هجمات حجب الخدمة
Denial of Service Attacks

إعداد: فيصل الحربي

مقدمة

التوفير أو تيسير الوصول إلى الخدمات (Availability) تُعرف بشكل إجمالي بأن البيانات والخدمات يجب أن يتم الوصول إليها من قبل المستخدمين المصرح لهم بذلك (أو المستخدمين الشرعيين legitimate users) وذلك خلال وقت معقول من فترة طلبهم لها. هذه الخاصية يجب أن تكون متوفرة في الشبكات والأنظمة التي يفترض بها أن تكون آمنة. لكن انتشرت في الآونة الأخيرة هجمات تستهدف تعطيل هذه الخاصية بالذات. يطلق على هذا النوع من الهجمات "هجمات حجب الخدمة" Denial of Service Attacks.

خطورة هجوم حجب الخدمة

تكمن خطورة هجمات حجب الخدمة في أنها من الصعب العمل على منعها تماماً. وهي أيضاً في تزايد مستمر بسبب سهولة تنفيذها ، وكونها لا تتطلب معرفة تقنية كبيرة من الشخص الذي يرغب بالقيام بهذا النوع من الهجوم بسبب توفر أدوات جاهزة كثيرة وسهلة الاستخدام. يطلق على الأشخاص الذين يستخدمون الأدوات الجاهزة في مهاجمة الآخرين script kiddies. وهم يشكلون خطورة كبيرة إذا ما توفرت لهم أدوات هجوم فعالة.

أنوع الهجوم

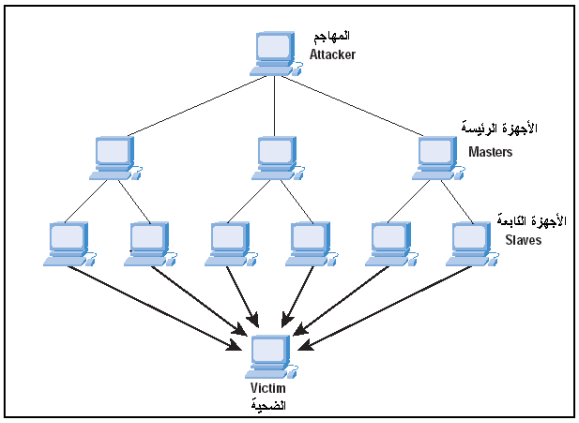
تصنف هجمات حجب الخدمة إلى:

- **حجب الخدمة التقليدي Typical Denial of Service**

حجب الخدمة التقليدي يحدث عندما يقوم المهاجم بإرسال كميات كبيرة من حزم البيانات إلى الجهاز المستهدف بغرض تعطيله عن الاستجابة ، وبالتالي منع المستخدمين العاديين من الوصول إليه والاستفادة من خدماته. إذا كان الهجوم يتم مباشرة من جهاز المهاجم فإنه لا ينجح عادة ، لأن الجهاز المستهدف غالباً يكون قادر على استيعاب هجوم قادم من طرف واحد.

