

ةيساسأل تابلطتمال

تابلطتمال

دنتسمال اذهل ةصاخ تابلطتم دجوت ال

ةمدختسمال تانوكمال

ةني عم ةي دام تانوكم وجمارب تارادصا يلع دنتسمال اذه رصتقي ال

تاحالطصال

تاحيملت تاحالطصا يلع عجرا ، تادنتسمال تاحالطصا لوح تامولعمل نم ديزم يلع لوصحلل
[ةينقتل Cisco](#).

اعويش (DoS) ةمدخلال ضفر تامجه رثكأ

يتل تامجهال لهاجتب تمق اذا يتح .ةلمتحمال ةمدخلال ضفر تامجه نم ةعساو ةعومجم كانه
ةلبلق رورم ةكرح يلع يتحت يتل ةمظنال ليعشت فاقيل جماربال اعطخأ مدختست
اهمدختسإ نكمي ةكبشال ربع اهلاسرا نكمي IP ةمزح يا نأ يه ةقويقحلال لظت ،اي بسن
امئاد ركفت نأ بجي ،موجه تحت نوكت ام دنع .ضي في يذال (DoS) ةمدخلال ضفر موجه ذي فننتل
ةداتعمل تافينصتلا نمض جردني ال عيش وه هارت ام نأ ةينام ي

ةريثك تامجه نا ركذتن نا اضيا ديحل نم ف ،رابتعال نيعب ريذحتلا اذه انذخا اذا نكلو
ريغ اه نأل وأ ،صاخ لكشب ةلاعف اه نأل ةعئاشلال تاقحالمال نومجهامال راتخي و .ةهباشتم
نابلط ةكرح" ييجمجهام نم ديدعل رقتفي و .ةحاتم تاودال نأل وأ ،صاخ لكشب بقعتلل ةلباق
يلع ةدوجومال جماربال ممدختساو ،ةصاخال مهتاودا عاشنال زفاحال وأ ةراهمال يلع "ناتسكاب
اهنم جورخال وأ ةضومال يلع لوحتلا يلع تاودال هذه ليمت و .تنرتنل

يلع لوصحلل ةالمعل تابلط مطعم تناك ، 1999 زومت/ويروي في ،لاقمال اذه ةباتك تقوي في
لسري . "سكاع" و "يئاهن فده" :ناتحض موجهال اذه . "smurf" موجه نمضتت Cisco ةدعاسم
ةكبش سكاعال نم ثبال ناو نع يلع ("pings") بلط يدص ICMP نم هي بنت قفدت مجهامال
ةمزح لك .يئاهنال فدهال ناو نع نوكتل مزحلل هذهل ردصمال نيوانع ريوزت متي .ةيعرف
ةيعرفال ةكبشال يلع ةفيضمال تائيبلال نم ديدعل بيحتسي ،مجهامال نم ةلسرم
اياحضال نم لكل يددرتلا قاطنل رادهو يئاهنال فدهال قارغل يلع كل ذي و .سكاعلل

هنكلو ،ةقيرطال سفنب ةهجومال ثبال تايلمع ، "قبيضتلا" يسمي ،لثامم موجه مدختسي و
تنرتنل يلع مكحتل لئاسر لوكوتورب يدص تابلط نم ال دب UDP يدص تابلط مدختسي
ةيبعش لقا هنا امك ،روفنس نم لقا ميحضت لماع لالتخال اذه ققحي ام ةداعو . (ICMP)
ريثكب

فصو دجوي .دئاز لكشب القثم حبصي ةكبشال طابترال نأل smurf تامجه ةطحال م ةداع متي
[ةمدخلال ضفر تامجه تامولعم ةحفض](#) في ،ةيعافدل ريبادتلل و ،تامجهال هذهل لماك

متي . TCP لاصتلا تابلط هب فده زاهج قفدت متي شيح ، SYN نافوط وه رخآ عئاش موجه كانه
رابجل وه ضرغل .ايئاشع لاصتال بلط مزحل ردصمال TCP ذفانم و ردصمال نيوانع ميسقت

متي ال يتل تالاصتالال نم ديدعلل ةلحال تامولعم ىلع ظافحلال ىلع فدهال فيضمال
ادبأ اهلامك

(SMTP مداخ أو HTTP نوكي ام ابلاغ) فدهال فيضمال نأل SYN ناضيف تامجه ةظحالمة دعام متي
نم عجرت يتل رورملا ةكرحل اضيا نكمملا نم . لطعتي وأ لبطعتي وأ ةياغلل ائيطب نوكي
رورملا ةكرح نأل عجري اذهو . تاهجوملا ىلع ةلكشم ثودح ي ف ببستت نأ فدهال فيضمال
ىل رقتفت يهو ، ةيلصلال مزحلل ةيئاوشعلا ردمال نيوانع ىل بهذت هذه ةدئاعلا
تاهجوم ي ف . راسملا نزاخم زواجتت نأ نكمي و ، "ةيقيقحلا" IP رورم ةكرحلا ةيلحمال صئاصخلال
هنم ةركاذل تدفن يذل هجوملا ي ف اهسفن ةلكشملا هذه رهظت ام ابلاغ ، Cisco

