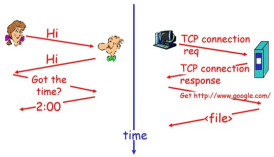
NMAP:

```
> nmap -sP 192.163.178.*
```

البروتوكول - Protocol

ما معنى بروتوكول Protocol ؟

هو لغة التواصل بين أجهزة الكمبيوتر المتصلة عبر الشبكة، بهدف تبادل المعلومات.

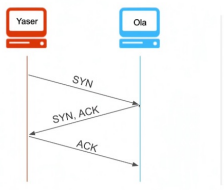


مصطلحات:

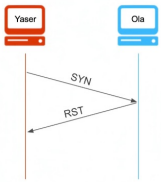
Protocol Suite
مجموعة من البروتوكولات

Protocol Stack
مجموعة بروتوكولات ترسل وتستقبل البيانات

أساليب الفحص

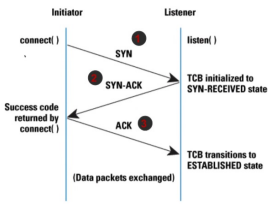


منفذ مفتوح Open Port



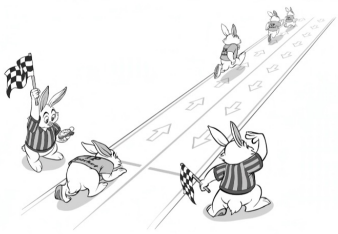
منفذ مغلق Close Port

Three Way HandShake



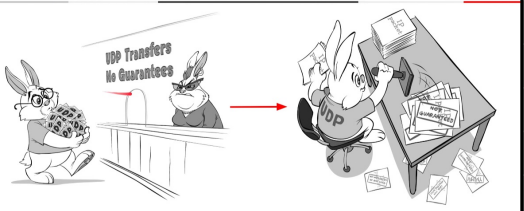
TCP

TCP Protocol



UDP

UDP Protocol

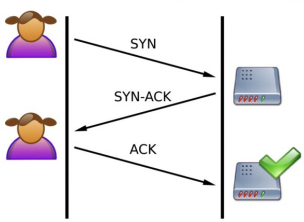


TCP Protocol

معنى TCP ؟

TCP : Transmission Communication Protocol

هو بروتوكول نقل الاتصال أي أن مهمة هذا البروتوكول هي نقل البيانات عبر الشبكة. بروتوكول TCP يتحقق من وصول الارسال بين الحواسيب كما يتأكد من أن جميع الرزم التي أرسلت قد تم استقبالها من الجهاز الآخر وفي حالة لم تصل هذه الرزم يقوم TCP بارسالها مرة ثانية وإذا تم الإستلام يأخذ شهادة مصادقة ويقوم بارسال الدفعة التالية



UDP Protocol

Port	Protocol
7	Echo
9	Discard
11	Users
13	Daytime
17	Quote
19	Chargen
53	Nameserver
67	Bootps
68	Bootpc
69	TFTP
111	RPC
123	NTP

معنى UDP ؟

UDP : User Datagram Protocol

و تعني بروتوكول بيانات المستخدم.

كيف يعمل بروتوكول UDP ؟

يقسم الرسالة إلى عدة أجزاء ويرسل هذه الأجزاء إلى المستقبل مع وضع عنوان المستقبل في كل جزء من أجزاء الرسالة وهذه الأجزاء لا تسلك نفس الطريق في الشبكة لذلك لايوجد اي ضمان لوصول الرسالة صحيحة 100% لأن هدف هذا البروتوكول هو إيصال الرسالة بأسرع وقت وليس وصولها صحيحة.

TCP Protocol

مميزات TCP ؟

- موثوق : يضمن وصول البيانات و بدون أخطاء.
- ينشئ رابطة قبل الإرسال : يقوم بعملية المصافحة Three Way Handshake.
- يقوم بترقيم الحزم و يرسلها بالترتيب.
- يتحكم في تدفق البيانات : لا يرسل إلا بعد استلام الجهاز الآخر البيانات.

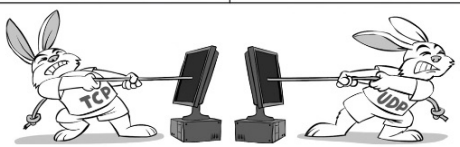
Port Number	Protocol	Application
20	TCP	FTP data
21	TCP	FTP control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP, TCP	DNS
67, 68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL
16,384–32,767	UDP	RTP-based Voice (VoIP) and Video