- **حجب الخدمة الموزع Distributed Denial of Service**

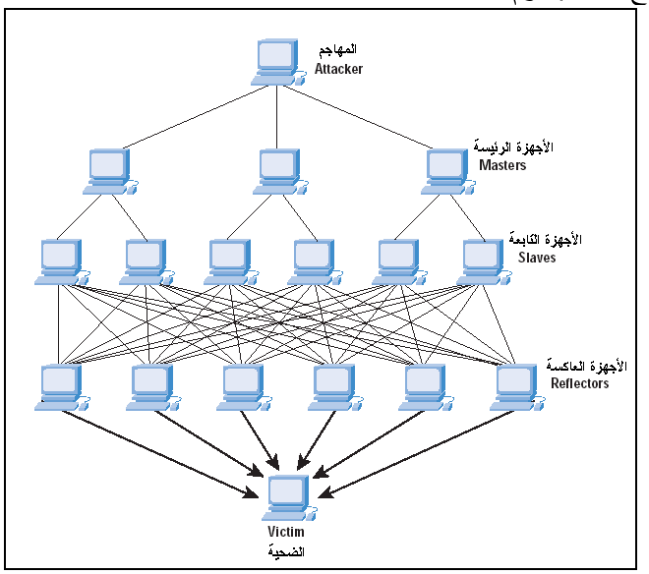
هجمات حجب الخدمة الموزعة هي الأكثر انتشاراً والأنجح في تحقيق أهدافها. فالمهاجم لا يقوم بتنفيذ الهجوم من جهازه مباشرة ، بل يعمد إلى استخدام أجهزة أخرى بأعداد كبيرة كمنطلق للهجوم. هذه الأجهزة الوسيطة تسمى zombies ، وهي تقع تحت تصرف المهاجم. وهي بالبداية تكون مصابة بثغرات أمنية ، ثم قام المهاجم باستغلال هذه الثغرات لزرع وتركيب أدوات خاصة بالهجوم عليها. ومن ثم يقوم بإصدار أمر إلى هذه الأجهزة لتنفيذ الهجوم في وقت محدد ضد هدف موحد. عادة تكون هذه الأجهزة مقسمة إلى صنفين: رئيسة master ، وتابعة slave. فالمهاجم يقوم بالاتصال بالأجهزة الرئيسة وإصدار الأوامر إليها ، والتي بدورها تتحكم في مجموعة من الأجهزة التابعة وتمرر أمر الهجوم لها. والأخيرة هي التي تنطلق منها عمليات الهجوم الفعلية. وهذا في الغالب يؤدي إلى عجز الجهاز المستهدف عن الاستجابة لهذا الكم الهائل من الهجمات ، وبالتاي عجزه عن الاستجابة لطلبات المستخدمين الشرعيين في الوصول إلى الموارد التي يقدمها. الشكل التالي يوضح هذا النوع من الهجوم:



1: هجوم حجب الخدمة الموزع

- **حجب الخدمة الموزع الانعكاسي Distributed Reflection Denial of Service**

وهي نوع غير منتشر على نطاق كبير من أنواع حجب الخدمة الموزع. ويختلف عنه في أن الأجهزة الوسيطة zombies تقوم بإرسال حزم بيانات مزورة spoofed packets (غالباً يتم استخدام حزم ICMP) إلى أهداف وسيطة ، وليست الهدف الأساسي للهجوم. وهي تسمى غالباً أهداف عاكسة reflected victims. الحزم المرسلة تم تزوير العنوان المصدر source address الخاص بها بالتحديد. ووضع بدلاً منه عنوان الهدف الرئيسي للهجوم. فما يحدث هنا هو أن الأهداف الوسيطة أو العاكسة تستقبل حزم البيانات المزورة وتقوم بإرسال الرد عليها إلى عنوان الهدف الرئيسي ، والذي قد لا يتمكن من استيعاب جميع الطلبات ويقع تحت تأثير حجب الخدمة. الشكل التالي يوضح هذا الهجوم:



2 : هجوم حجب الخدمة الموزع الانعكاسي

الأهداف المفضلة للأجهزة الوسيطة zombies

- الأجهزة الغير محدثة ، والتي توجد بها ثغرات أمنية.
- الأجهزة التي تكون دائمة الاتصال بانترنت، أو يكون متصلة بأوقات كبيرة.
- أن يكون اتصالها بانترنت سريعاً ، (مثل ADSL ، أو Cable ، ...).

الأهداف المفضلة للهجوم

يحاول المهاجمون استهداف أنواع مختلفة من المواقع، منها:

- بوابات الانترنت، وهي مواقع كبيرة تحوي خدمات متكاملة وتخدم قطاع كبير من المستخدمين.

- مواقع التجارة الالكترونية.
- المواقع الإخبارية.
- المواقع السياسية.

وكما نلاحظ أنه في الغالب يتم استهداف المواقع التي يكون إيقاف خدماتها ، ولو لوقت قصير ، له صدى كبير.

