$# AciD-WarZ #$
^^^^^^^^^^^^^^^^^^^
Found At :: ACIDBURN_EG@Hotmail.Com
^^^

السلام عليكم و رحمه الله و بركاته :
اليوم سوف نتطلع الى اداه فى النت ورك و هى اداه هامه جدا تستخدمها معظم السرفرات على الانترنت و هذه الاداه هى ال Secure Shell اى ال SSh ::

و لنبدأ الان الحديث عنها ::

ما هى ال SSh ؟
==========
الsecure shell هى اداه (برنامج) للاتصال و الدخول الى كمبيوتر او جهاز اخر على النت ورك لتنفيذ اوامر او مهام معينه داخل هذا الجهاز اى و هو الاتصال عن بعد remotely connection و تستخدم ايضا فى نقل الملفات من كمبيوتر الى اخر و هى تقدم توثيق قوى و اتصال امن جدا فى قنوات الاتصال الغير امنه و هى تعتبر كبديل جيد جدا لادوات تستعمل لنفس الغرض فى يونكس مثل (rlogin,rsh and rcp).
و تقدم ايضا ال secure shell اتصال امن جدا لشحنات اتصالات ال tcp كونيكشن .

و هنا يأتى سؤال مهم :: و السؤال هو ::

لماذا يفضل استخدام ال secure shell على الادوات الاخرى التى يطلق عليها r- commands فى يونكس
==========
==========
كالمذكورين فى الاعلى ؟
==========
فى توزيعات اليونكس مثل ال *BSD تتعرض الادوات التى يطلق عليها r- commands مثل (rlogin,rsh and rcp) الى انواع مختلفه من الهجمات حيث انه لو شخص استطاع ان يكتسب ال روت اكسيس (root access) للاجهزه التى على الشبكه بطريقه ما او فعلها ن طريق اتصال فيزيائى اى ريموتلى يمكنه ان يدخل الى كل بيانات الاجهزه التى على الشبكه بدون ادنى صعوبه لانه يستطيع بالروت اكسس ان يعبر من خلال اى اداه من المذكوره فى يونكس بدون اى صعوبه و يمكنه تفاديها بطرق معينه و هذا ما يسمى بأن الشخص لديه unauthorized access to systems اعتقد انكم فهمتونى الان ;) و يمكن ايضا لاى شخص ان يراقب و النت ورك ترافيك و يلتقط كل

الباكيدجس من خلال شبكتك و تكون هذه الباكيدجس تحتوى على الباسوردس للسيستم حق شبكتك

ملحوظه::(طريقه مراقبه النت ورك ترافيك هى طريقه حقيقيه فى الاختراق و تستخدم فى اختراق المنظمات الكبرى و تقع تحت بند تقفى الاثر و الاعداد للاختراق)

و الان نعود الى السيكيور شيل و مزايا السيكيور شيل تظهر هنا مع كل عيوب الادوات فى يونكس فالسيكيور شيل يطالب الشخص الذى لديه الروت اكسس ايضا بأن يتصل اتصال موثوق عبره اى لا يعطيه الحق للدخول الى بيانات اجهزه الشبكه الا بالباسورد و لا يمكن التحايل على الsshفى هذه النقطه و بذلك حتى لو تمكن الشخص من اكتساب الروت اكسس لن يستطسع الاطلاع على بيانات الشبكه :) الا ب authorized access to systems .

و النقطه الثانيه هى ان اذا حاول احد اختراقك عن طريق مراقبه النت وررك ترافيك لشبكتك و التقاط الباكيدجس التى تحمل معلوماتك و باسورداتك فسيخيب امله لان السيكيور شيل لا يرسل الباسوردات فى صوره واضحه كما ترسلها ادوات يونكس الاخرى و لكن يرسلها مشفره و لذلك سيكون على المخترق محاوله فك الشفره و الخ :):)

و لكن مع كل هذه المزايا لم يخلى ال secure shell من الثغرات و لكن تعتبر ثغراته قليلا و تقريبا معظمها يحتاج الى الرووت اكسس و الاخرى يمكن ان تخترق السيكيور شل فقط بها (هذا كلام بينى و بينكم ;) :))

و الان سؤال اخر ::

ما هى انواع الهجوم التى تحمى منها ال ssh ؟
==========

1- تحمى من ال ip spoofing اى تحمى من انتحال عنواين الاى بى حيث انه لو ارسل شخص ما باكيدجس من اى بى يظهر انه موثوق به و لكنه فى الحقيقه ليس موثوق به يكشفه ال ssh و تحمى ايضا ال ssh من المنتحلين على الشبكه المحليه اى localy .

2- تحمى مما يسمى ال DNS spoofing

3- تعترض ظهور التيكستس التى يكون مخزن عليها الباسوردات الواضحه و بيانات الهوستس

4- تحميك من معالجه البيانات المخزنه اى تمنع اى شخص غير موثوق به من عمل ايديت لاى داتا مخزنه

و لكن مع كل هذا فأن ال ssh ليس امن بدرجه كبيره حيث ان الاشخاص ذو خبره كبيره فى النت ورك يستطيعون ان يجعلون ال ssh ينقطع عن الاتصال اى disconnected و لكن لا يمكن ان يكسرو تشفير بياناته او يعيدون تشخيل الترافيك الذى كان ينقلها .

و ايضا كل الاشياء التى تكلمنا عنها فوق سوف تعمل فقط اذا كنت تستخدم خاصيه التشفير التى تسمح لك بها ال ssh و هى تسمح بأكثر من نوع تشفير مثل (three-key triple-DES, DES, RC4-128, TSS, Blowfish) يمكنك استخدام ما تريد منهم و ايضا هناك اوبشن اى خيار فى الاداه تسمح لك بعدم تشغيل التشفير اى" encryption of type "none" و بهذا تجعلنى اقول عليك احمق ! لان هذا يجعل ال ssh سهله الاختراق مثل الادوات التى تم ذكرها فى اول الموضوع فى يونكس , حيث ان هذا التشفير ايضا يمنع ال ip spoofing و ال DNS spoofing و هذا ايضا بالاضافه الى تغيير مفاتيح فك التشفير كل فتره معينه و يتم تدمير مفاتيح التدمير التى تم استعمالها تماما .

اذن فهى اداه حقا مميزه و تستحق الاحترام و الاهتمام مع انها لا تخلو من الثغرات و لكن لنجعلها افضل ما موجود فى هذا المجال :)

ارجو ان اكون قد افدتكم فى هذا الدرس بالتعرف على اداه مثل السيكيور شيل و ارجو ان اكون عند حسن ظنكم

و اعذرونى على الانقطاع لانى اواجه مشاكل بسيطه ان شاء الله تنتهى على خير و اعود :)

و سلامى ل Egyption-hunter و SaD jackAle و zayon و topzero و كل الاعضاء هنا :)

AciD-WarZ = pc

(; idiote hehe

A Member Of :: D-StoRM-TeaM & $A-TeaM

==========

==========

ACIDBURN_EG@HOTMAIL.COM

الماسنجر الجديد ::

Crying_FreeMan2@Hotmail.com

==========

==========

GreetZ::
$A-TeaM :: (AciD-WarZ , TweeTY , Jakal)
SADJackale , B-Hunter , BrokenArroW , KinG-Abdo , DJ-King ,
Egyption Fighter ,
USG-TeaM , ALL OF HACK 4 ARAB MEMBERS