(DoS) ةمدخلال صفر تامجه نم يمظعلا ةيبلغال اعلم SYN و Smurf تاناضيف تامجه لكشت
فرعتل نكمي . ةيمهالال غلاب ارمأ دعيا ةعرب اهيلع فرعتل نأ امك ، اهب Cisco غابال مت يتل
رابتل تاناضيف لثم ، "ةينائلال ةقبطال" تامجه ضعب كلذل (و نيوموهالال كىل ةلوهسب
Cisco نم لوصلال مئاوق مادختسا دنع (لاصتالال

(DoS) ةمدخلال صفر فصولا ةمئاق

دوزم وأ ةكرش ي ف ةيلخاد LAN ةكبشب Ethernet 0 لصتي . نيتهجاو مادختساب هجوم ةروص
متي . ليحتلل ISP ربع تنرتنل لاصتال Serial 0 رفوي . ريغصلا (ISP) تنرتنال ةمدخ
امك ، طابترالال لمكالل ي ددرتال قاطنلال ىلع 0 لسلستل ي ف لاخبالا ةمزح لدعم "تېبثت"
وأ قيلعت وأ لطف وأ عطب لمعلا ةيلحمالا ةكبشلال ىلع ةدوجوملا ةفيضملا ةزهجالا موقت
هب لصتي يذل ريغصلا عقوملا يوتحي ال . (DoS) ةمدخلال صفر موجهل ىلأ تامالع راهظا
ةمودعم وأ ةليلق ةربخم هيدل كانه نيديوملا صاخشال نأ امك ، ةكبشلال ىل هجوملا
ةرفوتم عبتتال تنال اذا يتح للحم راثأ ةءارق ي ف

جارخال اذه حضوي امك لوصلال ةمئاق قيبطتب تمق كنأ ضررتفا ، نألا

```
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any
```

```
interface serial 0
ip access-group 169 in
```

عمو . اهب حومسم تالخال عيمج ، قاطنالال ىلع رورم ةكرح ي ةيفصتب ةمئاقلا هذه موقت ال
عاونا عيمج صيخشتل ةمئاقلا مادختسا نكمي ، ةديفم قرطب مزحلل فنصت اهنال ارظن ، كلذل
بعلالالو ، SYN لويسو ، smurf : يضا رتفا لكشب ةثالثل تامجهال

Smurf ل يئاهنلا فدهال

اذهل ةلثامم تاجرخم ةيؤر كنكمي ي ف ، show access-list رمال رادصاب تمق اذا

للدعم الذي دعتو مداخل دودج تازيم مداخلتساب ثبلا رفوم موقوي نأيه يرخأة فينالكم | ICMP. قاطنلا ضرع يلعل لوقوعم دويق كرت نكمي. يدص دودرل حاتملا يدرتلا قاطنلا ديقتل عبنملا تامدخ مدقم تادعم يلعل نيجهنلا الك دمتعي. يمسم ريغ لجأله انالكم في يدرتلا. حاتم ريغ وردقلا هذه نوكت نايلحأال ضع ب فيفو، مزاللا وردقلا اهيدل يتل

يروفنس كاع

ناك اذا، رخأا ينعمب) دادترالا دودر نم الدب echo تابلط نم فلأتت دراولا رورملا كرح تنك اذا نكمي امم رثكأ تاقباطتلا نم ديدعل بسحي، فيناثلا نم الدب، يلاوأل لوصولا عمئاق لاخدا، سكاك كعبشلا مداخلتسا هي في متي smurf موجه شودح في كشت دقف، (لوقوعم لكشب هعقوت متنأف، موجهلا تحجن اذا، نيتهلحأال اتلك في. اطي سب لاصتالا رابتهلخا ناضي في نوكي امبر وأ ببسب، عقاولا في. مداقلا بناجلا كلكذكو، يلسلسلتلا طخال نم جراخال بناجلا قرغ نوعقوتت مداقلا بناجلا نم رثكأ المحم جراخال بناجلا نوكي نأعقوتت كنإف، ميخضتلا لماع

طيسبلا "جنيب" ضيفو "روفنسلالا" موجه نيبي زييتمتلل قرطه دعه كانه

- نيح في، يدالحأال ثبلا ناووع نم الدب، هجوم ثب ناووع يلا Smurf هي بنت مزح لاسرا متي فيور كنكمي. فيدالحأال لحاوسلا ابيرقت امئاد فيداعلا ping تاناضي في مدختست لوصولا عمئاق لاخدا في لجسلا لاخدا فيساسأالا عملكلا مدختست يتلل نيوانعلا بسانملا