يمكن تغيير الـ default port لكن البوت كان لا يتغير

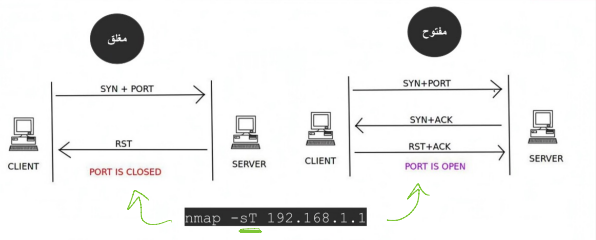
المدرب
ياسر العصيفير

الفرق بين TCP and UDP

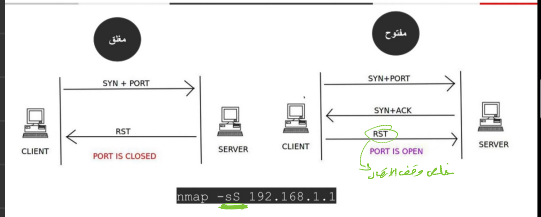
بروتوكول TCP	بروتوكول UDP
يرسل البيانات دفعة واحدة وبعد التحقق من استلامها يرسل دفعة أخرى	يقسم الرسالة المراد إرسالها إلى وحدات مما يسرع وصول البيانات
TCP يقدم لنا ضمانا أن التوصيل سليم تماما وإذا حدث خطأ فإنه يعيد الإرسال حتى يكون صحيحا	لا يقدم لنا أي ضماناً لوصول البيانات سليمة لأن هدف هذا البرتوكول هو توصيل الرسالة المطلوبة بسرعة
سرعة نقل البيانات أقل من UDP لأن يتم التأكد من سلامة وصول البيانات	تناقل البيانات باستعمال UDP أسرع لأنه لا يتحقق من صحة المعلومة



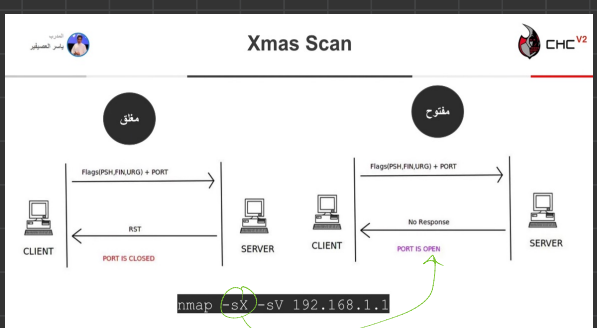
TCP Full Open Scan



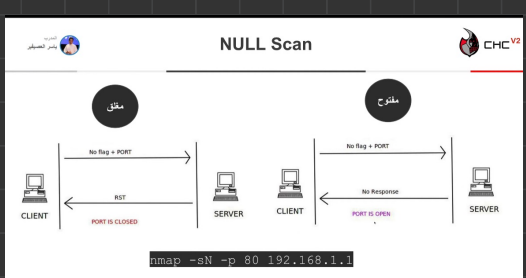
TCP Half Open Scan (Stealth Scan)



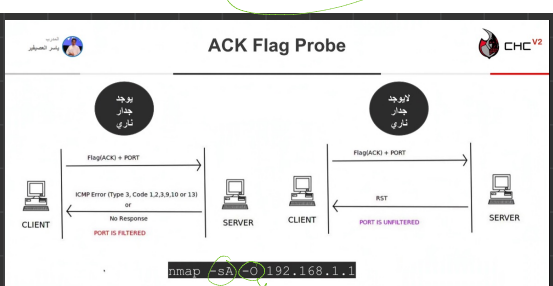
Xmas Scan



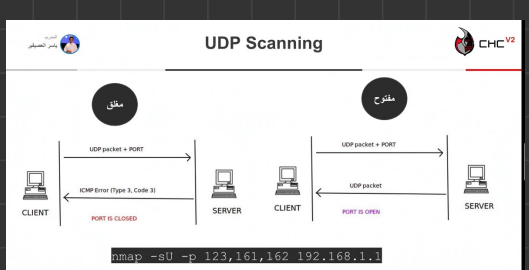
NULL Scan



ACK Flag Probe



UDP Scanning

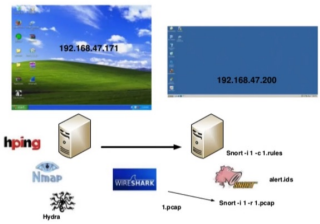


IDS

ماهو IDS ؟

Intrusion Detection System

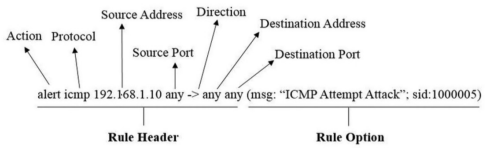
نظام حماية يشبه مضاد الفيروسات الموجود على أجهزتنا يقوم بتحليل كل Traffic عبر الشبكة. الهدف من IDS هو تحليل الـ Traffic وتحذيرنا في حالة كان هناك خطر محتمل أو هجمة محتملة تستهدف جهازنا أو شبكتنا.