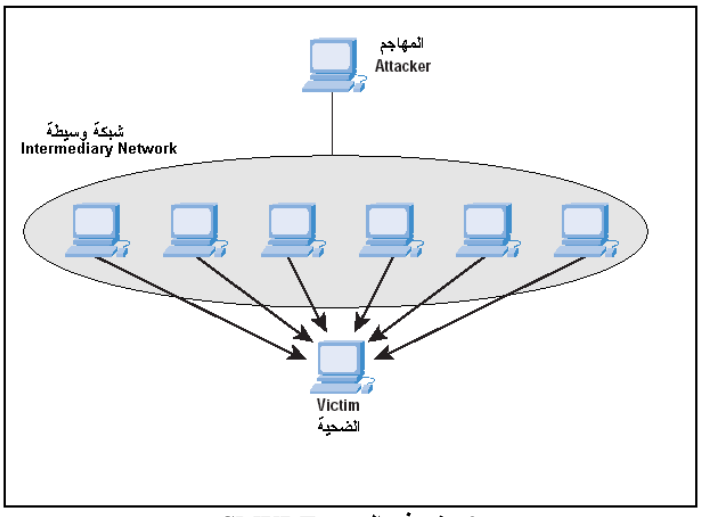
الطرق المستخدمة في الهجوم

يتبع المهاجمون عدة طرق لمهاجمة المواقع المستهدفة ، ومن أشهر هذه الطرق:

- **ICMP**. قد يكون استخدام حزم ICMP في الهجوم هو الأكثر انتشاراً. ترمز ICMP إلى Internet Control Message Protocol. وهو بروتوكول يستخدم لإرسال رسائل خاصة بالتحكم أو الأخطاء ويقع ضمن بروتوكول TCP/IP. ومن أمثلته Ping حيث يستخدم لمعرفة ما إذا كان الجهاز الآخر متصلاً أم لا. أغلب الأجهزة تقوم بالاستجابة لحزم ICMP وترد عليها بحزم مماثلة. وهذا ما يجعل من السهل تعطيل الجهاز المستهدف بإرسال سيل كبير من هذه الحزم. ولأن الجهاز المستهدف يحاول الرد على كل حزمة ، فإنه بالنهاية لن يستطيع الاستجابة لها جميعاً.
- **UDP**. ويحدث عندما يرسل المهاجم كمية كبيرة من حزم UDP إلى الجهاز المستهدف. UDP يرمز إلى User Datagram Protocol ، وهو بروتوكول غير معتمد على الاتصال connectionless protocol يقع ضمن بروتوكول TCP/IP. هذا يعني أنه لا يلزم إنشاء قناة اتصال بين المستقبل والمرسل لنقل حزم البيانات. وهذا ما يزيد من فعالية هذا الهجوم.
- **TCP**. بروتوكول TCP (Transmission Control Protocol) هو المقابل لبروتوكول UDP ضمن TCP/IP. فهو مبني على الاتصال connection-oriented ، أي أنه يلزم إنشاء قناة اتصال بين المستقبل والمرسل لتراسل حزم البيانات بينهما. وهذا يضمن أن تصل الحزم إلى المستقبل بشكل سليم وبالترتيب الصحيح ، بعكس بروتوكول UDP. من الممكن استخدام بروتوكول TCP في هجوم حجب الخدمة في حالات عدة. فمثلاً قد يحاول المهاجم إنشاء عدد كبير من قنوات الاتصال إلى الجهاز المستهدف إلى درجة لا يستطيع معها ذلك الجهاز الاستجابة. أو قد يقوم بإنشاء قناة اتصال مع الجهاز المستهدف ، ومن ثم يتم إرسال كمية كبيرة من البيانات عبر هذه القناة قد تؤدي إلى تعطل المستهدف عن الاستجابة.
- **TCP SYN**. في بروتوكول TCP ، عندما يرغب جهاز في إنشاء قناة اتصال مع جهاز آخر فإنه يقوم أولاً بعملية تسمى "المصافحة الثلاثية" 3-way handshaking . حيث يقوم الجهاز الأول بإرسال حزمة إلى الجهاز الثاني تسمى SYN packet. والذي بدوره يرد عليها بحزمة SYN-ACK. وأخيراً يرسل الجهاز الأول حزمة ACK ، ليبدأ الاتصال بعدها. بعد إرسال حزمة SYN-ACK وقبل استقبال حزمة ACK ، يجب أن يقوم الجهاز الثاني بحفظ سجل لطلبات الاتصال غير المكتملة. وعندما يستقبل حزمة ACK ويتم إنشاء الاتصال فإنه يقوم بمسح هذا السجل. ولأنه عادة لا يكون هنالك وقت كبير بين إرسال SYN-ACK واستقبال ACK ، فإن هذا السجل يتم مسحه بشكل سريع وبالتالي لا يشغل مساحة كبيرة. ما يحدث هنا هو أن المهاجم يقوم بإرسال كمية كبيرة من حزم SYN إلى الجهاز المستهدف ولا يقوم بالرد بحزمة ACK (أحياناً يقوم بتزوير العنوان المصدر لحزمة SYN إلى عنوان غير موجود). هذا يجعل الجهاز الثاني ، وهو المستهدف في الهجوم ، ينتظر إنشاء اتصال ويحتفظ بسجل لكل الحزم المرسلة. إذا كانت حزم SYN المرسلة أكثر من أن يتحملها الجهاز المستهدف ، أو أنه غير قادر على الاحتفاظ بسجل لها كلها ، فإن هذا يتسبب في تعطله وحجب الوصول إليه من قبل جميع المستخدمين.
- **Fragmentation**. في الاتصال العادي يتم تجزيء الرسالة التي تحوي بيانات كبيرة (والتي لا يمكن أن تنقل على حزمة واحدة خلال الشبكة) إلى أجزاء صغيرة تسمى fragments ، ويعطى كل fragment رقم تسلسلي sequence number. ويتم إرسال كل جزء fragment على حدة. وعند استقبال الطرف الآخر لهذه الأجزاء فإنه يقوم بإعادة تجميعها ، باستخدام الرقم التسلسلي. ليتم في النهاية إعادة تكوين البيانات كما أرسلت من الطرف الأول. لكن في هذا النوع من الهجوم يتم إرسال أجزاء fragments لها رقم تسلسلي خاطئ ، ليبدو عند المستقبل أن هنالك أجزاء كثيرة مفقودة. الطرف المستقبل يخصص مساحة لتخزين الأجزاء التي استلمها بانتظار اكتمال جميع

