ShieldsUP!

المراجع

1- https://www.grc.com/x/ne.dll?bh0bkyd2
/2- http://www.technoobogy.com/2005/09/22/shieldsup-free-internet-security-checkup
3- http://www.grcsucks.com/shieldsup.html
4-http://www.hewett.co.nz/gcg/ShieldsUp.html
5- Security+ Guide to Networking Security Fundamentals, Second Edition BY Mark Ciampa

جدول المحتويات

يعد نظام ShieldsUP! أحد الأنظمة المستخدمة لكشف عن سلامة الأجهزة من الاختراقات ويقوم باختبار سلامة المنافذ وهل هي آمنة أم لا . بداية سنقوم بكتابة مقدمة عن نظامShieldsUP! وبعد ذلك سنقوم بشرح كيفية استعمال نظامShieldsUP! والذي ينتج عنة تقيم المنفذ بأحد المصطلحات التالية (Stealth!,Closed,OPEN!). وسوف نقوم بشرح كل مصطلح على حدة والمعنى المقصود من كل مصطلحة.

أحمد معيض القحطاني
421007091

مقدمة

يعد نظام ShieldsUP! أحد الأنظمة المجانية المستخدمة للكشف عن سلامة الأجهزة من الاختراقات ويقوم باختبار سلامة المنافذ وهل هي آمنة أم لا وينتج عن هذا الاختبار تقيم المنفذ بأحد المصطلحات التالية:

1-Stealth!
2-Closed
3-OPEN!

ويمثل كل مصطلح حاله المنفذ واحتمال الخطر الذي قد يحصل من هذا المنفذ مما يمكن مستخدم النظام من التعرف على المنافذ التي قد تستغل لتسلل إلى جهازه واتخاذ الإجراءات المناسبة لمنع هذا الاختراق .

كيفية استخدام نظام ShieldsUP!

1-ادخل على الموقع https://www.grc.com/x/ne.dll?bh0bkyd2
2-ثم اضغط على زر Proceed أسفل الصفحة
3-اذهب الى مربع ShieldsUP!! Services
4 -واضغط على زر Common Ports

وستظهر النتيجه كالتالي:

Port	Service	Status	Security Implications
21	FTP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
23	Telnet	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
25	SMTP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
79	Finger	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
80	HTTP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!

Stealth!

عند ظهور كلمة Stealth! امام المنفذ فهذا يعني ان المنفذ مخفي ولايمكن الاتصال بة وهذا يعني ان جدار الحماية قد قام بإغلاق جميع المنافذعن الا شخاص الغير مصرح لهم وجعلها مخفية وغير مكتشفة ويقوم النظام بإرسال اربعة طلبات اتصال على المنفذ وينتظر الرد إذا لم يتم استقبال اي يرد يعتبر النظام المنفذ Stealth!.

Closed

عند ظهور كلمة Closed امام المنفذ فهذا يعني المنفذ مغلق وهذاويعني انة لا يمكن الاتصال بك الا عن طريق برامج الاختراق مثل السب سفن وغيره ويعتبر الافضل بعد Stealth! وعند عمل المسح على المنفذ يظهر المنفذ لكنة يكون مغلق ولايمكن الاتصال بة.

OPEN!

عند ظهور كلمة OPEN! امام المنفذ فهذا يعني المنفذ مفتوح ,ويكون المنفذ مفتوح في حالتين:

1- هناك خدمة تعمل على هذا المنفذ المفتوح:
كما هو الحال عند الاتصال بخدمة الانتر نت ويكون الجهاز عرضة للهجوم من خلال هذا المنفذ ونستطيع تقليل خطر الهجوم بستخدام جدار الحماية وبرامج مكافحة الفايروس .

2- لاتوجد خدمة تعمل على هذا المنفذ المفتوح:
في هذة الحالة يكون المنفذ مفتوح من دون استخدامة للاتصال بخدمة معينة, وغالبا يكون هذا المنفذ مفتوح من دون معرفة مستخدم الجهاز مما يجعل هذا المنفذ صيدا سهلا لبرامج التجسس والمخترقين .

عندما يكون الكمبيوتر الذي تستخدمه مكشوفا أمام العالم، وبمقدور أي شخص لديه بعض المعلومات عن الاختراق، أن يسيطر على جهازك بسهولة، هناك أيضا وسائل ميسره تجعله في مأمن من القراصنة والمخترقين، وأولها أن تحمله برنامجا خاصا بمقاومة الاختراق، وهناك برامج مجانية لهذا الغرض، منها برنامج زون الارم الذي تجده على العنوان التالي http://www.zonelabs.com/ : فهو يقوم بعمل جيد لحجب المخترقين.

وسائل وقاية

بالإضافة إلى برنامج الحماية من الاختراق، هناك وسائل وقاية مختلفة، تسد الباب أمام محاولات المخترقين، وهي مذكورة على إحدى صفحات الموقع السابق:
http://grc.com/su-fixit.htm
وتدور حول كيفية إيقاف أو تعطيل بعض الوظائـــف في وندوز مثل file and printer sharing في وندوز، كما يقدم الموقع نصائح حول كيفية اختيار كلمات مرور بحيث لا يمكن فكها ومعرفتها من قبل الآخرين.
رغم ذلك، ليست هذه الوسائل من الوقاية رادعة، وكافية تماما، ولكنها توفر مستوى جيدا من المناعة والأمن على الإنترنت.