ماهو DHCP :

هو اختصار لكلمة Dynamic Host Configuration Protocol

فهو السيرفر المسؤول عن ادارة ارقام وعناوين الأيبيات الموجودة على الشبكة بشكل دوري وتلقائي

ماهية اهمية DHCP :

كما ذكرنا انه يقوم بادارة ارقام الايبيات تخيل عزيزي القارئ انك تقوم بأستخدام خدمة ما وهذه الخدمة تقوم بتزويدك بأيبي معين وهنالك اكثر من 1000 مشترك معاك في هذه الخدمة فان منح ايبي لكل فرد مشترك في هذه الخدمة سيحتاج لوقت كبير وجهد اكبر في توفير ايبي ادريس لكل مشترك يقوم سيرفر DHCP تلقائي بتزويد كل مشترك بايبي ادريس خاص فيه اوتوماتيكيا

تعريف بهجمات DHCP Spoofing

هذا النوع من الهجمات هام جدا من الناحية الأمنية او من ناحية القيام بالهجوم ويعتبر هجوم بسيط كفكرة وضخم من باب تحقيق الأهداف المطلوبة لأي هجوم

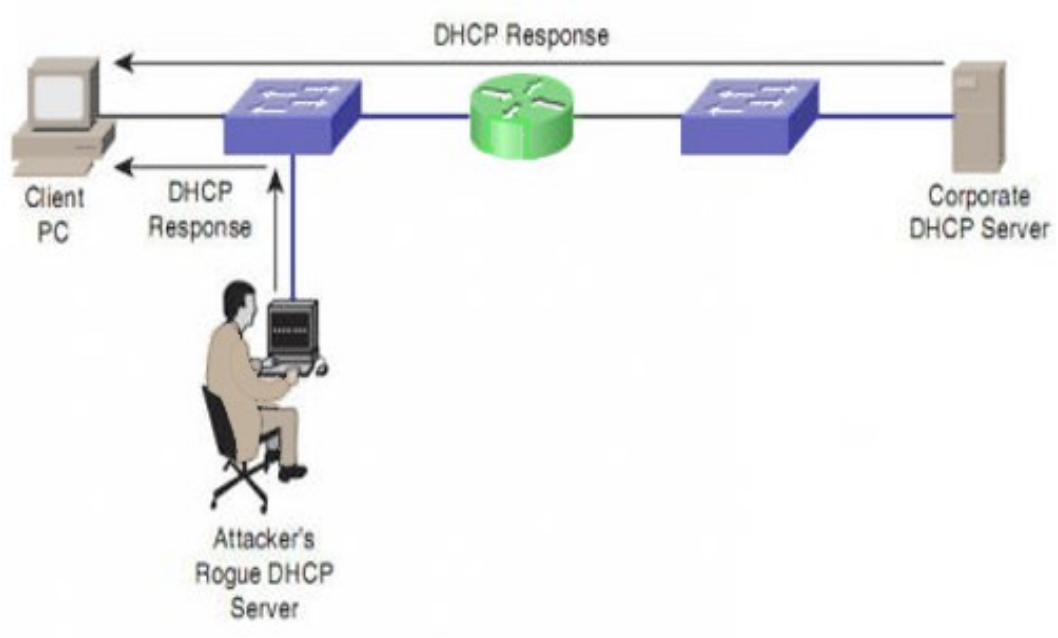
فكرة الهجوم

يقوم المهاجم بأنشاء جهاز شخصي يملك نفس المواصفات الموجودة في الجهاز الرئيسي الذي يعمل عليه سيرفر DHCP وبعد ذلك يقوم بتشغيل السيرفر مع القيام بتعديل طفيف على Gate way فيقوم بجعله جهازه نفسه الذي قام بتجهيزه ليبدا الهجوم
وبهذا الشكل يقوم بتحميل الترافيك الذي يمر من جهازه الى Gate way الحقيقي
وعلى هذا النحو ان اي معلومات او بيانات يتم ارسالها ضمن هذه الشبكة سيتم تمريرها على الجهاز
يمكنك تحميل الترافيك بعدة برامج ولكن افضلها واشهرها هو ettercap
وبهذا الشكل ان جميع البيانات والداتا التي ستمر على الشبكة سيكون لها مرور على جهازه وبعد ذلك تأتي مرحلة اخرى ئلا وهية تحليل البيانات او فك بروتوكولات الداتا
ويمكنك تحليلها عن طريق الكثير من البرامج ولكن افضلها WireSharK
هذا الهجوم هو هجوم مشابه لما يسمعى هجمات الرجل الوسيط Man in TheMiddeL