الأجزاء الخاصة بالرسالة. ولكن تزايد قدوم أجزاء ذات أرقام تسلسلية خاطئة ، يثقل على الطـــرف المستقبل ويجعله في النهاية غير قادر على استقبال المزيد.

- **SMURF**. في هذا النوع من الهجوم يقوم المهاجم بإرسال حزمة ICMP خاصة تسمى ICMP echo request إلى عنوان بث broadcast لشبكة وسيطة Intermediary Network (ليست هي المستهدفة في الهجوم). تطلب هذه الحزمة الرد عليها بحزمة أخرى ، ولكنها تحوي عنوان مصـــدر source address مزور. فقد تم وضع العنوان الخاص بالجهاز المستهدف كعنوان مصـــدر لهـــذه الحزمة. عندما تصل هذه الحزمة إلى عنوان البث broadcast للشبكة ، فإنها تُحول وترسل إلى كل جهاز في الشبكة الوسيطة. فيقوم كل جهاز هنا باستقبال هذه الحزمة والرد عليها بحزمـــة أخـــرى. ولكن الرد يذهب إلى العنوان المزور ، وهو خاص بالجهاز المستهدف. فينتج عن ذلك إرسال عـــدد من حزم ICMP إلى الجهاز المستهدف مساوٍ لعدد الأجهزة في الشبكة الوسيطة. فإذا كان عدد هذه الأجهزة كبيراً ، أو أنه تم الإرسال إلى عدد كبير من الشبكات الوسيطة فإن هذا قد يتسبب في تعطل الجهاز المستهدف عن الاستجابة للكم الكبير من حزم ICMP. هذا النموذج موضح بالشكل التالي:



3 : نموذج الهجوم SMURF

- **قنابل البريد Mail Bombing**. الهدف من هذا الهجوم هو إغراق صناديق البريد الالكتروني بكم هائل من الرسائل. وذلك يتسبب في ملء صندوق البريد الخاص بالمستخدم وعجزه عـــن اســـتقبال رسائل جديدة. أو على الأقل فهو يضيع وقت المستخدم في حذف هذه الرسائل ويتسبب في تـــأخيره في الوصول إلى الرسائل الفعلية. وهو أقل الأنواع خطورة.

