تضمين **معلومات السياق** الضرورية
- ضغط الملفات الكبيرة Compression
- إعداد **قائمة المحتويات** للملفات

حماية البيانات الحساسة

- إخفاء أو **تشويه** البيانات الشخصية
- إزالة **بيانات الاعتماد** والمفاتيح
- تشفير الملفات **بكلمة مرور** قوية
- تطبيق **قيود الوصول** للملفات
- الالتزام بـ **سياسات الخصوصية**

توثيق النتائج

- إنشاء **ملف ملخص** للتحليل
- توضيح **المنهجية** المستخدمة
- توثيق **الاستنتاجات** الرئيسية
- إرفاق **لقطات شاشة** توضيحية
- تضمين **التواريخ والأوقات** الدقيقة

أدوات المشاركة

- استخدام **المنصات الآمنة** للمشاركة
- التحكم في **صلاحيات الوصول**
- تفعيل **التتبع** للملفات المشتركة
- استخدام أدوات **التعاون** عن بعد
- توفير **الدعم الفني** لاستخدام الملفات

1 التحضير — 2 الأمان — 3 التوثيق — 4 المشاركة

مقارنة الجلسات وتحليل التباين الزمني

القسم السادس: التصدير والتقارير

مقارنة الجلسات المختلفة

- استخدام **ملفات متعددة** للمقارنة
- تحليل **اختلافات الأداء** بين الجلسات
- مقارنة **سلوك البروتوكولات**
- تحديد **التغيرات** في أنماط الاتصال
- استخدام أدوات **الرسوم البيانية** للمقارنة

جلسة 1 | جلسة 2

تحليل التوقيتات الزمنية

- قياس **زمن الاستجابة** Response Time
- تحليل **الفواصل الزمنية** بين الحزم
- مراقبة **تأخير الشبكة** Latency
- حساب **معدل نقل البيانات**
- تحديد **الاختناقات** في الأداء

11ms | 45ms | 12ms | 10ms

اكتشاف الأنماط

- تحديد **الدورات المتكررة** في الاتصالات
- كشف **الشذوذ** في الأنماط المعتادة
- تحليل **التغيرات الموسمية** في حركة المرور
- مراقبة **اتجاهات الأداء** عبر الزمن
- استخدام **التحليل الإحصائي** للأنماط

تطبيقات عملية

- **تحسين أداء** التطبيقات والشبكات
- كشف **الهجمات السيبرانية** عبر تحليل الأنماط
- تحديد **أوقات الذروة** في استخدام الشبكة
- تخطيط **السعة** والموارد المطلوبة
- إنشاء **خطوط أساسية** للأداء الطبيعي

كشف ARP Spoofing

القسم السابع: استخدام Wireshark في الأمن السيبراني

شرح هجوم ARP Spoofing

- هجوم **انتحال الهوية** على مستوى الشبكة
- يرسل المهاجم **رسائل ARP مزيفة**
- يربط **عنوان MAC** الخاص به بعنوان IP للضحية
- يتمكن من **اعتراض البيانات** المرسلة
- يمكن تنفيذ **هجمات MITM** Man-in-the-Middle

مؤشرات الهجوم في Wireshark

- وجود **رسائل ARP متكررة** لنفس IP
- تغيير **عناوين MAC** لنفس IP بشكل مفاجئ
- رسائل ARP **غير مطلوبة** Gratuitous ARP
- حركة مرور ARP **غير طبيعية**
- وجود **عناوين MAC متعددة** لنفس IP

تحليل الحزم المشبوهة

- فلترة حركة المرور بـ **arp**
- فحص **نوع رسالة ARP** Request/Reply
- مقارنة **عناوين MAC** مع السجلات المعروفة
- مراقبة **تواتر الرسائل** غير الطبيعي
- استخدام **إحصائيات ARP** في Wireshark

الوقاية والاستجابة

- تنفيذ **إدخالات ARP ثابتة** Static ARP
- استخدام **برامج الحماية** من هجمات ARP
- تفعيل **ميزات الأمان** في المعدات الشبكية
- مراقبة **الشبكة بشكل مستمر**
- عزل **الأجهزة المصابة** فوراً

