أمن المعلومات

GS224-9

أمن الشبكات

هجمات الحرمان من الخدمة

1- هجمات الحرمان من الخدمة (Denial of Service) (DoS)

طبيعة هجمات الحرمان من الخدمة هي شكل من أشكال الهجوم على توفر بعض الخدمات التي يقدمها نظام المعلومات. ويمكن هذا الانتهاك عن طريق اغراق النظام أو الشبكة بالرسائل او البرامج او طلبات المعلومات بحيث يقضى النظام او الشبكة كل الوقت في محاولة الاستجابة لهذه الرسائل او الطلبات دون جدوى. ولكن المهاجمين الأكثر حنكة يمكنهم عرقلة الخدمة او تحويل مسارها او استبدالها بأخرى. وفي سياق أمن المعلومات ينصب التركيز بشكل عام على خدمات الشبكة التي يتم مهاجمتها عبر اتصالات الشبكة.

الحرمان من الخدمة (DoS): هو إجراء يمنع أو يضعف الاستخدام المصرح به للشبكات أو الأنظمة أو التطبيقات عن طريق استنفاد الموارد مثل وحدات المعالجة المركزية او الذاكرة او عرض النطاق الترددي او مساحات التخزين.

لذلك هناك عدة فئات من الموارد التي يمكن مهاجمتها :

1) **عرض النطاق الترددي للشبكة** - يتعلق بسعة روابط الشبكة التي تربط الخادم بالروابط الاوسع لنظام الإنترنت. فعرض النطاق الترددي للشبكة يتعلق بقدرة روابط الشبكة على ربط خادم ما بالإنترنت الأوسع (الخارجية) ولمؤسسة ما هو قدرتها علي الاتصال بمزود خدمة الإنترنت (ISP)، وعادةً ما يكون لهذا الاتصال بسعة أقل من الروابط الداخلية والبينية لأجهزة توجيه مزود الخدمة. وهذا يعني أنه من الممكن وصول المزيد من حركة المرور إلى أجهزة التوجيه الخاصة بمزود خدمة الإنترنت عبر الروابط ذات السعة العالية أكثر مما يمكن نقله داخليا عبر الروابط الداخلية الى المؤسسة. في هذه الحالة، يجب أن يتجاهل جهاز التوجيه بعض الحزم ، ويمرر فقط أكبر عدد ممكن يمكن التعامل معه بواسطة الروابط الداخلية. في التشغيل العادي للشبكة ، قد تحدث مثل هذه الأحمال العالية لخادم مشهور يواجه حركة مرور من عدد كبير من المستخدمين الشرعيين، وسيواجه جزء عشوائي من هؤلاء المستخدمين خدمة متدهورة أو غير موجودة نتيجة لذلك.

1- هجمات الحرمان من الخدمة (DoS)

في هجوم (DoS) ، تكون الغالبية العظمى من حركة المرور الموجهة إلى الخادم المستهدف ضارة ، ويتم إنشاؤها إما بشكل مباشر أو غير مباشر بواسطة المهاجم. يطغى هذا المرور على أي حركة مرور مشروعة ، مما يحرم المستخدمين الشرعيين من الوصول إلى الخادم بشكل فعال. اخيرا، تم توجيه بعض الهجمات الكبيرة إلى شبكة مزودي الخدمة (ISP) التي تدعم المؤسسة المستهدفة ، وذلك بهدف تعطيل اتصالاتها بالشبكات الأخرى.

2) **موارد النظام** - تهدف عادةً إلى زيادة التحميل أو تعطيل برامج مناولة الشبكة. يهدف هجوم (DoS) الذي يستهدف موارد النظام إلى زيادة التحميل أو تعطل برنامج مناول الشبكة. بدلاً من استهلاك النطاق الترددي لروابط الشبكة بأحجام كبيرة من حركة المرور، يتم إرسال أنواع معينة من الحزم التي تستهلك الموارد المحدودة المتاحة على النظام. وتشمل هذه التخزين المؤقت المستخدم للاحتفاظ بالحزم القادمة ، وجداول الروابط المفتوحة ، وغيرها. وهجوم (SYN) المخادع هو من هذا النوع ويستهدف جدول روابط (TCP) على الخادم. ويستخدم شكل آخر من أشكال هجوم على موارد النظام بحزم بيانات تتسبب في تحفيز شفرة برمجية خبيثة في برنامج مناول شبكة النظام ، مما يؤدي إلى تعطله. وهذا يعني أن النظام لم يعد بإمكانه الاتصال عبر الشبكة حتى يتم إعادة تحميل هذا البرنامج ، وذلك عن طريق إعادة الإقلاع بنظام مصاب، ويُعرف هذا باسم الحزمة المسمومة. كانت هجمات (ping) الكلاسيكية و هجمات قطرات الدموع التي تستهدف أنظمة (Windows 9x) القديمة من هذا الشكل، وكانت تستغل ثغرة في برمجية ويندوز الشبكية والتي تتعامل مع حزم طلبات الرد لبرتوكول متابعة الرسائل (ICMP) وتجزئة الحزمة ، على التوالي.

1- هجمات الحرمان من الخدمة (DoS)

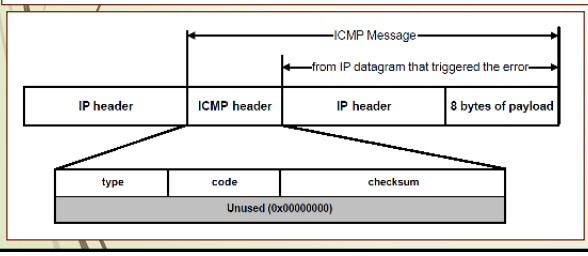
3) **موارد التطبيقات** - تهدف إلى انهاك لقدرات الخادم والحد من قدرته على الاستجابة لطلبات المستخدمين الآخرين. عادةً ما يتضمن الهجوم على تطبيق معين - مثل خادم الويب - عددًا من الطلبات الشرعية، كل منها يستهلك موارد كبيرة. وهذا يحد من قدرة الخادم على الاستجابة لطلبات المستخدمين الآخرين. على سبيل المثال ، قد يكون خادم الويب قادر على اجراء استعلامات على قاعدة البيانات، فإذا كان من الممكن إنشاء استعلام كبير ومكلف ، فأنه يمكن للمهاجم إنشاء عدد كبير منها مما ينتج عنه حمل شديد على الخادم. وهذا يحد من قدرته على الاستجابة للطلبات الشرعية من المستخدمين الآخرين. يُعرف هذا النوع من الهجوم باسم الإغلاق الإلكتروني (Cyberslam) . هناك بديل آخر وهو إنشاء طلب يتسبب في تحفيز برنامج خبيث في الخادم ، مما يتسبب في تعطله. هذا يعني أن الخادم لم يعد قادرًا على الاستجابة للطلبات حتى يتم إعادة تشغيله. قد تتميز هجمات (DoS) أيضًا بعدد الأنظمة المستخدمة لتوجيه حركة المرور إلى النظام المستهدف. في الأصل ، يتم استخدام نظام واحد فقط، أو عدد صغير من الأنظمة الواقعة مباشرة تحت سيطرة المهاجم. وهذا هو المطلوب لإرسال الحزم المطلوبة لأي هجوم يستهدف تحفيز شفرة برمجية خبيثة في مناول شبكة الخادم أو بعض التطبيقات. الهجمات التي تحتاج احجام مرورية ضخمة يتم عادة ارسالها من أنظمة متعددة في نفس الوقت باستخدام هجوم (DoS) موزع.

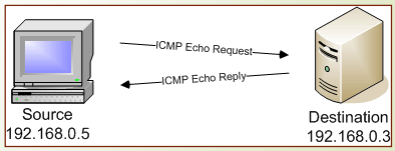
كانت هجمات الحرمان من الخدمة مشكلة لسنوات عديدة. أفاد استطلاع مكتب التحقيقات الفدرالي الأمريكي لجرائم الحاسوب والأمن لعام 2006 أن 25٪ من المستطلعين قد تعرضوا لشكل من أشكال هجوم الحرمان من الخدمة في السنة الماضية. وقد تفاوتت هذه القيمة بين 25٪ و 40٪ خلال السنوات الثماني الماضية من الدراسات الاستقصائية.

بروتوكول متابعة الرسائل (ICMP)

يعد برتوكول "متابعة الرسائل" - التحكم في الإنترنت - (Internet Control Message Protocol) (ICMP) لمتابعة وصول الرسائل و الإفادة عن أي خطأ في وصول هذه الرسائل الى وجهتها، وهو يستخدم بروتوكول الانترنت (IP) لإرسال المعلومات التي يحصل عليها عبر الشبكة؛ ويتم استخدامه بواسطة أجهزة الشبكة ، مثل أجهزة التوجيه (الموجه) ، لإرسال رسائل تشير للخطأ (على سبيل المثال ، الخدمة المطلوبة غير متوفرة أو تعذر الوصول إلى المضيف أو جهاز توجيه). عادة ما يتم استخدام (ICMP) بواسطة مهام تشخيص الشبكة ، مثل تحديد ما إذا كان النظام المضيف نشطا أو العثور على المسار الذي تستخدمه الحزم للوصول إلى المضيف. برتوكول (ICMP) يحدد ما اذا كان هناك ارتباط فعلي بين نظامين على الشبكة، وهو يستطيع كذلك ان يخبر المرسل من خلال رسائله المتنوعة ان المستقبل لا يستطيع التجاوب مع سرعة الارسال العالية التي يرسل بها حزم البيانات، ويظل يرسل هذه الرسائل حتى يقلل المرسل من سرعة ارساله الى الحد الذى يستطيع المستقبل التجاوب معه.