استخدام IRC في حجب الخدمة

IRC هو اختصار لـــ Internet Relay Chat ، وهو أشهر وأقدم البروتوكولات الخاصـــة بالمحادثـــة chatting على الانترنت. وتستخدم كثير من النماذج المتبعة في تنفيذ هجوم حجب الخدمة هذا البروتوكـــول. ما يحدث هنا هو أن الأجهزة الوسيطة (أو ما تعرف بالـــ zombies) تقوم ، حال توفر اتصـــال بانترنـــت ، بالدخول إلى خادم IRC والانضمام إلى "غرفة" أو "قناة" محادثة channel خاصة. وتستجيب للأوامر التـــي يصدرها المهاجم عبر هذه القناة. هذا يوفر على المهاجم جهد إضافي للتعامل الأجهزة الوســـيطة ، حيـــث لا يحتاج إلى البحث عنها وإنشاء اتصال عبر منفذ خاص لإرسال الأوامر. بل سيجد جميع هذه الأجهزة موجودة في مكان واحد ومستعدة لتلقي الأوامر. ولأنه يتم استخدام منافذ IRC المعروفة لتلقي الأوامر ، فإن هذا يزيد من صعوبة اكتشاف أدوات الهجوم على الأجهزة الوسيطة. عادةً تسمى هذه الأجهزة في هذه الحالـــة bots ، أو zombie bots.

أدوات الهجوم Attacking tools

كما ذكرنا سابقاً فإن المهاجم يقوم بزرع أدوات في الأجهزة المعدة للهجـــوم (الـــ zombies) ليقـــوم باستخدامها في تنفيذ هجوم حجب الخدمة. وكما قلنا فإن هنالك العديد من الأدوات ، فـــلا حاجـــة لأن يقـــوم المهاجم بتطوير أدوات خاصة به. أول هذه الأدوات ظهـــوراً كـــان Trin00 و Tribe Flood Network

(TFN). ثم توالى بعد ظهور أدوات أخرى مثل TFN2K و Stacheldraht و Eggdrop وغيرها من الأدوات التي تتنوع في المواصفات وإمكانيات الهجوم.

اكتشاف ومنع أدوات الهجوم

إذا لم يكن لديك موقع ولا تخشى من أن تتعرض لهجوم حجب خدمة ، فلا تكن ممن يستخدمهم المهاجمون لتنفيذ الهجوم على موقع آخر! فيجب أن تتأكد من أن جهازك غير مصاب بثغرة أمنية ولا توجد به أي من أدوات الهجوم المستخدمة لحجب الخدمة. الخطوات المهمة دائماً: استخدم برامج مكافحة الفيروسات وجدران النار ، قم بتثبيت الرقع الأمنية أولاً بأول واجعل جميع برامجك محدثة باستمرار. إن الكثير من هذه الأدوات تستخدم طرق متقدمة للتخفي ، فلا يشعر المستخدم بوجودها. وأيضاً تستخدم التشفير في تراسل البيانات بينها. أمر آخر يجعل ملاحقة مصدر الهجوم أكثر صعوبة ، هو أنها ترسل حزم البيانات بعنوان مصدر مزيف. لذلك يُنصح مدراء الشبكات بعمل إعدادات خاصة للموجهات routers بحيث لا تقوم بالسماح بمرور حزم البيانات التي عنوان المصدر الخاص بها ليس ضمن الشبكة. هذه الإعدادات لن توقف جميع الهجمات الصادرة من الشبكة ، ولكنها ستساعد في تخفيفها وتجعل تعقبها أمراً ممكناً. أيضاً هنالك أدوات مساعدة خاصة تساهم في اكتشاف ما إذا كانت أجهزة في الشبكة تستخدم في تنفيذ هجوم حجب خدمة. من هذه الأدوات find_ddos31 من National Information Protection Center ، و ddos_scan ، و rid ، وغيرها من الأدوات.

الدفاع ضد هجوم حجب الخدمة

منذ بداية ظهور هذه الهجمات حاول الكثيرون اتخاذ إجراءات للدفاع ضدها. لكن ، وبالرغم من بذل الكثير من الجهود في هذا المجال ، يظل خطر هذه الهجمات قائماً. ولقد حاول الخبراء تصنيف طرق الدفاع، فقد تم وضع طرق وقائية preventive ، وطرق تفاعلية reactive.

الطرق الوقائية: حيث يتم التقليل من احتمال التعرض لهجوم حجب خدمة. أو على الأقل جعل الضحايا المستهدفين يستمرون في تقديم الخدمات للمستخدمين الشرعيين بالرغم من تعرضهم للهجوم.