كشف DNS Poisoning

القسم السابع: استخدام Wireshark في الأمن السيبراني

شرح هجوم DNS Poisoning

- هجوم يستهدف **تسميم ذاكرة DNS**
- يحقن المهاجم **سجلات DNS مزيفة**
- يحول المستخدمين إلى **مواقع ضارة**
- يمكن سرقة **بيانات الاعتماد** والمعلومات
- أنواع: DNS Cache Poisoning و DNS Spoofing

الضحية ← المهاجم ← خادم DNS

مؤشرات الهجوم في Wireshark

- استجابات DNS **سريعة جداً**
- استجابات DNS من **خوادم غير معروفة**
- عناوين IP **غير متوقعة** في الاستجابات
- عدد كبير من **استجابات DNS** لطلب واحد
- تكرار **نفس استجابة DNS** بشكل غير طبيعي

تحليل حزم DNS المشبوهة

- فلترة حركة المرور بـ **dns**
- فحص **نوع الاستعلام** والاستجابة
- مقارنة **عناوين IP** مع القوائم البيضاء
- مراقبة **زمن الاستجابة** Response Time
- استخدام **إحصائيات DNS** في Wireshark

الوقاية والاستجابة

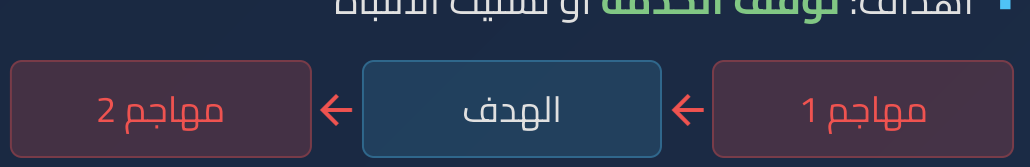
- استخدام **DNSSEC** للتحقق من الاستجابات
- تفعيل **DNS over HTTPS** أو DNS over TLS
- تحديث **برامج مكافحة الفيروسات**
- مراقبة **سجلات DNS** بشكل دوري
- عزل **الأجهزة المصابة** فوراً

تحليل DDoSg SYN Flood

القسم السابع: استخدام Wireshark في الأمن السيبراني

شرح هجمات DDoSg SYN Flood

- **SYN Flood**: إغراق الخادم بطلبات اتصال مزيفة
- **DDoS**: هجوم من مصادر متعددة Distributed
- استنزاف **موارد الخادم** حتى يتعطل
- منع **المستخدمين الشرعيين** من الوصول
- أهداف: **توقف الخدمة** أو تشتيت الانتباه



مؤشرات الهجوم في Wireshark

- عدد كبير من حزم **SYN** بدون **ACK**
- حزم من **عناوين IP متنوعة** لنفس المنفذ
- حجم **غير طبيعي** لحركة المرور
- زيادة مفاجئة في **طلبات الاتصال**
- فشل **مصافحة TCP** الثلاثية

تحليل أنماط الهجوم

- فلترة حركة المرور بـ **tcp.flags.syn == 1**
- تحليل **مصدر الحزم** وتوزيعها الجغرافي
- مراقبة **المنافذ المستهدفة**
- قياس **معدل الحزم** في الثانية
- استخدام **إحصائيات TCP** في Wireshark

زيادة مفاجئة | مصادر متعددة | فشل المصافحة

الاستجابة والتخفيف

- تفعيل **SYN Cookies** على الخوادم
- استخدام **جدار حماية** متخصص WAF
- زيادة **سعة الخادم** أو استخدام موازنة التحميل
- التعاون مع **مزود الخدمة** لمنع الهجوم
- استخدام **خدمات الحماية** من DDoS

تتبع هجمات Man-in-the-Middle

القسم السابع: استخدام Wireshark في الأمن السيبراني

شرح هجمات Man-in-the-Middle

- المهاجم **يتوسط** بين الطرفين
- يعترض **الاتصالات** بشكل خفي
- يمكن **قراءة وتعديل** البيانات
- أنواع: ARP Spoofing ، DNS Spoofing
- قد لا يلاحظها **المستخدمون**

مؤشرات الهجوم في Wireshark

- تكرار **رسائل ARP** لنفس IP
- استجابات DNS من **خوادم غير معروفة**
- شهادات SSL/TLS **غير صالحة**
- تغير **عناوين MAC** بشكل متكرر
- اتصالات مزدوجة **لنفس الجلسة**

تحليل الجلسات المخترقة

- فحص **مصافحة TCP** الثلاثية
- تحليل **شهادات SSL/TLS**
- مراقبة **تسلسل الحزم** غير الطبيعي
- استخدام **Follow Stream** لفحص المحادثات
- تحليل **البيانات الوصفية** للحزم