تستفيد الموجهات من هذه البرتوكول في اخطار موجه اخر عن وجود طريق افضل لمرور الرسالة، فيعاد توجيه الرسالة الى الطريق المناسب، كذلك رسالة "تجاوز المهلة المحددة لوصول الرسالة" والتي يستخدمها الموجه لإخطار المرسل بسبب عدم وصول رسالته.





يجب أن يستجيب المضيف لجميع طلبات (ICMP) بجواب (ICMP) الذى يحتوي على البيانات الدقيقة الواردة في رسالة الطلب .

بروتوكول إدارة الارتباط (TCP)

لفهم عمل هذه الهجمات نحتاج إلى مراجعة المخاطبة ثلاثية الاتجاهات الذي يستخدمه بروتوكول (TCP) لإنشاء ارتباط شبكي (الشكل التالي):

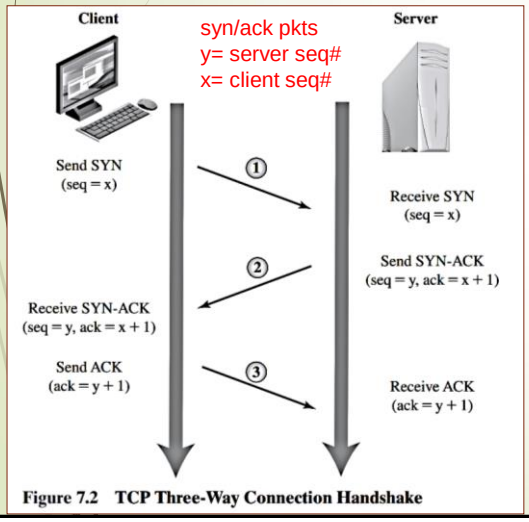


Figure 7.2 TCP Three-Way Connection Handshake

1) يبدأ نظام العميل طلب ارتباط (TCP) عن طريق إرسال حزمة (SYN) إلى الخادم. يحدد هذا عنوان العميل ورقم المنفذ (حيث يكون المنفذ على الخادم في وضع ترقب)، ويقدم رقم تسلسل أولي.
2) يسجل الخادم جميع التفاصيل المتعلقة بهذا الطلب في جدول ارتباطات (TCP) معروف، ثم يستجيب للعميل بحزمة (SYN-ACK) وتتضمن هذه رقم تسلسل للخادم ، ويزيد رقم تسلسل العميل لتأكيد على استلام حزمة (SYN) واستعداده للارتباط.
3) بمجرد أن يتلقى العميل ذلك ، فإنه يرسل حزمة (ACK) إلى الخادم برقم تسلسل خادم متزايد ، ويضع علامة على ان الارتباط قد تم إنشاؤه وتم التعارف. وبالمثل، عندما يتلقى الخادم حزمة (ACK) هذه، فإنه يشير أيضًا للارتباط على أنه تم إنشاؤه ويمكن لأي من الطرفين بعد ذلك متابعة نقل البيانات.

بروتوكول إدارة الارتباط (TCP)

من الناحية العملية يفشل هذا التبادل المثالي أحيانًا، حيث يتم نقل هذه الحزم باستخدام بروتوكول (IP) ، وهو بروتوكول شبكة غير موثوق به وإن كان هو الأفضل، فقد يتم فقد أي من الحزم أثناء النقل نتيجة الازدحام على سبيل المثال.

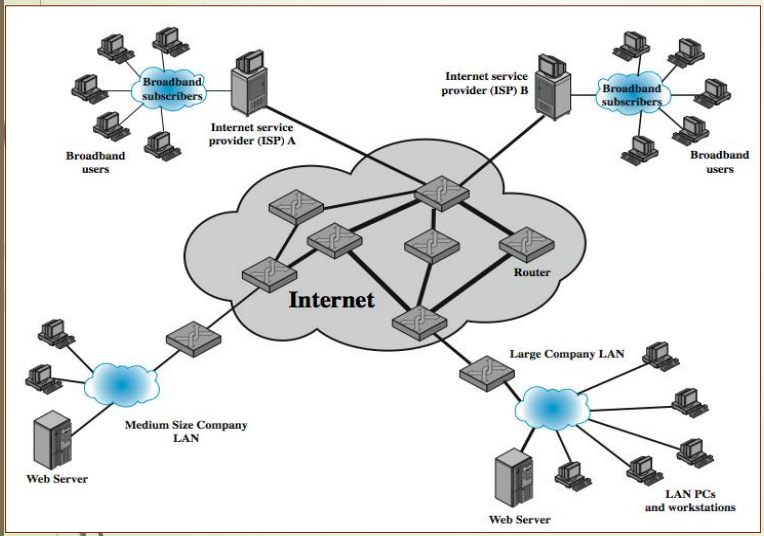
ومن ثم يتتبع كل من العميل والخادم الحزم التي أرسلوها ، وإذا لم يتم تلقي استجابة في وقت مقبول ، فسيعيد إرسال هذه الحزم. نتيجة لذلك ، ويعد بروتوكول (TCP) بروتوكول نقل موثوقًا به ، وأي تطبيقات تستخدمه لا تحتاج إلى الاهتمام بمشاكل الحزم المفقودة أو المعاد ترتيبها.

1- هجمات (DoS) : هجوم الحرمان من الخدمة التقليدي

هجوم (DoS) التقليدي هو هجوم إغراق المؤسسة بهدف التغلب على قدرتها للاتصال بالشبكة المستهدفة. إذا كان للمهاجم قدرة وصول إلى نظام له ارتباط بسعة عالية على شبكة ، فمن المحتمل أن ينتج عن هذا النظام حجم حركة مرور أعلى مما يمكن أن يتعامل معه ارتباط بسعة منخفضة للنظام المستهدف. فعلى سبيل المثال ، في الشبكة الموضحة في الشكل التالي ، قد يستخدم المهاجم خادم الويب لشركة كبيرة لاستهداف شركة متوسطة الحجم ذات اتصال شبكي منخفض السعة. قد يكون الهجوم بسيطًا مثل **فيضان (Ping)** موجه إلى خادم الويب للشركة المستهدفة. حيث يرسل الحاسوب رسالة طلب صدى (ICMP) إلى مضيف. يستجيب المضيف برسالة استجابة صدى (ICMP) ، مما يشير إلى أنه لا يزال نشطا. في هجوم فيضان (Ping) ، ترسل أجهزة حاسوب متعددة بسرعة عددا كبيرا من طلبات صدى (ICMP)، مما يؤدي إلى إرباك الخادم (وكذلك الشبكة) إلى الحد الذي لا يمكنه الاستجابة بسرعة كافية وستفشل الارتباطات المشروعة لعملاء اخرين وترفض أي ارتباطات جديدة.

ويتم معالجة حركة المرور هذه من خلال الروابط ذات السعة الأعلى على المسارات البينية، حتى الوصول إلى جهاز التوجيه النهائي في الإنترنت. في هذه المرحلة يتم التخلص من بعض الحزم ، ويستهلك الباقي معظم السعة الموجودة على الرابط إلى الشركة متوسطة الحجم. وسيكون لحركة المرور الشرعية الأخرى فرصة ضئيلة للاستمرار حتى يستجيب الموجه نتيجة للازدحام الشديد الناتج على هذا الارتباط. ففي **هجوم فيضان (Ping) التقليدي** ، يتم تحديد مصدر الهجوم بوضوح نظرًا لاستخدام عنوان المضيف كعنوان المصدر (المرسل) في حزم طلبات الرد لبروتوكول متابعة الرسائل (ICMP). وهذا له **عيبان** من وجهة نظر المهاجم. **أولاً** ، يتم تحديد مصدر الهجوم صراحةً ، مما يزيد من فرصة التعرف على المهاجم واتخاذ الإجراءات القانونية ردًا على ذلك. **ثانيًا** ، سيحاول النظام المستهدف الاستجابة للحزم المرسلة، ففي هذه الحالة أي حزم طلب الرد لبرتوكول متابعة الرسائل (ICMP) يستقبلها الخادم ، فإنه سيستجيب لكل منها بحزمة استجابة لطلب (ICMP) موجهة مرة أخرى إلى المرسل. وهذا يعكس بشكل فعال الهجوم مرة أخرى على النظام المصدر (المرسل). نظرًا لأن النظام المصدر يحتوي على نطاق ترددي أعلى للشبكة ، فمن المرجح أن ينجو من هذا الهجوم العكسي. ومع ذلك ، سيتأثر أداء شبكته بشكل ملحوظ ، مما يزيد مرة أخرى من فرص اكتشاف الهجوم واتخاذ الإجراءات اللازمة للرد. لكل من هذين السببين يرغب المهاجم في إخفاء هوية النظام المصدر. وهذا يعني أن أي حزم هجوم من هذا القبيل تحتاج إلى استخدام عنوان مزور أو وهمي.

1- هجمات (DoS) : هجوم الحرمان من الخدمة التقليدي



- على سبيل المثال ، في الشبكة الموضحة في الشكل ، قد يستخدم المهاجم خادم الويب للشركة الكبيرة ذات سعة اتصال عالي بالشبكة لاستهداف شركة متوسطة الحجم ذات اتصال بشبكة منخفض السعة.