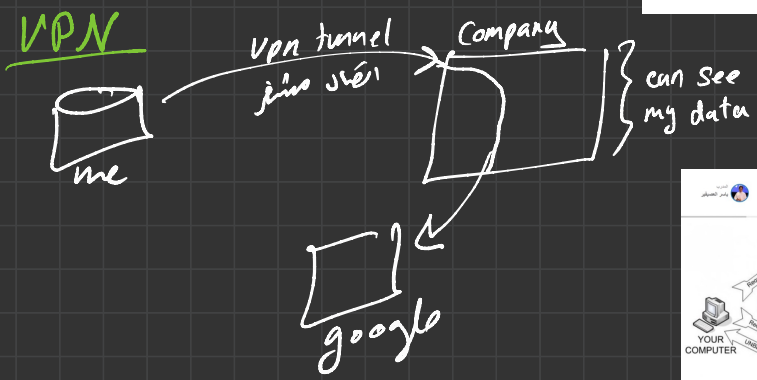


أهميته في عالم الانترنت؟

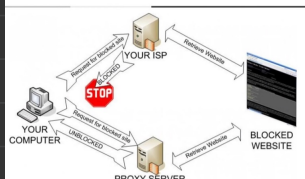
- كشف الثغرات الموجودة في أنظمة الحماية
- أرشفة كل أنواع التهديدات التى تحدث للشبكة
- تحديد الأخطاء التي وقع فيها مسؤولين الحماية وتصحيحها

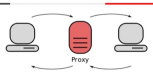
IDS Rule





Proxy





ماهو تعريف Proxy ؟

بروكسي هو وسيط يتم تطبيقه على الخوادم يستخدم كوسيط بين المستخدم والإنترنت ومن مميزاته السرعة والأمان والحماية بلا حدود.

مكن غير مشفر

VPN

ماهو تعريف VPN ؟

الـ VPN هي عبارة عن توصيل شبكتين أو جهازين عن طريق الإنترنت، حيث تقوم بتشفير البيانات لحمايتها من السرقة وإخفاء هوية المستخدم.

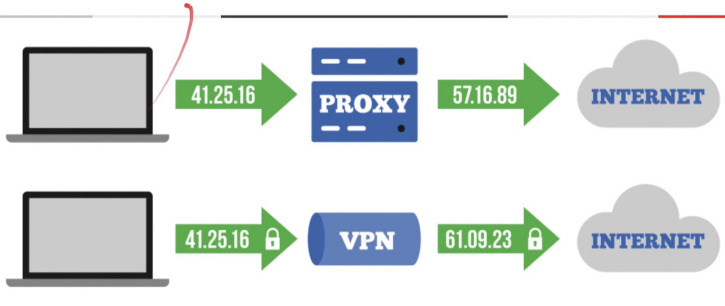
مميزات VPN ؟

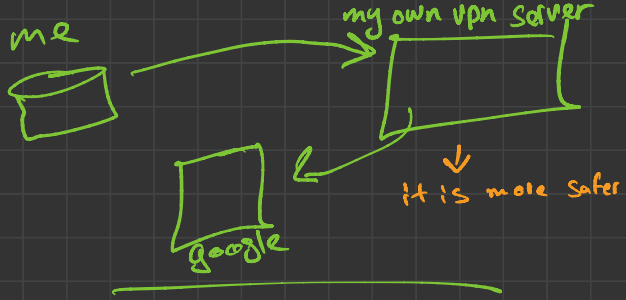
- لن تستطيع الشركة المزودة لخدمة الإنترنت التطفل على بياناتك.
- تصفح الإنترنت بأكثر أماناً وسرية.
- منع تتبع المخترقين والمتطفلين.
- تشفير جميع البيانات التي تستخدمها على الإنترنت.

Web Proxy

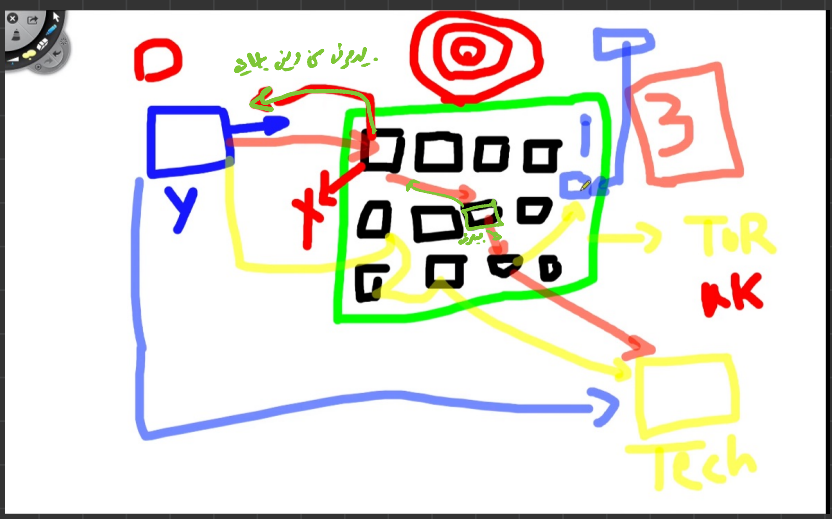
on github

VPN vs Proxy





* Tor explained in CEH.



read also nmap book