شهادات غير صالحة | اتصالات مزدوجة

الوقاية والاستجابة

- استخدام **HTTPS** بدلاً من HTTP
- تفعيل **HSTS** في المتصفحات
- استخدام **شبكات VPN** موثوقة
- تفعيل **التحقق من الشهادات**
- عزل **الأجهزة المشبوهة** فوراً

استرجاع الملفات والصور من الشبكة

القسم السابع: استخدام Wireshark في الأمن السيبراني

استخراج الملفات من الحزم

- استخدام **File > Export Objects**
- اختيار **نوع الملف** المطلوب استخراجه
- استخدام **Follow TCP Stream** لإعادة بناء الملفات
- حفظ الملفات المستخرجة **بصيغها الأصلية**
- استخراج **البيانات الثنائية** من الحزم

تحليل بروتوكولات نقل الملفات

- **HTTP**: تحميل الملفات عبر الويب
- **FTP**: بروتوكول نقل الملفات
- **SMTP**: نقل الملفات كملحقات بريد
- **SMB**: مشاركة الملفات في الشبكات المحلية
- **TFTP**: نقل الملفات البسيط

صور | نصوص | فيديو

أدوات مساعدة

- **NetworkMiner**: استخراج الملفات تلقائياً
- **Xplico**: إعادة بناء بيانات التطبيقات
- **Foremost**: استرجاع الملفات المحذوفة
- **Scalpel**: استخراج الملفات من البيانات الثنائية
- **Bulk Extractor**: تحليل الملفات الكبيرة

قيود وتحديات

- **الملفات المشفرة** يصعب استرجاعها
- **الملفات المضغوطة** تحتاج لفك الضغط
- **الملفات المجزأة** تحتاج لإعادة تجميع
- مشاكل **فقدان الحزم** أثناء النقل
- قيود **قانونية وأخلاقية** في الاستخدام

تحديد الأجهزة المهددة في الشبكة الداخلية

القسم السابع: استخدام Wireshark في الأمن السيبراني

تحليل سلوك الأجهزة

- مراقبة **نمط الاتصالات** لكل جهاز
- تحليل **البروتوكولات** المستخدمة
- مراقبة **حجم البيانات** المنقولة
- تتبع **التوقيتات** غير المعتادة
- مقارنة السلوك الحالي **بالسلوك الأساسي**

مؤشرات الأجهزة المخترقة

- اتصالات مع **عناوين IP غريبة**
- زيادة **حركة المرور** بشكل مفاجئ
- استخدام **بروتوكولات غير معتادة**
- محاولات **مسح الشبكة** Port Scanning
- اتصالات مع **خوادم معروفة** ضارة

عادي | مخترق | شبكة

تحليل الاتصالات المشبوهة

- فلترة حركة المرور حسب **عنوان MAC**
- تحليل **الجلسات النشطة** للجهاز
- فحص **البيانات الوصفية** للحزم
- مراقبة **محاولات الاتصال** الفاشلة
- استخدام **إحصائيات النهاية** Endpoint Statistics

إجراءات الاستجابة

- **عزل الجهاز** فوراً عن الشبكة
- إجراء **فحص شامل** للجهاز
- تحديث **برامج الحماية** والتصحيحات
- مراجعة **السجلات** والنشاطات
- إعادة **الاتصال بالشبكة** بعد التأكد من الأمان

تحليل شبكة منزلية

القسم الثامن: سيناريوهات عملية ودراسات حالة

إعداد بيئة الشبكة المنزلية

- توصيل جهاز **الكمبيوتر** بالشبكة
- تثبيت **Wireshark** على الجهاز
- تحديد **واجهة الشبكة** المراد مراقبتها
- تفعيل **وضع المراقبة** Promiscuous Mode
- التأكد من **الصلاحيات** اللازمة

كمبيوتر | راوتر | أجهزة أخرى

تحليل الأجهزة المتصلة

- استخدام **فلتر ARP** لاكتشاف الأجهزة
- تحديد **عناوين MAC** للأجهزة المتصلة
- تعريف **نوع الجهاز** من خلال العنوان
- مراقبة **الجهاز الجديد** عند الاتصال
- إنشاء **قائمة جرد** بالأجهزة الشبكية