1- هجمات (DoS) : تزوير عنوان المصدر (المرسل)

السمة الشائعة للحزم المستخدمة في العديد من أنواع هجمات (DoS) هي استخدام عناوين مصدر مزورة. يُعرف هذا باسم **تزوير عنوان المصدر**. ففي حالة الحصول على امتيازات كافية على شفرة برنامج مناول الشبكة على نظام الحاسوب ، فمن السهل إنشاء حزم بعنوان مصدر مزور (أو أي سمة أخرى مرغوبة). عادة ما يكون هذا النوع من الوصول عبر واجهة المقبس الشبكي في العديد من أنظمة التشغيل. تم توفير هذه الواجهة لاختبار مخصص للشبكة والبحث في بروتوكولات الشبكة، لا حاجة لها اثناء التشغيل العادي للشبكة. ومع ذلك ، لأسباب تتعلق بالتوافقية، تم الحفاظ على هذه الواجهة في العديد من أنظمة التشغيل الحالية. إن توفر هذه الواجهة القياسية يسهل إلى حد كبير مهمة أي مهاجم يحاول إنشاء حزم بسمات مزورة. بخلاف ذلك، سيحتاج المهاجم إلى تثبيت برنامج تشغيل مخصص على النظام المصدر (المضيف) للحصول على هذا المستوى من الوصول إلى الشبكة ، مما يعرضه للخطأ. وبوصول المهاجم إلى واجهة الشبكة ، يقوم المهاجم الآن بإنشاء كميات كبيرة من الحزم، وسيكون لكل منها النظام المستهدف كعنوان الوجهة ولكنها ستستخدم عناوين مصدر (المرسل) مختارة عشوائيًا ، وعادة ما تكون مختلفة لكل حزمة. ضع في اعتبارك مثال الفيضان بأمر (Ping) المذكور سابقا. سوف تتدفق هذه الحزم المخصصة لطلبات الرد لبروتوكول متابعة الرسائل (ICMP) عبر نفس المسار من المصدر باتجاه النظام المستهدف. مما يؤدي الى ازدحام على جهاز التوجيه على المسار النهائي ذو السعة المنخفضة. ومع ذلك ، فإن حزم الاستجابة لطلبات الرد لبروتوكول متابعة الرسائل (ICMP)، والتي تم إنشاؤها استجابة لتلك الحزم التي وصلت إلى النظام الهدف ، لن تنعكس مرة أخرى على النظام المصدر.

1- هجمات (DoS) : تزوير عنوان المصدر (المرسل)

بدلاً من ذلك ، سيتم نشرها عبر الإنترنت إلى جميع عناوين المصدر المزورة المختلفة. وقد تتوافق بعض هذه العناوين مع أنظمة حقيقية. وقد ترد هذه بشكل من أشكال حزم الخطأ ، لأنها لم تكن تتوقع أن تستلم حزمة الاستجابة . مما يزيد من اغراق حركة المرور الموجهة إلى النظام المستهدف. قد لا يتم استخدام بعض العناوين أو قد لا يمكن الوصول إليها. لذلك الحزم التي لا يمكن الوصول إلي وجهة (ICMP) المحدد بها يعاد ارسالها مرة أخرى، أو قد يتم ببساطة تجاهلها. أي حزم استجابة يتم إرجاعها تزيد من فيض تدفق حركة المرور الموجهة إلى النظام المستهدف. أن استخدام الحزم بعناوين مصدر مزورة يعني أن التعرف على نظام المهاجم أصعب بكثير، حيث يبدو أن حزم الهجوم قد نشأت من عناوين منتشرة عبر الإنترنت. ومن ثم ، فإن مجرد فحص رأس كل حزمة لا يكفي لتحديد مصدرها. حيث يخدع هذا الهجوم الأجهزة للاستجابة لطلبات كاذبة لضحية غير متوقعة. فهو يبث طلب (Ping) إلى جميع الحواسيب على الشبكة ولكنه يغير العنوان الذي جاء منه الطلب إلى حاسوب الضحية (يسمى هذا الانتحال لحاسوب آخر بالتحايل). هذا يجعل الأمر يبدو أن حاسوب الضحية يطلب ردا. ثم يرسل كل حاسوب استجابة إلى حاسوب الضحية بحيث يتم إرباكه بسرعة ثم يتعطل أو يصبح غير قابل للاستخدام الشرعي.

وللحد من تأثير هذا الهجوم ، يجب تحديد تدفق الحزم بشكل محدد عبر أجهزة التوجيه على طول المسار من المصدر إلى النظام المستهدف. يتطلب ذلك تعاون مهندسي الشبكات الذين يديرون جميع أجهزة التوجيه هذه وهي مهمة أصعب بكثير من مجرد قراءة عنوان المصدر، وهى ليست مهمة يمكن لمستلمي الحزم طلبها تلقائيًا. بدلاً من ذلك ، يتطلب الأمر عادةً من مهندسي الشبكة للاستعلام على وجه التحديد عن معلومات التدفق من أجهزة التوجيه الخاصة بهم، وهذه عملية يدوية تستغرق وقتًا وجهدًا للتنظيم.

1- هجمات (DoS) : تزوير عنوان المصدر (المرسل)

ان سبب السماح بالتزوير السهل لعناوين المصدر على الإنترنت يعود الى تاريخ تطوير بروتوكول (TCP/IP)، والذي حدث بشكل عام في بيئة تعاونية وموثوقة. لا يتضمن بروتوكول (TCP/IP) ببساطة القدرة ، افتراضيًا ، على التأكد من أن عنوان المصدر في الحزمة يتوافق فعليا مع عنوان النظام المصدر (المرسل). ومن الممكن فرض تصفية على أجهزة التوجيه للتأكد من ذلك (أو على الأقل ان هذا العنوان لشبكة المصدر شرعي). ومع ذلك ، يجب فرض هذا التصفية في أقرب نقطة من النظام المصدر (المرسل) ، حيث تكون معرفة عناوين المصادر الشرعية دقيقة قدر الإمكان. بشكل عام ، يجب أن يحدث هذا في النقطة التي تتصل فيها شبكة المؤسسة بالإنترنت الأوسع ، وعند حدود مزود خدمة الإنترنت الذي يوفر هذا الاتصال. على الرغم من أن هذه توصية الأمنية طويلة الأمد لمكافحة المشاكل مثل هجمات (DoS) ، لكن العديد من مزودي خدمة الإنترنت لا يطبقون مثل هذا التصفية. نتيجة لذلك ، تستمر الهجمات التي تستخدم حزم المصدر المخادعة في الحدوث بشكل متكرر.

هناك تأثير جانبي مفيد لتشتت حزم الاستجابة لبعض الحزم ذات المصدر المزور. فعندما أخذ باحثون امنيون مجموعة من عناوين (IP) غير المستخدمة ، والاعلان عن مساراتها، ثم جمعوا تفاصيل أي حزم مرسلة بهذه العناوين. نظرًا لعدم وجود أنظمة حقيقية تستخدم هذه العناوين ، فلا يجب توجيه أي حزم شرعية إليها، وأي حزم تم استلامها تعتبر ببساطة فاسدة. ومن الأرجح أنها نتيجة مباشرة أو غير مباشرة لهجمات علي الشبكة. وتعد حزم استجابة لطلب (ICMP) التي تم إنشاؤها ردًا على فيضان (Ping) باستخدام عناوين مصدر مزورة عشوائيًة مثالًا جيدًا على ذلك. يُعرف هذا باسم حركة المرور المبعثرة عكسيا (backscatter traffic). وتوفر مراقبة نوع الحزم معلومات قيمة عن نوع وحجم الهجمات المستخدمة.

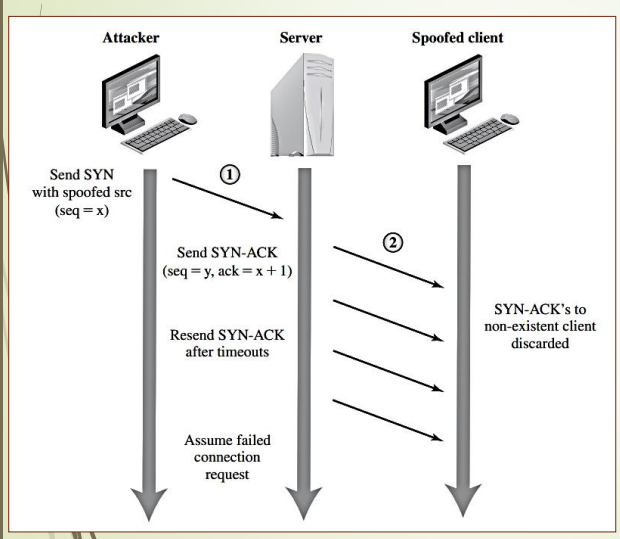
تزوير عنوان المصدر (ملخص)

- من الخصائص الشائعة للحزم المستخدمة في العديد من أنواع هجمات تعطيل الخدمة استخدام عناوين مصدر مزورة. يُعرف هذا باسم **تزوير عنوان المصدر**.
- في حال الحصول على امتيازات الكافية للوصول الى برنامج مناول الشبكة على نظام الحاسب ، فمن السهل إنشاء حزم بعنوان مصدر مزور (وفي الواقع أي سمة أخرى مرغوبة).
- عند التمكن من الوصول إلى واجهة الشبكة ، يقوم المهاجم بإنشاء كميات كبيرة من الحزم. سيكون لكل منها النظام الهدف كعنوان الوجهة ، ولكن مستخدمة عناوين مصدر يتم اختيارها عشوائيًا وعادةً ما تكون مختلفة لكل حزمة. وسوف تتدفق هذه الحزم على نفس المسار من المصدر نحو النظام الهدف.
- نفس الازدحام سيتم على جهاز التوجيه المرتبط بالمسار النهائي ذي السعة المنخفضة. ومع ذلك ، فإن حزم الاستجابة والتي تم إنشاؤها استجابة للحزم التي وصلت الى النظام المستهدف ، لن تنعكس مرة أخرى الى النظام المصدر. بدلاً من ذلك سيتم نشرها عبر الإنترنت لجميع عناوين المصادر المزورة المختلفة.
- قد تتوافق بعض هذه العناوين مع أنظمة حقيقية ، وقد لا يتم استخدام البعض الآخر أو لا يمكن الوصول إليها. بالإضافة إلى ذلك ، فإن استخدام حزم ذات عناوين مصدر مزورة يعني صعوبة التعرف على نظام المهاجم.
- حزم الهجوم تبدو و كأنها قد أنشأت من عناوين منتشرة عبر الإنترنت. ومن ثم فإن مجرد فحص رأس كل حزمة لا يكفي لتحديد مصدرها. وبدلاً من ذلك ، يجب تحديد تدفق الحزم بشكل معين عبر أجهزة التوجيه على طول المسار من المصدر إلى النظام الهدف.