الطرق التفاعلية: حيث يتم محاولة اكتشاف الهجوم مبكراً والاستجابة له بالحال. وبالتالي يتم تقليل تأثير الهجوم على الضحية. لكن هنالك خطر من إمكانية تصنيف طلب مستخدم شرعي على أنه هجوم حجب خدمة.هذا يدعو إلى الحذر الشديد في تصنيف الحزم على أنها حزم هجوم.

يمكن اكتشاف الهجوم بعدة طرق منها:

- يمكن اكتشاف الهجمات التي لها طابع مميز أو نموذج معين (يسمى توقيع signature). حيث تتم مقارنة كل حزمة مع قاعدة بيانات تحوي نماذج لهجمات معروفة. فإذا تمت المطابقة يتم تصنيف الحزمة على أنها هجوم ، وبالتالي يتم منعها واتخاذ الإجراءات اللازمة. تتميز هذه الطريقة بأنها تتصدى بكفاءة للهجمات ذات الطابع المعروف. لكنها في المقابل لا تستطيع التعرف على الهجمات الجديدة. أيضاً يجب تحديث قاعدة البيانات الخاصة بنماذج الهجوم باستمرار.
- أحياناً يتم اللجوء إلى طريقة أخرى لاكتشاف الهجوم. هذه الطريقة تكون بمراقبة مرور البيانات ومقارنتها مع نموذج للمرور الطبيعي للبيانات في الأوضاع العادية. هذه الطريقة تسمى Anomaly. وإذا زاد حجم البيانات بشكل مميز عن النموذج الطبيعي يتم اعتبار الشبكة تحت هجوم حجب خدمة.
- يمكن دمج الطريقتين أعلاه واستخدامهما في وقت واحد.

نصائح للتعامل مع هجوم حجب الخدمة

بالإضافة إلى ما ذكر في ما يخص اكتشاف ومنع أدوات الهجوم ، فإنه ينصح بالقيام بالأمور التالية للتعامل مع هجوم حجب الخدمة:

- التدريب للطوارئ ، يجب أن يكون المسئولين عن الشبكة مؤهلين ومدربين جيداً.
- تقوية البنية التحتية للشبكة ، والأنظمة الموجودة بها.
- التأكد من وضع إعدادات مناسبة لأجهزة الشبكة ، وبالخصوص الموجهات routers.
- استخدام المرشحات filters. وهي أدوات قادرة على إلغاء حزم البيانات التي تكون مطابقة لنماذج أو شروط معرفة مسبقاً. يمكن وضع هذه المرشحات في عدة أجهزة مثل:
  - الموجهات routers: عادة يتم استخدام Access Control List ACL (قائمة ضبط الوصول) في الموجهات. وهي غير كافية لمواجهة هجوم حجب الخدمة. ذلك لأنها لا تقوم

بفحص ترويسة header كل حزمة قادمة. لكن في المقابل فإن تركيب المرشحات على الموجه يسبب تأثيراً كبيراً في الأداء. وقد لا يكون من مهام الموجه فحص ترويسة كل حزمة قادمة.

- جدران النار firewalls: وتركيب المرشحات هنا أفضل. لأن جدار النار يقوم بفحص كل حزمة تمر من خلاله.
- أجهزة مخصصة لمكافحة الهجوم: وهي بالطبع الأفضل. فهي تجمع طرق مختلفة للدفاع وأنماط متعددة للترشيح. وتكون مهمتها مخصصة للتصدي لهجوم حجب الخدمة فقط. ولأنها تقوم بفحص كل حزمة وعمل مقارنات متعددة ، فإنها يجب أن تكون قادرة على تحمل معدل كبير لمرور البيانات.

- إتباع سياسات أمنية قوية.
- بعد وقوع هجوم حجب خدمة ، لا بد من القيام بتحليله (معرفة نوع البروتوكول المستخدم، مصادر الهجوم، نوع حزم البيانات، الطرق المتبعة في الهجوم، ... الخ). ومن ثم الاستفادة من نتائج التحليل لزيادة الأمن وتحديث المرشحات وضبط الإعدادات.
- توزيع الحمل load balancing ، بين الأجهزة التي تقدم الخدمات.
- الحصول على سعة حزمة bandwidth أكبر، واستخدام أجهزة أكثر!