تحليل حركة المرور

- تصنيف **البروتوكولات** المستخدمة
- تحليل **حجم البيانات** لكل جهاز
- مراقبة **التوقيتات** الذروة للاستخدام
- تحديد **التطبيقات** الأكثر استخداماً
- رصد **الاتصالات الخارجية**

اكتشاف المشاكل الأمنية

- كشف **الأجهزة غير المصرح بها**
- مراقبة **محاولات الاختراق**
- تحليل **الاتصالات المشبوهة**
- فحص **إعدادات الراوتر** والأمان
- تقييم **قوة كلمات المرور** للشبكة

شبكة غير محمية | جهاز غير معروف

تحليل شبكة مؤسسة وهمية

القسم الثامن: سيناريوهات عملية ودراسات حالة

تصميم بيئة المؤسسة

- تقسيم الشبكة إلى **شرائح** VLANs
- فصل **الأقسام** عن بعضها
- إنشاء **منطقة DMZ** للخوادم العامة
- تطبيق **سياسات الأمان** على جميع المستويات
- نشر **أجهزة المراقبة** في النقاط الرئيسية

الموظفون | الإدارة | **الخوادم** | DMZ

تحليل حركة المرور التجارية

- تصنيف **التطبيقات** المستخدمة
- تحليل **أحجام البيانات** بين الأقسام
- مراقبة **أوقات الذروة** للاستخدام
- تحديد **البروتوكولات** السائدة
- قياس **أداء الشبكة** وتحديد الاختناقات

تحليل الاتصالات الخارجية

- مراقبة **الاتصالات الصادرة** للإنترنت
- تحليل **الزيارات** للمواقع الخارجية
- فحص **اتصالات VPN** عن بعد
- مراقبة **البريد الإلكتروني** الخارجي
- تحليل **خدمات السحابة** المستخدمة

اكتشاف التهديدات المحتملة

- كشف **محاولات الاختراق** من الخارج
- مراقبة **البيانات الحساسة** المنقولة
- تحليل **الاتصالات غير المصرح بها**
- فحص **سلوك الموظفين** المشبوه
- تطبيق **إجراءات الاستجابة** للحوادث

تصيد احتيالي | تسريب بيانات

اكتشاف خرق بيانات داخلي

القسم الثامن: سيناريوهات عملية ودراسات حالة

مؤشرات خرق البيانات

- زيادة **غير طبيعية** في حجم البيانات المنقولة
- اتصالات من **خوادم داخلية** إلى خارجية
- نشاط **غير معتاد** في أوقات غير العمل
- استخدام **بروتوكولات** غير معتادة
- محاولات **الوصول** لملفات حساسة

زيادة البيانات | نشاط ليلي

تحليل الاتصالات غير المعتادة

- فلترة حركة المرور حسب **البروتوكولات**
- تحليل **الاتجاه** غير الطبيعي للبيانات
- فحص **المنافذ** غير المعروفة
- مراقبة **تكرار الاتصالات**
- استخدام **إحصائيات التدفق** Flow Statistics

تحديد مصدر الخرق

- تتبع **عنوان IP** المصدر
- تحليل **سلوك المستخدم** على الشبكة
- فحص **الجهاز المصدر** للبرامج الضارة
- مراجعة **سجلات النظام** والنشاطات
- تحديد **طريقة الاختراق** المستخدمة

1 الاكتشاف | 2 التحليل | 3 المصدر | 4 الاحتواء

توثيق النتائج

- تسجيل **جميع الأدلة** الرقمية
- إنشاء **تقرير مفصل** بالحادث
- توثيق **الإجراءات** المتخذة
- حفظ **ملفات الالتقاط** كدليل
- توصيات **لتحسين الأمان** مستقبلاً

تحليل برمجيات خبيثة تتصل بخادم C2

القسم الثامن: سيناريوهات عملية ودراسات حالة

تحديد سلوك البرمجيات الخبيثة

- مراقبة **الاتصالات غير المعتادة**
- تحليل **العمليات المشبوهة**
- كشف **التغييرات** في النظام
- فحص **الملفات** والعمليات الجديدة
- مراقبة **استخدام الموارد** غير الطبيعي

اتصالات دورية | تعديل السجل

تحليل اتصالات C2

- فلترة حركة المرور حسب **عناوين IP** المشبوهة
- تحليل **البروتوكولات** المستخدمة في الاتصال
- فحص **التشفير** والبيانات المخفية
- مراقبة **توقيتات الاتصال** وتكرارها
- تحليل **البيانات المنقولة** بين الجهاز والخادم