1- هجمات (DoS) : تحايل (SYN) - SYN Spoofing

يعتبر هجوم **تحايل (SYN)** احد أنواع هجمات (DoS) التقليدية الشائعة. وهو يهاجم قدرة خادم الشبكة على الاستجابة لطلبات ارتباط (TCP) عن طريق تجاوز سقف حجم الجداول المستخدمة لإدارة مثل هذه الارتباطات. وهذا يعني أن طلبات الارتباط المستقبلية من المستخدمين الشرعيين ستفشل، مما يمنعهم من الوصول إلى الخادم. وبالتالي فهو هجوم على موارد النظام ، وتحديداً الشفرة البرمجية لمناول الشبكة في نظام التشغيل. لفهم طريقة عمل هذه الهجمات ، نحتاج إلى مراجعة تأكيد المخاطبة الثلاثي الذي يستخدمه بروتوكول (TCP) لإنشاء ارتباط، وكما هو موضح في الشكل السابق ذكره. يبدأ نظام العميل طلب ارتباط (TCP) عن طريق إرسال حزمة (SYN) إلى الخادم. يحدد هذا عنوان العميل ورقم المنفذ ويقدم رقم تسلسل أولي. قد يتضمن أيضًا طلبًا لخيارات (TCP) الأخرى. يسجل الخادم جميع التفاصيل المتعلقة بهذا الطلب في جدول لارتباطات (TCP) معروف. ثم يستجيب للعميل بحزمة (SYN+ACK). يتضمن هذا رقم تسلسلي للخادم ويزيد الرقم التسلسلي للعميل لتأكيد استلام حزمة (SYN). بمجرد أن يتلقى العميل ذلك ، فإنه يرسل حزمة (ACK) إلى الخادم برقم تسلسل الخادم مضاف اليه واحد ويضع علامة على الارتباط على أنه تم إنشاؤه. وبالمثل، عندما يتلقى الخادم حزمة (ACK) هذه، فإنه يشير أيضًا إلى ان الارتباط تم إنشاؤه وتم التعارف. يمكن لأي من الطرفين بعد ذلك متابعة نقل البيانات. أحيانا، من الناحية العملية، قد يفشل هذا التبادل المثالي، حيث يتم نقل هذه الحزم باستخدام (IP)، وهو بروتوكول شبكة غير موثوق به وإن كان هو الأفضل. على سبيل المثال، فقد يتم فقد أي من الحزم أثناء النقل نتيجة الازدحام. ونتيجة متابعة كل من العميل والخادم في ارسال حزمهما ، فإن لم يتم تلقي استجابة في وقت مقبول ، فسيعاد إرسال هذه الحزم. ونتيجة لذلك ، يعد بروتوكول (TCP) بروتوكول نقل موثوقًا به ، وأي تطبيقات تستخدمه لا تحتاج إلى الاهتمام بمشاكل الحزم المفقودة أو المعاد ترتيبها. ومع ذلك ، فإن هذا يفرض عبئًا على الأنظمة في إدارة هذا النقل الموثوق للحزم.

1- هجمات (DoS) : تحايل (SYN)



يستغل هجوم تحايل (SYN) هذا السلوك على الخادم المستهدف.

- ينشئ المهاجم عددًا من حزم طلبات ارتباط (SYN) بعناوين مصدر (مرسل) مزورة.
- لكل منها ، يسجل الخادم تفاصيل طلب ارتباط (TCP) ، ويرسل حزمة (SYN+ACK) إلى عنوان المصدر (المرسل) المطالب به ، كما هو موضح في الشكل.
- الفرضية : معظم الارتباطات ناجحة لذلك سوف تزال الجداول بسرعة.

1- هجمات (DoS) : تحايل (SYN)

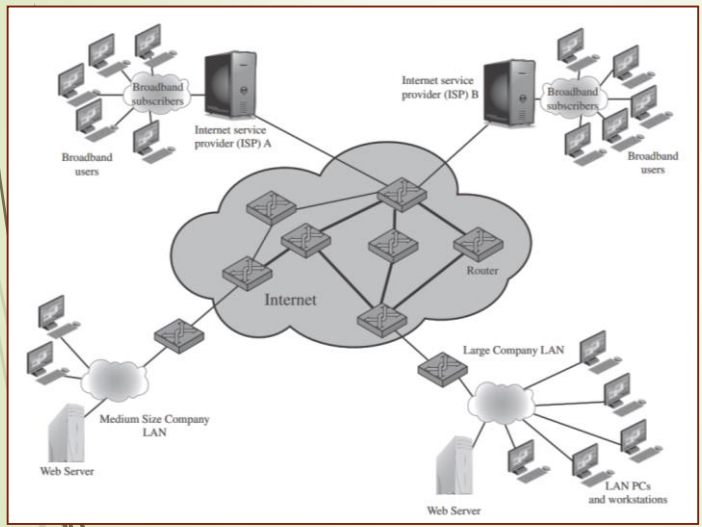
يستغل هجوم انتحال (SYN) هذا الاسلوب على الخادم المستهدف. ينشئ المهاجم عددًا من حزم طلبات ارتباط (SYN) بعناوين مصدر (مرسل) مزورة. ويسجل الخادم تفاصيل طلب ارتباط (TCP) لكل منها ويرسل حزمة (SYN+ACK) إلى عنوان المصدر المطالب به ، كما هو موضح في الشكل السابق. إذا كان هناك نظام صالح في هذا العنوان ، فسوف يستجيب بحزمة (RST) (إعادة تعيين) لإلغاء طلب هذا الارتباط الغير معرف. عندما يتلقى الخادم هذه الحزمة ، فإنه يلغي طلب الارتباط ويزيل المعلومات المحفوظة. ومع ذلك ، إذا كان النظام المصدر (المرسل) مشغولاً للغاية ، أو لا يوجد نظام على العنوان المزور، فلن يعود أي رد. في مثل هذه الحالة، سيقوم الخادم بإعادة إرسال حزمة (SYN+ACK) عدة مرات قبل افتراض فشل طلب الارتباط وحذف المعلومات المحفوظة المتعلقة به. في الفترة ما بين تلقي حزمة (SYN) الأصلية وافتراض الخادم بفشل الطلب ، فإن الخادم يستخدم مدخلاًت جدول الارتباط (TCP) المعرف. ويتم تحديد حجم هذا الجدول عادةً على افتراض أن معظم طلبات الارتباط تنجح بسرعة وأنه يمكن معالجة عدد معقول من الطلبات في وقت واحد. ومع ذلك، في هجوم انتحال (SYN)، يوجه المهاجم عددًا كبيرًا جدًا من طلبات الارتباط المزورة على الخادم المستهدف. تملأ هذه بسرعة جدول ارتباطات (TCP) المعرفة للخادم. بمجرد امتلاء هذا الجدول ، يتم رفض أي طلبات مستقبلية ، بما في ذلك الطلبات المشروعة من مستخدمين آخرين. ستنتهي مهلة الإدخال للجدول ومن ثم ستتم إزالتها ، مما يؤدي عند الاستخدام العادي للشبكة إلى مشاكل تجاوز سعة التخزين المؤقت و إجراءات تصحيحها. ومع ذلك ، إذا احتفظ المهاجم بكمية كافية من الطلبات المزورة متدفقة ، فسيمتلئ هذا الجدول باستمرار وسيتم قطع الخادم بشكل فعال عن الإنترنت ، ويكون غير قادر على الاستجابة لمعظم طلبات الارتباط المشروعة.

1- هجمات (DoS) : تحايل (SYN)

من أجل زيادة استخدام جدول ارتباطات (TCP) المعرفة، يرغب المهاجم بشكل مثالي في استخدام العناوين التي لن تجيب على (SYN+ACK) بجواب (RST) . يمكن القيام بذلك عن طريق التحميل الزائد على المضيف صاحب عنوان المصدر (المرسل) المزور المختار ، أو ببساطة عن طريق استخدام مجموعة واسعة من العناوين العشوائية. في هذه الحالة ، يعتمد المهاجم على حقيقة وجود العديد من العناوين غير المستخدمة على الإنترنت. وبالتالي ، فإن نسبة معقولة من العناوين التي تم إنشاؤها عشوائيًا لن تتوافق مع مضيف حقيقي. هناك فرق كبير في حجم حركة مرور الشبكة بين هجوم (SYN) المخادع وهجوم الإغراق (الفيضان) الأساسي الذي درسناه سابقا. يمكن أن يكون الحجم الفعلي لحركة مرور (SYN) منخفضًا نسبيًا، ولا يقترب من السعة القصوى للارتباط بالخادم، ولكنه يكون مرتفعًا بدرجة كافية لإبقاء جدول ارتباطات (TCP) المعرف ممتلئًا. على عكس هجوم الإغراق ، فإن هذا يعني أن المهاجم لا يحتاج إلى الوصول إلى ارتباط بشبكة كبير الحجم. في الشبكة الموضحة في الشكل التالي ، يمكن للمؤسسة متوسطة الحجم ، أو حتى مستخدم منزلي واسع النطاق ، مهاجمة خادم الشركة الكبيرة بنجاح باستخدام هجوم تحايل (SYN). ربما كان تدفق الحزم من خادم واحد أو هجوم (SYN) المخادع المنشأ من نظام واحد أكثر الأشكال المبكرة شيوعًا لهجمات (DoS)، وشكل هذا قيدًا كبيرًا، وتطورت الهجمات باستخدام أنظمة متعددة لزيادة فعاليتها.

