شرح عملية SSH Tunneling في إختبار الإختراق

جميعنا بالطبع نعلم ما هو الـSSH فهو بروتوكول Secure Shell الذي نقوم باستخدامه في الاتصال بالسيرفر الخاص بنا لتنفيذ أي أوامر بشكل آمن فهذا البروتوكول مشفر وهذا ما يجعله مهمًا. ولكننا لسنا هنا الآن لنتحدث عن وظائفه العادية. بل سنتحدث عن كيفية استخدامه لتخطي الصعوبات التي تواجهنا أثناء عمليات اختبار الاختراق.

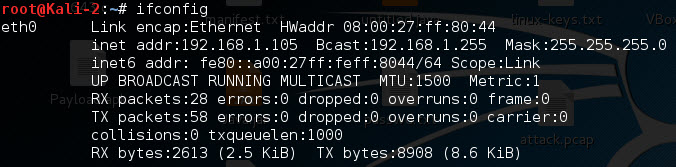
ما سأتحدث عنه في هذا المقال هو ما يسمى بالـSSH Tunneling وهو مشابه للـPort Forwarding أو ما يسمى بالـPort Redirection، وهي عملية يتم فيها القيام بتحويل الترافيك. هذه العملية لها وظائف كثيرة ومن أفضلها هي تخطي بعض القواعد التي تضعها الجدران النارية للتحكم في الترافيك.

السيناريو الذي سنتحدث عنه كالتالي:

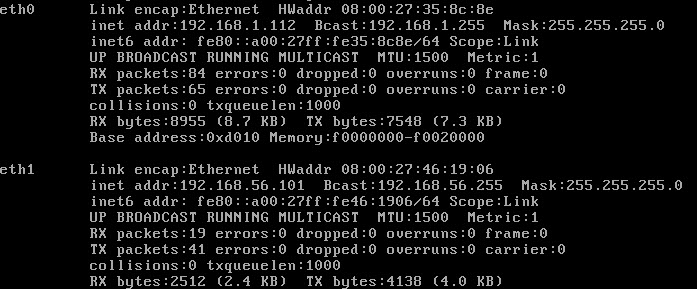
فلنفترض أننا قمنا باختراق نظام واكتشفنا بعدها أن هذا النظام مرتبط بشبكة أخرى لا أستطيع الوصول لها مباشرةً. في هذه الحالة سنجد أن مبدأ الـSSH Tunneling مناسب جدًا لتخطي هذا الأمر.

المعمل الذي سنعمل عليه سيكون مكون من ثلاثة أجهزة:

الجهاز الأول يعمل بنظام كالي لينكس، وسيكون هو الجهاز الذي سأستخدمه كمهاجم:

**[](http://www.isecur1ty.org/wp-content/uploads/2016/01/01-2.jpg)**

2. الجهاز الثاني سيكون الوسيط الذي سأعمل من خلاله والذي من المفترض أن أكون قد قمت باختراقه واكتشفت عليه شبكة داخلية:

**[](http://www.isecur1ty.org/wp-content/uploads/2016/01/02-2.jpg)**

3. الجهاز الذي أريد أن أصل إليه ويعمل من على شبكة منفصلة ولا أستطيع أن أصل له مباشرةً من خلال الجهاز المهاجم:

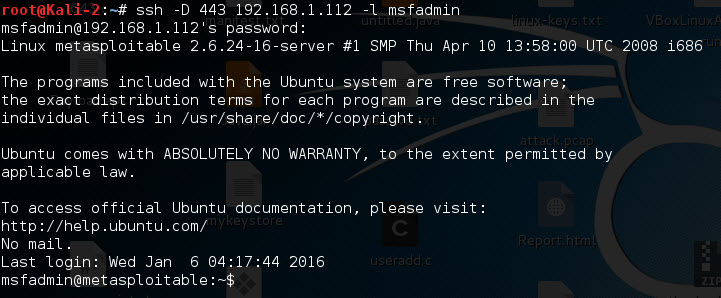
**[](http://www.isecur1ty.org/wp-content/uploads/2016/01/03-2.jpg)**

الآن السيناريو واضح، أمامنا ثلاثة أجهزة، ما سأقوم بشرحه في هذا المقال ثلاثة أشياء يمكننا أن نقوم بها من خلال الـSSH Tunneling:

الـDynamic Port Forwarding:

04

في الصورة السابقة نوضح كيفية استخدام الـDynamic Port Forwarding من خلال الـSSH، فكما نرى سنقوم بربط بورت على الكالي مع الوسيط الذي سيكون في هذه الحالة الهدف الذي قمت باختراق ووجدت أنه بداخله شبكة داخلية.

[](http://www.isecur1ty.org/wp-content/uploads/2016/01/05-2.jpg)

كما نرى في الصورة السابقة لقد قمت بربط البورت رقم 443 داخل الكالي بالوسيط الذي أملك صلاحيات عليه من خلال الـSSH، لاحظ أيضًا أنني استخدمت أمر إضافي وهو الـ(l) وذلك لأحدد اسم المستخدم الذي أريد أن أسجل دخولي من خلاله على الوسيط وهو في هذه الحالة msfadmin، فالافتراضي بالنسبة للـSSH أن يكون المستخدم هو root.