الجهاز المصاب ← خادم C2

استخراج مؤشرات الاختراق

- تسجيل **عناوين IP** للخوادم C2
- تحديد **المنافذ** المستخدمة في الاتصال
- استخراج **البروتوكولات** والتقنيات المستخدمة
- تحليل **البيانات الوصفية** للبرمجيات الخبيثة
- إنشاء **قائمة مؤشرات** IOCs للكشف

الاستجابة والاحتواء

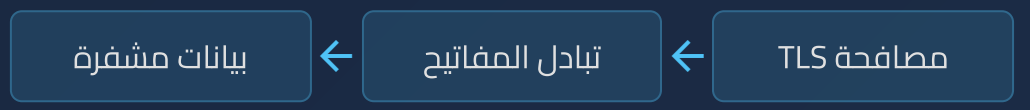
- **عزل الجهاز** المصاب فوراً
- حظر **عناوين IP** الخاصة بخوادم C2
- إجراء **فحص شامل** للجهاز
- تحديث **برامج الحماية** والتصحيحات
- مراجعة **السياسات الأمنية** وتحسينها

تحليل جلسات اتصال مشفرة HTTPS

القسم الثامن: سيناريوهات عملية ودراسات حالة

تحليل اتصالات TLS/SSL

- فحص **مصافحة TLS** Handshake
- تحليل **إصدار البروتوكول** TLS 1.2/1.3
- مراقبة **خوارزميات التشفير** المستخدمة
- فحص **تغيير تشفير** Change Cipher Spec
- تحليل **البيانات الوصفية** للاتصال المشفر



تحليل شهادات SSL

- فحص **صلاحية الشهادة** وتاريخ انتهائها
- تحليل **جهة الإصدار** Certificate Authority
- التحقق من **سلسلة الشهادات**
- كشف **الشهادات المزيفة** أو غير الموثوقة
- تحليل **الخوارزميات** المستخدمة في التوقيع

صالحة | منتهية | مزيفة

محاولات فك التشفير

- استخدام **ملفات المفاتيح** Key Log
- استيراد **مفاتيح الجلسة** في Wireshark
- محاولة **كسر التشفير** بالقوة الغاشمة
- استغلال **ثغرات البروتوكول**
- استخدام **وسيط TLS** TLS Proxy

تحليل التدفقات المشفرة

- تحليل **البيانات الوصفية** للتدفقات المشفرة
- مراقبة **حجم البيانات** ونمط النقل
- تحديد **التوقيتات** غير الطبيعية
- كشف **الاتصالات المتكررة**
- استخدام **إحصائيات TLS** في Wireshark

مقارنة سلوك الأجهزة في بيئة اختبار

القسم الثامن: سيناريوهات عملية ودراسات حالة

إعداد بيئة الاختبار

- إنشاء **شبكة معزولة** للاختبار
- تجهيز **الأجهزة** المراد اختبارها
- تثبيت **Wireshark** على جهاز المراقبة
- تكوين **المرآب** Port Mirroring
- تحديد **سيناريوهات الاختبار** المطلوبة

جهاز 1 | مراقب | جهاز 2

تحليل سلوك الأجهزة

- مراقبة **حركة المرور** لكل جهاز
- تحليل **البروتوكولات** المستخدمة
- قياس **أداء الشبكة** لكل جهاز
- تسجيل **الاستجابات** للاستشارات المختلفة
- مقارنة **استهلاك الموارد** بين الأجهزة

اكتشاف الأنماط غير المعتادة

- تحديد **الاتصالات غير المتوقعة**
- كشف **السلوك المتكرر** أو غير الطبيعي
- مراقبة **التوقيتات** غير المعتادة للنشاط
- تحليل **البيانات غير المشفرة** المرسلة
- مقارنة **السلوك الأساسي** مع السلوك الحالي

توقيتات غير عادية | اتصالات مشبوهة

توثيق النتائج

- إنشاء **تقارير مفصلة** بالاختبارات
- تسجيل **جميع الملاحظات** والاستنتاجات
- حفظ **ملفات الالتقاط** كدليل
- إنشاء **مقارنات** بين الأجهزة المختلفة
- تقديم **توصيات** لتحسين الأداء والأمان