1- هجمات (DoS) : تحايل (SYN) - شكل الهجوم

- في الشبكة الموضحة في الشكل ، يمكن للمؤسسة متوسطة الحجم ، أو حتى مستخدم منزلي واسع النطاق ، مهاجمة خادم شركة كبيرة بنجاح باستخدام هجوم تحايل (SYN).



2- هجمات الإغراق: (Flooding attacks)

تتخذ هجمات الاغراق أشكالًا متنوعة ، بناءً على بروتوكول الشبكة المستخدم لتنفيذ الهجوم. في جميع الحالات ، يكون القصد عمومًا هو زيادة التحميل على سعة الشبكة للارتباط بخادم ما. وقد يهدف الهجوم بدلاً من ذلك إلى زيادة الحمل على قدرة الخادم على معالجة حركة المرور والاستجابة لها. تغمر هذه الهجمات روابط الشبكة بالخادم بسيل من الحزم الخبيثة تنافس وتغلب حركة المرور الشرعية المتدفقة إلى الخادم. ويسبب هذا ازدحام لبعض أجهزة التوجيه على المسار إلى الخادم المستهدف، وينتج عنه حذف للعديد من الحزم. هذا الاغراق يسبب احتمالية بقاء حركة المرور الشرعية التي تصل الى الخادم منخفضة ، مما ينتج عن هذا ان قدرة الخادم على الاستجابة لطلبات الارتباط بالشبكة إن تدهور بشدة أو تفشل تمامًا.

يمكن استخدام أي نوع من حزم الشبكة تقريبًا في هجوم الاغراق. إنه يحتاج ببساطة إلى أن يكون من النوع المسموح له بالتدفق عبر الروابط نحو النظام المستهدف، بحيث يمكنه استهلاك كل السعة المتاحة على رابط ما إلى الخادم المستهدف. في الواقع ، كلما كانت الحزمة أكبر كان الهجوم أكثر فعالية.

تستخدم هجمات الإغراق الشائعة أيًا من أنواع حزم (ICMP) أو (UDP) أو (TCP-SYN). من الممكن أيضًا الإغراق ببعض أنواع حزم (IP) الأخرى، ولكن نظرًا لأن هذه أقل شيوعًا واستخدامها معروف فمن السهل تصفيتها وبالتالي يمكن إعاقة أو منع مثل هذه الهجمات.

2- هجمات الإغراق: الإغراق ببرتوكول (ICMP)

يُعتبر الإغراق (Ping) باستخدام حزم طلبات برتوكول (ICMP) التي تمت مناقشتها سابقا مثالًا كلاسيكيًا على هجوم الإغراق ببرتوكول (ICMP). تم اختيار هذا النوع من حزم (ICMP) نظرًا لأنه تقليديًا يسمح مشرفي الشبكة لمثل هذه الحزم في شبكاتهم كأداة مفيدة لتشخيص الشبكة. في الآونة الأخيرة، قامت العديد من المؤسسات بتقييد قدرة هذه الحزم على المرور عبر جدران الحماية الخاصة بها. رداً على ذلك ، بدأ المهاجمون في استخدام أنواع أخرى من حزم (ICMP)، وذلك للحاجة اليها في التشغيل الصحيح لبرتوكول (TCP/IP)، فمن المرجح أن يتم السماح بها من خلال جدار حماية المؤسسة. قد يؤدي تصفية بعض أنواع حزم (ICMP) المهمة إلى تدهور أو قطع في العمل العادي لشبكة (TCP/IP). عنوان وجهة (ICMP) الذى يتعذر الوصول إليها والحزم التي تجاوزات المهلة الزمنية هي أمثلة على أنواع من الحزم المهمة.

يمكن للمهاجم إنشاء اعداد كبيرة من أحد أنواع هذه الحزم. ونظرًا لأن هذه الحزم تتضمن جزءًا من بعض الحزم الخاطئة التي من المفترض أنها تسببت في الخطأ الذي تم الإبلاغ عنه ، فيمكن جعلها كبيرة نسبيًا مما يزيد من فعاليتها في إغراق الارتباط.

2- هجمات الإغراق: الإغراق ببرتوكول (UDP)

يتمثل أحد البدائل لاستخدام حزم (ICMP) هي استخدام حزم (UDP) الموجهة إلى رقم منفذ معين، وبالتالي خدمة محتملة على النظام المستهدف. والاختيار الشائع هو حزمة موجهة إلى خدمة تشخيصية حيث انها عادة مفعلة على العديد من أنظمة الخوادم. فإذا كانت هذه الخدمة قيد التشغيل على الخادم، فسوف يستجيب بحزمة (UDP) إلى المصدر المطالب بها وتتضمن بيانات الحزمة الأصلية. وإذا لم تكن الخدمة قيد التشغيل فسيتم تجاهل الحزمة، وربما يتم إرجاع حزمة لا يمكن لوجهة (ICMP) الوصول إلى المرسل. بهذا، فعليا حقق الهجوم هدفه المتمثل في شغل سعة على الرابط إلى الخادم. يمكن استخدام أي منفذ (UDP) لهذه الغاية، وأي حزمة استجابة يتم إنشاؤها تعمل على زيادة الحمل على الخادم وروابط الشبكة الخاصة به. إذا تم إنشاء الهجوم باستخدام نظام واحد فُستخدم عادة عناوين مصدر مزورة لنفس أسباب هجمات (ICMP). وإذا تم استخدام أنظمة متعددة للهجوم ، فغالبًا ما يتم استخدام العناوين الحقيقية للأنظمة الزومبي المخترقة. كذلك عند استخدام أنظمة متعددة، فإن مضاعفات كل من التدفق العكسي للحزم والقدرة على تحديد المهاجم تعتبر محدودة.

2- هجمات الإغراق: الإغراق ببرتوكول (TCP-SYN)

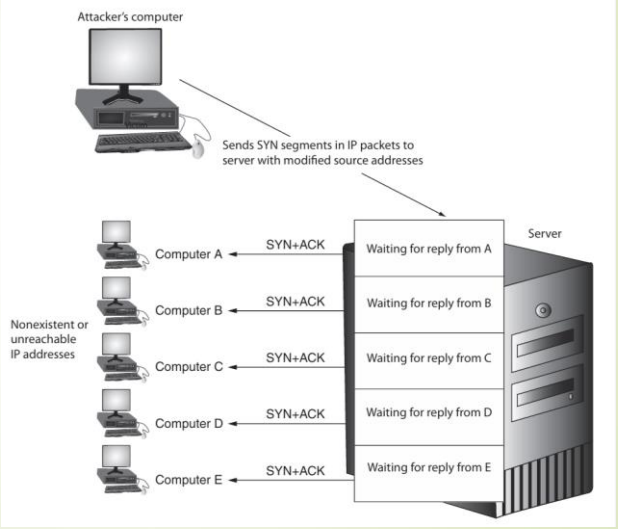
بديل آخر هو إرسال حزم (TCP) إلى النظام المستهدف. على الأرجح ستكون هذه طلبات ارتباط (TCP) عادية ، مع عناوين مصدر حقيقية أو مزورة فسيكون لها تأثير مشابه لهجوم تحايل (SYN) الذي وصفناه سابقا.

يستفيد هجوم فيضان (SYN) من إجراءات بدء الجلسة . في ظل ظروف الشبكة العادية وباستخدام برتوكول TCP/IP، يتصل الجهاز بخادم شبكة لطلب مثلا عرض صفحة ويب أو فتح ملف. يستخدم هذا الطلب رسالة تحكم، تسمى رسالة مزامنة أو (SYN) ، وذلك لتهيئة الارتباط. يستجيب الخادم مرة أخرى (SYN) الخاص به مع إقرار (ACK) بأنه تلقى الطلب الأولي ، يسمى (SYN + ACK) . ثم ينتظر الخادم رد (ACK) من الجهاز يشير إلى أنه تلقى (SYN) الخاص بالخادم. للسماح بارتباط بطيء ، قد ينتظر الخادم فترة من الوقت للرد. بمجرد رد الجهاز ، يمكن أن يبدأ نقل البيانات.

ففي هذه الحالة ، فإن الهدف من الهجوم هو الكم الإجمالي من الحزم وليس برمجيات النظام. هذا هو الفرق بين هجوم تحايل (SYN) وهجوم إغراق (SYN). أيضًا، يمكن أن يستخدم هذا الهجوم حزم بيانات (TCP) والتي سيرفضها الخادم لأنها لا تنتمي إلى أي ارتباط معرف وبحلول ذلك يكون الهجوم فعليا نجح في إغراق الروابط بالخادم.

2- هجمات الإغراق: الإغراق ببرتوكول (TCP-SYN)

في هجوم فيضان (SYN) ضد خادم ويب ، يرسل المهاجم مقاطع (SYN) في حزم (IP) إلى الخادم. ومع ذلك، يقوم المهاجم بتعديل العنوان المصدر لكل حزمة إلى عناوين حواسيب غير موجودة أو لا يمكن الوصول إليها. يستمر الخادم في "الاحتفاظ بالخط مفتوح" وانتظر الرد (الذي لن يأتي) أثناء تلقي المزيد من الطلبات الخاطئة وإبقاء المزيد من الخطوط مفتوحة للردود. بعد فترة قصيرة من الوقت تنفد موارد الخادم ولم يعد بإمكانه الاستجابة للطلبات المشروعة أو العمل بشكل صحيح. يوضح الشكل التالى خادما ينتظر الردود أثناء هجوم فيضان (SYN).