توجيه الهجوم إلى الـ Honeypots

الـ honeypots (وتعني "أوعية العسل") هي أجهزة يتم وضعها في بيئة أمنية محدودة لتقوم بجذب المهاجمين إليها. بالطبع هي لا تحتوي على بيانات أو خدمات حقيقة. والهدف منها هو جذب عمليات الهجوم إليها (كما ينجذب النحل إلى وعاء العسل) ، وبالتالي يمكن معرفة الهجوم في حالة وقوعه. وهذا يساعد في إبعاد المهاجمين عن الأهداف المهمة داخل الشبكة، وأيضاً يفيد في تحليل هذا الهجوم بعد وقوعه.

خاتمة

في فبراير عام 2000 م قام مراهق كندي بتنفيذ هجوم حجب خدمة موزع ضد مواقع مشهورة تسبب في إيقافها عن العمل عدة ساعات. من هذه المواقع yahoo.com ، Buy.com ، eBay.com ، CNN.com وغيرها. تسبب هذه الهجوم في خسائر قدرت بملايين الدولارات. وقد تم معرفة المهاجم وإلقاء القبض عليه بعد فترة ، والذي أدى إلى التعرف هو أنه قام بالتباهي بهذا العمل! هذا يوضح مدى خطورة وسهولة حدوث هذا الهجوم. وقد يكون أخطر في المستقبل مع استخدام الدودة worm ، والتي تقوم بالانتشار ذاتياً في الأجهزة ومن ثم تقوم بتنفيذ هجوم حجب خدمة ، كما حصل في دودة بلاستر وغيرها. ومتى ما كان عدد الأجهزة الوسيطة (zombies) كبير جداً ، فإنه يمكن القيام بالهجوم عبر إنشاء طلبات اتصال شرعية في وقت واحد ضد هدف الهجوم. هذا يدفع إلى المزيد من الاهتمام والبحث في طرق الوقاية والتعامل مع هجمات حجب الخدمة.

المراجع

[1] M. Ciampa, "*Security+ Guide To Network Security*", second edition, Course Technology, 2005

[2] J. Brendel, "Distributed Denial of Service: The current states and counter measures", http://questnet.scu.edu.au/uploads/28.pdf , 2002

[3] A. Mangarae, "Denial of Service FAQ Basic", http://www.securitydocs.com/library/2774, Dec. 2004

[4] Denial-of-Service Presentation Seoul, "Denial of Service", http://www.unescap.org/stat/meet/dataprot/backlund02.pdf , Aug. 2001

[5] HP web site, "Protecting Against Denial of Service Attacks", http://www.hp.com/rnd/support/manuals/pdf/release_06628_07110/Bk2_ApixB_DoS_Protection.pdf , May.2005

[6] C. Patrikakis, M., and O. Zouraraki, "Distributed Denial of Service Attacks", The Internet Protocol Journal volume 7 number 4, http://www.cisco.com/application/pdf/en/us/guest/about/about/c644/ccmigration_09186a00803b34d4.pdf , Dec.2004

[7] Computer Incident Advisory Capability, " Distributed Denial of Service Attacks", http://www.ciac.org/ciac/documents/CIAC-2319_Distributed_Denial_of_Service.pdf , Feb.2000

[8] C. Rahmani, M. Sharifi, T. Tafazzoli, " An Exprimental Analysis of Proactive Detection of Distributed Denial of Service Attacks ", http://www.security.iitk.ac.in/IITKHACK04/papers/cp08.pdf , May.2005

[9] Stephen M. Spech and Ruby B. Lee, "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures", http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf, May.2005
[10] Internet Security Systems, "Distributed Denial of Service Attack Tools", http://documents.iss.net/whitepapers/ddos.pdf, May.2005
[11] S. Romig, "Distributed Denial of Service Attacks", http://www.net.ohio-state.edu/security/talks/2000/2000-01-26_ddos_secwog/ddos.pdf, May.2005
[12] N. Weiler, "Honeypots for Distributed Denial of Service Attacks", http://www.tik.ee.ethz.ch/~weiler/papers/wetice02.pdf, May.2005
[13] T. Chen, "Denial of Service", http://engr.smu.edu/~tchen/papers/talk-bupt-ddos-Aug2004.pdf , May.2005
[14] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, D. Zamboni, "Analysis of a Denial of Service Attack on TCP" , http://www.cs.jhu.edu/~fabian/courses/CS600.424/course_papers/schuba.pdf , May.2005