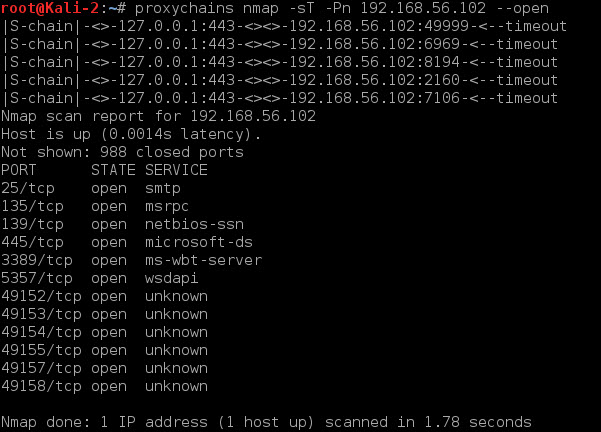
للتأكد من أن البورت 443 أصبح مشغولاً داخل الكالي سأقوم باستخدام الأمر التالي:

06الخطوة الأخيرة لتمريك الترافيك هي أن أقوم بتفعيل إعدادات الـProxyChains وذلك لأستطيع من خلالها تمرير الترافيك للهدف الخاص بي وهو الذي يعمل على شبكة منفصلة لا أستطيع الوصول لها من خلال الكالي، سأقوم الآن بالدخول على إعدادات الـProxyChains على الكالي والتعديل فيها كما هو موضح في الصورة التالية:



كما هو موضح في الصورة السابقة ملف إعدادات الـProxyChains موجود في المسار المذكور بالأعلى، كل ما عليّ فعله هو أن أقوم بتوضيح أنني سأستخدم socks4 ووضع اللوكال هوست بالإضافة إلى البورت الذي قمت من بتمرير الترافيك من خلاله.

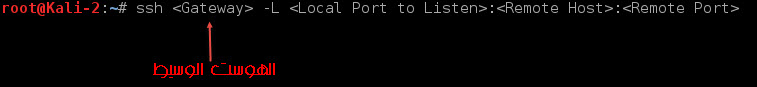
الآن بكل بساطة أستطيع تمرير الترافيك كما أريد، دعنا نرى مثالاً، سأقوم الآن باستخدام أداة Nmap لعمل فحص على الهدف والذي يعمل على نطاق مختلف تمامًا عن نطاق الكالي:



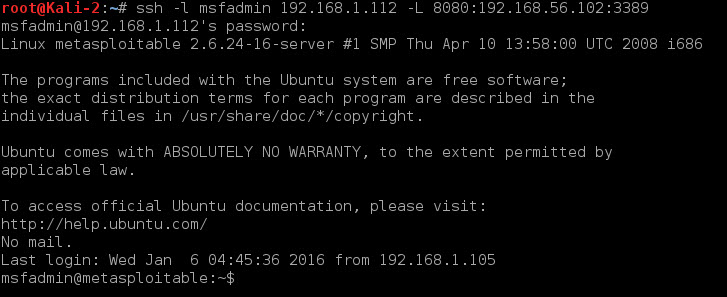
كما نرى في الصورة السابقة، فقد نجحنا في عمل فحص من خلال الـProxyChains والذي يستخدم الـTunnel الذي قمنا بإنشاءه لتنفيذ الأوامر. لاحظ أننا وجدنا أن البورت 3389 مفتوح وهذا يعني أن خدمة الـRDP أو الـRemote Desktop مفعلة. السؤال هنا، ماذا لو أردت أن أتصل بها، ولكن المشكلة أنني لا أستطيع الوصول لها مباشرة 🙁 هنا يأتي الحل من إحدى الطريقتين أما أن أقوم بعمل Local Port Forwarding أو Remote Port Forwarding.

Local Port Forwarding:

الأمر الخاص بالـLocal Port Forwarding من خلال الـSSH يكون بالشكل التالي:

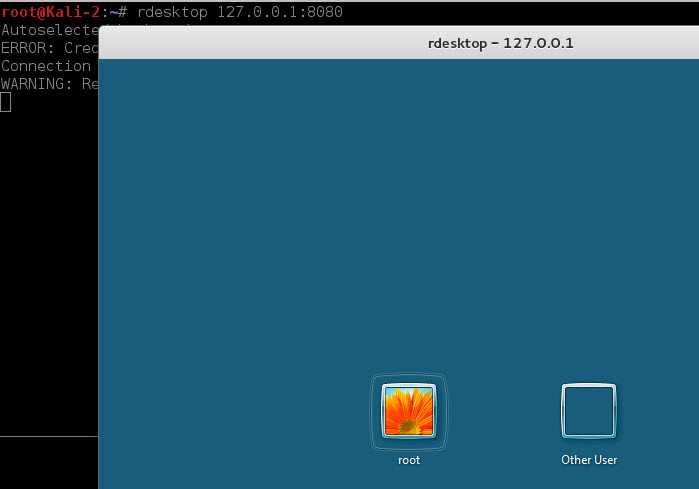


ما سأقوم به من خلال الـLocal Port Forwarding هو أنني سأقوم بربط بورت على الكالي مع البورت الهدف الذي أريد الوصول له وذلك من خلال الوسيط الذي يستطيع الوصول للشبكتين:



ما حدث في الصورة السابقة أنني قمت بربط البورت رقم 8080 على الكالي بالبورت 3389 الخاص بالويندوز وهو الهدف الذي يعمل على شبكة أخرى وذلك من خلال الوسيط الذي قمت بتسجيل الدخول إليه من خلال الـSSH.