3- هجوم الحرمان من الخدمة الموزع (Distributed Denial of Service) (DDoS)

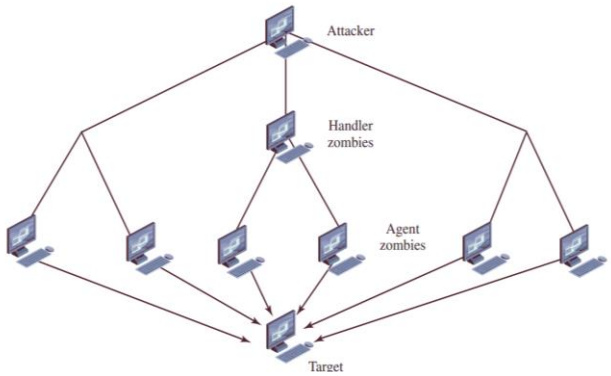
نتيجة للقيود على هجمات الإغراق التي تشن من نظام واحد ، تم تطوير أدوات هجوم (DoS) وذلك باستخدام أنظمة متعددة لشن الهجمات، حيث تم اختراق هذه الأنظمة التي عادةً ما تكون محطات عمل أو حواسيب شخصية. يستخدم المهاجم برامج خبيثة لتخريب النظام وتثبيت عامل هجوم يمكنه من التحكم في النظام المخترق ، وتُعرف هذه الأنظمة باسم **الزومبي**.

يمكن إنشاء مجموعات كبيرة من هذه الأنظمة تحت سيطرة مهاجم واحد ، لتشكيل كلها بشكل جماعي شبكة روبوت. هذه الشبكات من الأنظمة المخترقة هي أداة مفضلة للمهاجم ، ويمكن استخدامها لمجموعة متنوعة من الأغراض منها هجوم الحرمان من الخدمة الموزع (DDoS).

في مثال الشبكة الموضحة في الشكل المذكور (شريحة-18)، قد يتم اختراق بعض أنظمة التي تستخدم نطاق ترددى عريض واستخدامها كزومبي لمهاجمة شركة أو روابط الأخرى. بينما يمكن للمهاجم أن يأمر كل زومبي على حدة ، ويتم استخدام التسلسل الهرمي للتحكم بشكل عام، حيث يعمل عدد قليل من الأنظمة كوكلاء تتحكم في عدد أكبر بكثير من الأنظمة العميلة ، كما هو موضح في شكل هيكلية الهجوم التالي . هناك عدد من المزايا لهذا الترتيب، حيث يمكن للمهاجم إرسال أمر واحد إلى وكيل ، والذي يقوم بدوره بإعادة توجيهه تلقائيًا إلى جميع العملاء الخاضعين لسيطرته. يمكن أيضًا استخدام أدوات الاصابة المؤتمتة للبحث عن أنظمة الزومبي المناسبة و اختراقها. بمجرد تحميل برنامج العميل إلى نظام تم اختراقه حديثًا ، يمكنه الاتصال بواحد أو أكثر من الوكلاء لإخطارهم تلقائيًا بجهوزيته. وبهذه الوسيلة يمكن للمهاجم أن ينمي شبكات روبوت مناسبة تلقائيًا.

3- هجوم الحرمان من الخدمة الموزع (DDoS)

واحدة من أقدم وأشهر أدوات (DDoS) هي (Tribe Flood Network)- (TFN).
تستخدم كل من (TFN) و (TFN2K) إصدارًا من التسلسل الهرمي للأوامر المكون من طبقتين كما هو موضح في الشكل السابق . كان العميل عبارة عن برنامج حصان طروادة تم نسخه وتشغيله على أنظمة الزومبي المخترقة. كانت قادرة على تنفيذ أشكال من هجوم اغراق (ICMP)، واغراق (SYN) ، واغراق (UDP). لا يقوم (TFN) بانتحال عناوين المصدر (المرسل) في حزم الهجوم، ولكن وبدلاً من ذلك ، فقد اعتمد على العدد الضخم من الأنظمة المخترقة ، وهيكلية الأوامر ذي الطبقات ، لإخفاء مسار العودة إلى المهاجم.



يرسل المهاجم أمرًا واحدًا إلى الوكلاء الزومبي؛ الوكيل يعيد توجيهه إلى الوكلاء والعملاء الآخريين.

الوكيل عبارة عن برنامج من سطر أوامر يعمل على بعض الأنظمة المخترقة. ويصل المهاجم إلى هذه الأنظمة باستخدام أي آلية مناسبة تمنح وصولاً لجذر نظام التشغيل ، ثم تشغّيل برنامج الوكيل بالخيارات المرغوبة. يمكن لكل وكيل التحكم في عدد كبير من الأنظمة العميلة والمحددة مسبقا في القائمة. تم تشفير الاتصالات بين الوكيل وعملائه ويمكن مزجها مع عدد من حزم المخادعة، مما يعيق محاولات رصد وتحليل حركة التحكم في المرور.

3- هجوم الحرمان من الخدمة الموزع (DDoS)

تم تطوير العديد من أدوات (DDoS) الأخرى، فبدلاً من استخدام برامج معالجة مخصصة ، يستخدم الكثير منها الآن برنامج خادم المراسلة الفورية ، أو خوادم (HTTP) على شبكة الإنترنت ، لإدارة الاتصالات مع الوكلاء. تستخدم العديد من هذه الأدوات الحديثة أيضًا آليات التشفير لمصادقة العملاء إلى الوكلاء ، ومن أجل إعاقة تحليل حركة مرور الأوامر.

أفضل دفاع ضد أن تكون مشاركًا بغير قصد في هجوم (DDoS) هو منع اختراق أنظمتك. يتطلب ذلك ممارسات أمان جيدة للنظام والحفاظ على أنظمة التشغيل والتطبيقات الموجودة على هذه الأنظمة محدثة ومصححة.

بالنسبة للأنظمة المستهدفة لهجوم (DDoS) تكون الاستجابة مماثلة لأي هجوم إغراق ولكن بحجم وتعقيد أكبر.

4- مكافحة هجمات الحرمان من الخدمة (DoS)

هناك عدد من الخطوات التي يمكن اتخاذها للحد من عواقب كونك هدفًا لهجوم (DoS) وللحد من فرصة اختراق أنظمتك ثم استخدامها لشن هجمات (DoS). من المهم أن ندرك أنه لا يمكن منع هذه الهجمات بالكامل. على وجه الخصوص ، إذا تمكن المهاجم من توجيه حجم ضخم الكافي من حركة المرور المشروعة إلى نظامك ، فهناك احتمال كبير أن يؤدي ذلك إلى إرباك اتصال شبكة النظام ، وبالتالي الحد من طلبات المرور المشروعة للمستخدمين الآخرين. في الواقع ، يحدث هذا أحيانًا عن طريق الصدفة نتيجة الدعاية الكبيرة حول موقع معين.

تقليديًا ، غالبًا ما يؤدي النشر على مواقع تجميع الأخبار الشهيرة إلى زيادة التحميل على نظام خادم المواقع المشار إليها. فمثلا ، عند حدوث أحداث رياضية شهيرة مثل الأولمبياد أو مباريات كأس العالم لكرة القدم ، تشهد المواقع التي تقدم تقارير عنها مستويات حركة مرور عالية جدًا. وقد أدى ذلك إلى استخدام المصطلحات مثل: النقطة المائلة (*slash dotted*) أو حشد فلاش (*flash crowd*) أو حدث فلاش (*flash event*) ، لوصف مثل هذه الأحداث. هناك القليل جدًا مما يمكن فعله لمنع هذا النوع من التحميل الزائد العرضي أو المتعمد دون المساس بأداء الشبكة أيضًا. الاستجابة المعتادة هي توفير عرض النطاق الترددي الفائض للشبكة والخوادم الموزعة المكررة ، لا سيما عند توقع الحمل الزائد. يتم ذلك بانتظام للمواقع الرياضية الشهيرة. ومع ذلك ، فإن هذه الاستجابة لها تكلفة تنفيذية كبيرة.

4- مكافحة هجمات الحرمان من الخدمة (DoS)

بشكل عام ، هناك أربعة خطوط دفاع ضد هجمات (DDoS) :

- منع الهجوم والوقاية منه (قبل الهجوم): هذه الآليات تمكن الضحية من تحمل محاولات الهجوم دون حرمان العملاء الشرعيين من الخدمة. تتضمن الأساليب فرض سياسات لاستهلاك الموارد وتوفير موارد احتياطية متاحة عند الطلب. بالإضافة إلى ذلك ، تقوم آليات المنع بتعديل الأنظمة والبروتوكولات على الإنترنت لتقليل احتمالية هجمات (DDoS) .
- اكتشاف الهجوم وتصفيته (أثناء الهجوم): تحاول هذه الآليات اكتشاف الهجوم فور بدئه والاستجابة له على الفور. هذا يقلل من تأثير الهجوم على النظام المستهدف. يتضمن الاكتشاف البحث عن أنماط السلوك المشبوهة. تتضمن الاستجابة تصفية الحزم التي يحتمل أن تكون جزءًا من الهجوم.
- تتبع مصدر الهجوم وتحديد هويته (أثناء الهجوم وبعده): هذه محاولة لتحديد مصدر الهجوم كخطوة أولى في منع الهجمات المستقبلية. ومع ذلك ، فإن هذه الطريقة عادة لا تسفر عن نتائج سريعة بما يكفي ، إن وجدت ، للتخفيف من هجوم مستمر.
- رد فعل الهجوم (بعد الهجوم): هذه محاولة للقضاء على آثار الهجوم أو الحد منها.