ملاحظة :

هذا النوع من الهجوم ينتهي بنوع اخر يسمعى MITM عندما نصل لمرحلة تحليل البيانات

صورة توضيحية للهجوم



تعريف بهجمات DHCP Starvation

بعد ان انتهينا من النوع الأول من الهجمات التي تستهدف DHCP SERVERسأتكلم عن النوع الثاني

يعتبر هذا النوع من احد انواع هجمات حجب الخدمة Danial Of Service او هجمات Dos

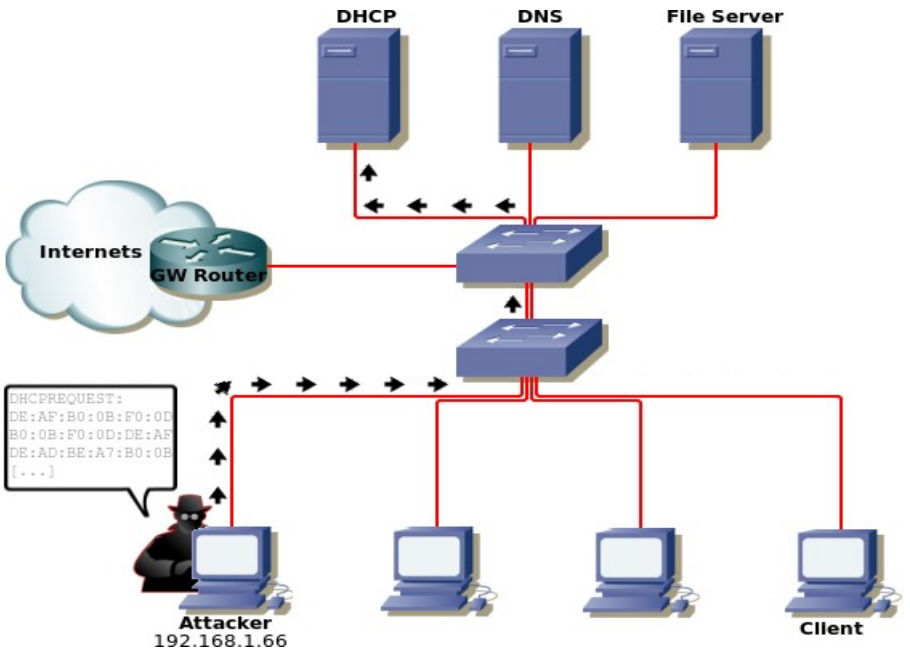
فكرة الهجوم

يقوم المهاجم بارسال رسائل على سيرفر DHCP بغزارة وبعدد غير محدود ويكون محتوى هذه الرسالة طلب بتمنحه ايبي خاص للجهاز الذي يعمل عليه طبعا مع تغير الادريس مع كل مرة يقوم بها في عملية الطلب

وبهذه الحالة يكون المهاجم قام بحجز جميع الايبيات الموجودة على السيرفر فعند قيام اي شخص بانشاء طلب حقيقي لن يحصل على اي نتيجة والسبب واضح تم استنفاذ جميع الايبيات الممكنة وهذا ما نسميه بحجب الخدمة او هجمات الاغراق

طبعا هذا الهجوم يفضل ان يكون سابق للهجوم الأول بالمهاجم يقوم بعملية حجز للايبيات وحجب خدمة للمزود وبعد ذلك يقوم بعملية التقاط الترافيك وتحليله

صورة توضيحية للهجوم



Help Link

http://hakipedia.com/index.php/DHCP_Starvation
http://www.ibh.de/netglossary/net_09.htm

rOckHuntEr
r0ck.hunt3r@gmail.com

Gr33tz : All A4s – All Ubuntu User – Medo – Hacker – rOckMastEr