كل ما عليّ فعله الآن هو أنني سأتصل بالبورت 8080 على شبكتي المحلية من خلال rdesktop وسنجد أننا وصلنا للويندوز وكأننا وصلنا له مباشرة:

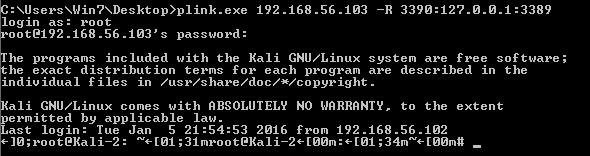


الصورة السابقة تعبر عن كل شيء ولا تحتاج إلى شرح، فكما نرى نجحنا في الاتصال بخدمة RDP بنجاح، يمكننا الآن إدخال اسم المستخدم والباسورد إن كنت تملكهم.

Remote Port Forwarding:

لتوضيح الـRemote Port Forwarding سنحتاج مثال مختلف قليلاً، فسأفترض أنني قمت باختراق هدف من نوع ويندوز يعمل خلف NAT وحصلت على CMD Shell ولكني لا أستطيع الوصول له مباشرة من خلال الكالي بسبب الـNAT، ووجدت أن الويندوز مفعل الـRDP وبالرغم من ذلك لا أستطيع الوصول له مباشرة لنفس السبب وهو الـNAT، في هذه الحالة سأقوم بتخطي هذه المشكلة من خلال ما يسمى بالـReverse Remote Tunneling أو الـReverse Remote Port Forwarding، فسأجعل الويندوز يقوم بربط البورت الداخلي الذي يعمل عليه الـRDP وهو البورت الـ3389 ببورت خارجي خاص بالكالي، في هذا المثال لن أحتاج إلى وسيط، دعنا نرى كيف يمكننا فعل ذلك:

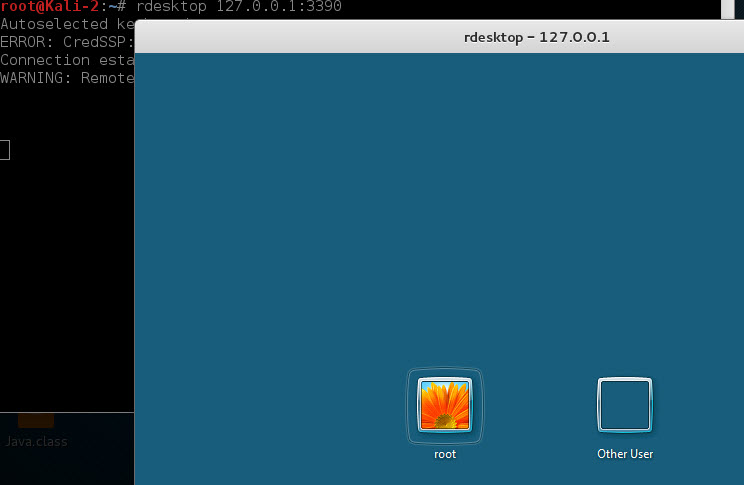
أولاً: سأحتاج SSH Client على الويندوز وسأقوم باستخدام Plink في هذه الحالة وهو SSH Client يعمل بكفاءة عالية ولا يحتاج إلى تثبيت:



ما قمت بفعله في الصورة السابقة هو أنني جعلت الويندوز يقوم بالاتصال بالكالي (على افتراض أن الكالي له Public IP)، وقمت بجعله يربط البورت الخارجي 3390 الخاص بالكالي بالبورت الداخلي للويندوز 3389، وللتأكد يمكنك الذهاب للكالي والتأكد من أن البورت 3390 أصبح مشغولاً الآن:

14

الآن كل ما علينا فعله هو محاولة الاتصال بالبورت 3390 الخاص بالكالي وسنستطيع أن نصل للـRDP الخاصة بالويندوز كما هو موضح في الصورة التالية:



كما نرى في الصورة السابقة فقد نجحنا في الوصول للـRDP بشكل عكسي كما أردنا.

الختام:

الـSSH Tunneling مفيدة جدًا في هذه الأمور ولها الكثير من الخبايا، ولكنها تحتاج تدريب منك وفهم للأمور. حاول أن تجرب بنفسك وتضع لنفسك بعض العقبات وحاول أن تقوم بتخطيها.