4- مكافحة هجمات الحرمان من الخدمة (DoS): منع الهجوم والوقاية

يعد استخدام عناوين المصدر (المرسل) مزورة أحد المكونات الحاسمة للعديد من هجمات (DoS) . وهذه إما تحجب النظام المرسل الاصلي لهجمات (DoS) المباشرة والموزعة أو تستخدم لتوجيه حركة المرور المنعكسة إلى النظام المستهدف. ومن ثم فإن إحدى التوصيات الأساسية والأطول أمداً للدفاع ضد هذه الهجمات هي الحد من قدرة الأنظمة على إرسال حزم مع عناوين مصادر مزورة. للقضاء على هجمات الحرمان من الخدمة التي تستخدم انتحال عنوان المصدر يوصى بتصفية دخول للشبكة. ويجب إجراء هذا التصفية بالقرب من المصدر قدر الإمكان ، عن طريق أجهزة التوجيه أو البوابات التي تعرف نطاقات العناوين الصالحة للحزم الواردة. عادةً ما يكون هذا هو مزود خدمة الإنترنت الذي يوفر اتصال الشبكة لمؤسسة أو مستخدم منزلي. يعرف مزود خدمة الإنترنت العناوين المخصصة لجميع عملائه ، وبالتالي فهو في أفضل وضع لضمان استخدام عناوين مصدر شرعية في جميع الحزم من عملائه. يمكن تنفيذ هذا النوع من التصفية باستخدام قواعد صريحة للتحكم في الوصول في جهاز توجيه للتأكد من أن عنوان المصدر في أي حزمة عميل هو عنوان مخصص لمزود خدمة الإنترنت.

بدلاً من ذلك ، يمكن استخدام المصفيات للتأكد من أن مسار العودة إلى عنوان المصدر المطالب به هو الذي تستخدمه الحزمة الحالية.

على سبيل المثال ، يمكن القيام بذلك على أجهزة توجيه (Cisco) باستخدام الأمر (ip verify unicast reverse-path) . قد لا يكون هذا النهج الأخير ممكنًا لبعض مزودي خدمة الإنترنت الذين يستخدمون بنية تحتية معقدة ومتكررة للتوجيه.

4- مكافحة هجمات الحرمان من الخدمة (DoS): منع الهجوم والوقاية

يضمن تنفيذ شكل من أشكال هذه التصفية أن عملاء مزود خدمة الإنترنت لا يمكن أن يكونوا مصدر الحزم المزورة. للأسف ، على الرغم من أن هذه التوصية معروفة جيدًا ، لا يزال العديد من مزودي خدمة الإنترنت لا يقومون بهذا النوع من التصفية. على وجه الخصوص ، أولئك الذين لديهم أعداد كبيرة من المستخدمين المنزليين المتصلين بالنطاق العريض فهم مصدر قلق كبير. غالبًا ما يتم استهداف مثل هذه الأنظمة للهجوم لأنها غالبًا ما تكون أقل أمانًا من أنظمة الشركات. بمجرد اختراقها ، يتم استخدامها بعد ذلك كوسطاء في هجمات أخرى ، مثل هجمات (DoS) . من خلال عدم تنفيذ مصفيات مكافحة الانتحال يساهم مزودو خدمات الإنترنت بشكل واضح في هذه المشكلة. غالبًا ما يتم تقديم حجة لعدم القيام بذلك وهي تأثير الأداء على أجهزة التوجيه الخاصة بهم، حيث تتكبد عملية التصفية عقبات بسيطة نتيجة الاضطرار إلى معالجة كميات من حركة المرور الهجومية. نظرًا لارتفاع معدل انتشار هجمات (DoS) ، لا يوجد ببساطة أي مبرر لأي مزود خدمة إنترنت أو مؤسسة لعدم تنفيذ مثل هذه التوصية الأمنية الأساسية.

لأي دفاعات ضد هجمات الإغراق يجب تحديد موقعها الأصلي على الإنترنت وليس على جهاز توجيه الذى في حدود المؤسسة المستهدفة ، نظرًا لأن هذا يقع عادةً بعد تعرض المورد للهجوم. لذلك يجب تطبيق التصفية على حركة المرور قبل أن تغادر شبكة مزود خدمة الإنترنت ، أو حتى عند نقطة الدخول إلى شبكته. في حين أنه من غير الممكن، بشكل عام ، تحديد الحزم ذات عناوين المصدر المزورة ، فإن استخدام مصفي المسار العكسي يمكن أن يساعد في تحديد بعض هذه الحزم حيث يختلف المسار من مزود خدمة الإنترنت إلى العنوان المزور عن المسار الذي تستخدمه الحزمة للوصول إلى مزود خدمة الإنترنت.

4- مكافحة هجمات الحرمان من الخدمة (DoS): منع الهجوم والوقاية

أيضًا ، يمكن خنق الهجمات التي تستخدم أنواع حزم معينة ، مثل اغراق (ICMP) أو اغراق (UDP) ، من خلال فرض قيود على المعدل الذي سيتم به قبول هذه الحزم. في التشغيل العادي للشبكة ، يجب أن تشكل هذه جزءًا صغيرًا نسبيًا من الحجم الإجمالي لحركة مرور الشبكة. تمتلك العديد من أجهزة التوجيه ، وخاصة أجهزة التوجيه المتطورة التي يستخدمها مزودو خدمة الإنترنت ، القدرة على الحد من معدلات الحزم. يمكن أن يساعد وضع حدود معدل مناسبة على هذه الأنواع من الحزم في التخفيف من تأثير الإغراق باستخدام هذه الحزم ، مما يسمح لأنواع أخرى من حركة المرور بالتدفق إلى المنظمة المستهدفة حتى في حالة حدوث هجوم.

أحد الدفاعات ضد هجمات الفيضانات (DoS) و (DDoS SYN) هو استخدام واقي الفيضانات. واقي الفيضانات هو ميزة تتحكم في تحمل النظام لطلبات الخدمة التي لم يتم الرد عليها وتساعد على منع هجوم (DoS) .يمكن لمسؤول الشبكة تعيين الحد الأقصى لعدد الاتصالات "النامية" التي سيتحملها النظام. بمجرد الوصول إلى هذا الحد ، يتم اعتراض كل (SYN) وارد موجه إلى الخادم المتأثر وإفلاته ، ويتم إرجاع حزمة (SYN + ACK) فارغة. توجد واقيات الفيضانات بشكل شائع على جدران الحماية وأنظمة كشف التسلل (IDS) وأنظمة منع التسلل (IPS).

من الممكن الدفاع بشكل خاص ضد هجوم انتحال (SYN) باستخدام نسخة معدلة من برنامج مناول الارتباط (TCP). فبدلاً من حفظ تفاصيل الارتباط على الخادم ، يتم تشفير المعلومات الهامة حول الارتباط المطلوب بشكل مشفر في ملف تعريف الارتباط يتم إرساله كرقم التسلسل الأولي للخادم. يتم إرسال هذا في حزمة (SYN-ACK) من الخادم إلى العميل مرة أخرى. عندما يستجيب العميل الشرعي بحزمة (ACK) تحتوي على ملف تعريف الارتباط برقم تسلسلي متزايد ، يكون الخادم عندئذٍ قادرًا على إعادة بناء المعلومات حول الارتباط الذى سيحفظه عادةً في جدول ارتباط (TCP) معرف. عادةً ما يتم استخدام هذه التقنية فقط عندما يفيض الجدول. وتتميز بميزة عدم استهلاك أي موارد ذاكرة على الخادم حتى اكتمال مخاطبة ارتباط (TCP) ثلاثي الاتجاهات. عندئذٍ يكون لدى الخادم ثقة أكبر في أن عنوان المصدر يتوافق بالفعل مع عميل حقيقي يتفاعل مع الخادم.

4- مكافحة هجمات الحرمان من الخدمة (DoS): منع الهجوم والوقاية

هناك بعض عيوب هذه التقنية، حيث يستغرق الأمر موارد حسابية على الخادم لحساب ملف تعريف الارتباط. كما أنه يحظر استخدام بعض امتدادات (TCP) ، مثل النوافذ الكبيرة. عادةً ما يتم حفظ طلب لمثل هذا الامتداد بواسطة الخادم ، إلى جانب تفاصيل أخرى للارتباط المطلوب. ومع ذلك ، لا يمكن تشفير معلومات الارتباط هذه في ملف تعريف الارتباط نظرًا لعدم وجود مساحة كافية للقيام بذلك. والبديل هو أن يرفض الخادم الارتباط تمامًا لأنه لا توجد لديه موارد متبقية لإدارة الطلب ، لكن لا يزال هذا تحسينًا في قدرة النظام على التعامل مع أحمال طلب الارتباط العالية.

بدلاً من ذلك ، يمكن تعديل برنامج الشبكي (TCP/IP) الخاص بالنظام لإسقاط بشكل انتقائي مدخلات ارتباط غير مكتمل من جدول ارتباطات (TCP) عند فيضانه ، مما يسمح بمتابعة محاولة ارتباط جديدة. يُعرف هذا **بالإسقاط الانتقائي** . بافتراض أن غالبية المدخلات في جدول الفائض ناتجة عن الهجوم ، فمن المرجح أن الإدخال الذي تم إسقاطه سيتوافق مع حزمة هجوم. ومن ثم لن يكون لإزالته أي عواقب. إذا لم يكن الأمر كذلك ، فستفشل محاولة ارتباط مشروعة ، وسيتعين عليها إعادة المحاولة. وعلى كل حال ، فإن هذا الأسلوب يعطي فرصة لمحاولات الارتباط الجديدة للنجاح بدلاً من إسقاطها فورًا عند تجاوز الجدول.

4- مكافحة هجمات الحرمان من الخدمة (DoS): منع الهجوم والوقاية

دفاع آخر ضد هجمات انتحال (SYN) يتضمن تعديل المتغيرات المستخدمة في برنامج الشبكي (TCP/IP) للنظام. وتشمل هذه حجم جدول ارتباطات (TCP) وفترة المهلة المستخدمة لإزالة الإدخالات من هذا الجدول عند عدم تلقي أي استجابة. يمكن دمجها مع حدود المعدل المناسبة لاتصال شبكة المؤسسة لإدارة الحد الأقصى المسموح به لطلبات الارتباط. لا يمكن لأي من هذه المتغيرات منع هذه الهجمات لكنها تجعل مهمة المهاجم أكثر صعوبة. كما أشرنا سابقًا ، يعد أسلوب التصفية ضد الانتحال من توصيات الأمان الطويلة الأمد التي يجب على جميع المؤسسات تنفيذها. بشكل عام، يمكن أن يؤدي تقييد أو حظر حركة المرور للخدمات المشبوهة ، أو مجموعات من مناقذ المصدر والوجهة إلى تقييد أنواع هجمات الانعكاس التي يمكن استخدامها ضد مؤسسة.

يتطلب الدفاع ضد الهجمات على موارد التطبيقات عمومًا تعديل التطبيقات المستهدفة ، مثل خوادم الويب. قد تتضمن الدفاعات محاولات للتمييز و التعرف على التعاملات المشروعة من التعاملات الناتجة من هجمات (DoS) آلية. غالبًا ما تتخذ هذه الأشكال شكل أحجية رسومية ، وهي كلمة التحقق (captcha) ويسهل حلها لمعظم المستخدمين ولكن يصعب تشغيلها آليًا. يتم استخدام هذا الأسلوب من قبل العديد من المواقع الكبيرة مثل (Hotmail) و (Yahoo) . كذلك ، قد تحد التطبيقات بعض أنواع التعاملات من أجل الاستمرار في تقديم شكل من أشكال الخدمة. إلى جانب هذه الدفاعات المباشرة ضد آليات هجوم (DoS)، يجب الحفاظ على ممارسات أمان النظام الجيدة بشكل عام. والهدف هو ضمان عدم تعرض أنظمتك للخطر واستخدامها كأنظمة زومبي. هناك حاجة أيضًا إلى التهيئة المناسبة ومراقبة الأداء المحموم.

أخيرًا ، إذا كانت مؤسسة ما تعتمد على خدمات الشبكة ، فيجب أن تفكر في نسخ هذه الخوادم وتكرارها عبر مواقع متعددة مع اتصالات شبكة متعددة. هذه ممارسة عامة جيدة للخوادم عالية الأداء ، وتوفر مستويات أعلى من الموثوقية وتحمل الأخطاء بشكل عام وليس مجرد استجابة لهذه الأنواع من الهجمات.

4- مكافحة هجمات الحرمان من الخدمة (DoS): الاستجابة للهجوم

- من أجل الاستجابة بنجاح لهجوم رفض الخدمة ، هناك حاجة إلى خطة استجابة جيدة للحوادث ، بما في ذلك تفاصيل حول كيفية الاتصال بالشخص الفني لمزود (موفر) خدمة الإنترنت الخاص بك. لا يمكن تصفية هجمات الحرمان من الخدمة ، وخاصة هجمات الإغراق ، إلا في الاتصالات الداخلة للشبكة. يجب أن تحتوي الخطة أيضًا على تفاصيل حول كيفية الرد على الهجوم. سيعتمد تقسيم المسؤوليات بين الموظفين التنظيميين ومزود خدمة الإنترنت على الموارد المتاحة والقدرات الفنية للمنظمة.
- داخل المؤسسة ، يجب أن تكون قد نفذت مصفيات قياسية لمكافحة الانتحال وتحديد المعدل التي ناقشناها سابقًا. من الناحية المثالية ، يجب أن يكون لديك أيضًا شكل من أشكال مراقبة الشبكة الآلية ونظام كشف التسلل (IDS) قيد التشغيل ، حيث سيتم إخطار المستخدمين في حالة اكتشاف حركة مرور غير طبيعية.
- عند اكتشاف هجوم الحرمان من الخدمة ، فإن الخطوة الأولى هي تحديد نوع الهجوم ومن ثم أفضل طريقة للدفاع ضده. عادةً ما يتضمن ذلك التقاط الحزم المتدفقة إلى المؤسسة ، وتحليلها بحثًا عن أنواع حزم الهجوم الشائعة. قد يتم ذلك من قبل موظفي المؤسسة أو مزود خدمة الإنترنت ، اعتمادًا على الخبرة ذات الصلة. من هذا التحليل يتم تحديد نوع الهجوم ، والمصفيات المناسبة المصممة لمنع تدفق حزم الهجوم. هذه يجب أن يتم تثبيتها من قبل مزود خدمة الانترنت على أجهزة التوجيه الخاصة بهم. إذا كان الهجوم يستهدف خطأً في نظام أو تطبيق، بدلاً من حجم حركة المرور ضخمة ، فيجب تحديد ذلك واتخاذ الخطوات لتصحيحه لمنع الهجمات المستقبلية.

4- مكافحة هجمات الحرمان من الخدمة (DoS): الاستجابة للهجوم

- قد ترغب المؤسسة في مطالبة مزود خدمة الإنترنت بتتبع تدفق الحزم مرة أخرى في محاولة لتحديد مصدرها. ولكن ، إذا تم استخدام عناوين مصدر مزورة فقد يكون ذلك صعبًا ويستغرق وقتًا طويلاً. قد تعتمد محاولة القيام بذلك على ما إذا كانت المؤسسة تنوي إبلاغ وكالات إنفاذ القانون ذات الصلة بالهجوم. في مثل هذه الحالة ، يجب جمع أدلة إضافية وتوثيق الإجراءات لدعم أي إجراء قانوني لاحق.
- في حالة هجوم موسع ومنسق ، فقد لا يكون من الممكن تصفية ما يكفي من حزم الهجوم بنجاح لاستعادة اتصال الشبكة. في مثل هذه الحالات ، تحتاج المؤسسة إلى استراتيجية طوارئ للتبديل إلى خوادم النسخ الاحتياطي البديلة ، أو لتكليف خوادم جديدة بسرعة في موقع جديد بعناوين جديدة ، من أجل استعادة الخدمة. بدون التخطيط المسبق لتحقيق ذلك ، ستكون نتيجة هذا الهجوم هي فقدان اتصال الشبكة الواسع.
- بعد الاستجابة الفورية ، قد تحدد سياسة الاستجابة للحوادث في المؤسسة خطوات أخرى يتم اتخاذها للاستجابة للحالات طارئة.

5 - هجوم قطرة الدمع (Teardrop Attack)

احد أنواع هجمات (DoS) هجوم قطرة الدمع (Teardrop Attack) الذى يعتمد على المعلومات الواردة في مقدمة حزمة الرسائل في إعادة ترتيب الرسالة.

فعندما يتسلم الموجه حزمة رسائل اكبر مما ينبغي، فإنه يقوم بتجزئتها قبل تمريرها، وفي هذه الحالة يستخدم الموجه حقلين من حقول مقدمة الرسالة (IP Header) هما "مؤشر التجزئة" (Fragmentation offset field) وحقل "طول الرسالة" (Length Field) لتمكين النظام المتلقي للرسالة من إعادة ترتيب اجزئها بالشكل الصحيح. وعندما يستقبل النظام المتلقي حقل مؤشر التجزئة وقيمته (0) فإنه يفترض ان هذا هو الجزء الأول من الحزمة، او ان هذه الحزمة لم تتعرض للتجزئة.

عند حدوث التجزئة، يستخدم النظام المتلقي مثل "مؤشر التجزئة" لتحديد مكان هذا الجزء من الرسالة (بعده عن بدايتها)، ويستخدم حقل "طول الرسالة" كنوع من التأكيد للتأكد من انه لا يوجد خطأ في حساب حقل "مؤشر التجزئة" وانه لم تحدث أخطاء خلال نقل الرسالة، فمثلا اذا تم نقل الجزء الأول من الرسالة ووضعه في مكانه المخصص وتم نقل الجزء الثالث ووضعه في مكانه المخصص، ثم اتى الدور على الجزء الثاني من الرسالة ووجد النظام المتلقي ان محتويات حقل "طول الرسالة" تشير الي ان الجزء الثاني أطول مما كان مقدرا له و انه سيمتد ليغطي جزءا من محتويات الحقل الثالث، فلابد وان خطا ما قد حدث. عندئذ سيحاول النظام إعادة ترتيب أجزاء الرسالة من جديد، فاذا لم يتمكن فانه سوف يرسل في طلب إعادة ارسال أجزاء الرسالة من جديد.

والان كيف يتم هجوم "قطرة الدمع"؟، يقوم المهاجم بإرسال حزمة بيانات عادية بحيث يحتوى حقل مؤشر التجزئة على قيمة (0) وهذا امر طبيعي، ولكنه يتلاعب في بيانات حقلي "مؤشر التجزئة" و "طول الرسالة" في الحزم التالية من الرسالة، وعندما يصل الجزء الثاني من الرسالة (الحزمة الثانية) يقوم النظام المتلقي بمراجعة حقل "مؤشر التجزئة" لمعرفة المكان الذى يضع فيه هذا الجزء من الرسالة، فيكتشف ان هذا الحقل يشير الى ان هذا الجزء يبدأ قبل انتهاء الجزء الأول، وعندما يراجع النظام الحقل الاخر (حقل "طول الرسالة") يكتشف ان طول هذا الجزء اقل من ان يمتد بعد نهاية الجزء الأول، أي ان الجزء الثاني سيكون متضمنا بالكامل في الجزء الأول. وهذا الخطأ ليس في الحسبان، فالنظام اذا اكتشف ان الجزء الثاني من الرسالة يمتد بعد الجزء الأول (Overlap) فإنه قد يطلب إعادة الارسال، ولكن في هذه الحالة فان هذا النوع من الخطأ لا يوجد له برنامج للتعامل معه (Handling Routine) ومن ثم – في كثير من الأحيان – يتوقف النظام المتلقي عن العمل.