- في جراخال ثب تاي لمع نم بسانتم ريغ دعه كانه في، Smurf سكاك مدختست تنك اذا نم بسانتم ريغ ادعه نوكي ام دواعو، ماظنلا في تثرثيالا بناجلا يلعل show هجاوولا ضرع لاصتالا رابتهلخا ضيف فيزي ال IP. رورم كرح ضرع عشاش في لاسرمل ثبلا تاي لمع فيفلخال في ثبلا تاناي ب رورم كرح فيساي قلا

- نم تثرثيالا يلا ردصي رورم كرح ريثك كانه، smurf سكاك تلمعتسا تنأ نوكي نا لاخدا مزح نم تاجرخلما مزح نم ديزملا كانه، ماع لكشب. تثرثيالا نم مداق رورم كرح، لمالك لكشب لاخدا هجاوب زي فحتلا قفدت ألتما اذا يتح. فيلسلسلتلا هجاوولا يلعل طاقسا تاي لمع باسح متي و، زي فحتلا قفدت نم ربكأ نوكي فباجتسالا قفدت نإف مزحلا

فاقي سكاكال راتخا اذا Smurf موجهل فيئاهنلا فدهلا نم رثكأ تاراخي يلعل Smurf سكاك يوتحي نم كلذ لداعي ام وأ) ثبلا هي جوت مدعل بسانملا مداخلتسالا داعي فيكي، موجهلا ليغشت طشن موجه كانه نكي مل اذا يتح، نيوكت لك يلا رماوأل هذه فيمتنت. (IOS فالخب رماوأل [نامألا نيسحت](#) يلا عجرا، smurf موجه في Cisco هجا مداخلتسا عنم لوح تامولعمل نم ديزملا لوح تامولعملو، ماع لكشب smurf تامجه لوح عماعلا تامولعمل نم ديزملا. [Cisco تاهجوم يلعل](#) [عمدخال صفر تامجه تامولعمل قح فص](#) يلا عجرا، Cisco كرشل عمباتلا ريغ تادعملل فيم

عضو في وه فيلاتلابو، فيئاهنلا فدهلا نم رثكأ مجاهملا نم برقأه عوطخ وه روفنس سكاكال نا عم ديزملا عم لمعلا يلا عجاب كنإف، موجهلا بقعت تثرثأا اذا. موجهلا عبتتل لصفأا لمعلا عجاب كنإف، عبتتلا لامكإ دنع عارجا يا ذاختا في بغرت تنك اذا. نيي نعمل تثرثيالا موقت ناب صوي، ام موجه عبتتل عست تنك اذا. بسانملا نوناقلا صرف تالكوعم لوح فينف تامولعمل يلعل لوصولل [عبتتل](#) مسق عجار. نكمم تقو برقأا في نوناقلا صرفب تاناضي فل تامجه بقعت

زي فحتل قفدتل مدختست UDP يدص تابلطنأ انثتساب smurf، موجه لذاختل موجه لثام ي تامجهل لوصول عمئاق نم عبارل او ثلثل لاطخل ددحي ICMP يدص تابلطنم الدب عم دح وه UDP يدص نأ انثتساب، اهسفن يه اياحضلل عبسانملا عباختسالا. ةكل اهتمل جئاتن عم امامت اهليطعت كنكمي، كذلذ ICMP يدص نم تاكبشلا مطعم يف ةيمهأ لقأ لقأ ةيبلس.

تاناضي فالو زليس

يه لوصول عمئاق نم سداسل او سماخل رطسأل

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
```

وه اقح اذه هينعي ام، انضارغأل ACK تب ةعومجم عم TCP ةمزي ي عم طوطخل هذه لوأ قباطتي TCP SYNs نوكت يتل مزحل يثالثل رطسأل قباطي و TCP ماظن تسيل ةمزي ي قباطت اهنا. هذه عمئاقل لاطخل يف ةدوجومل تاداعل نم SYN قفدت يلع ةلوهسب فرعتل نكمي. طقف ةداعو، لقأل يلع نينثا لماعم ب SYN ددع SYN ريغ TCP مزح زواجتت، ةيداعل رورملا ةكرح يف تارم ةدع SYN ريغ TCP مزح ددع ةداع SYNs قوفي، SYN نافوط يف. ةسمخ وأ ةعبرأ نم رثكأ

تابلطل لئاهل دئازل لمحلل وه عيقوتل اذه عاشن اب موق ي ذللا موجهل ريغ ديجولل طرشلل لمشي نلو، عقوتم ريغ لكشب دئازل لمحتل اذه يتأي نل، ماع لكشبو. ةيلصلال لاصتال يلع يوتحت ام ابلاغ SYN تاناضي ف نأ امك. يقيقحل SYN ناضي ف لثم SYN مزح نم ديدعل نم، لجسل لاطخل ةيساسأل ةمكلل مادختساب؛ امامت ةححص ريغ ردصم نينوانع تاذ مزح نينوانعل هذه نم يتأت لاصتال تابلطل تناك اذا ام ةفرعم نكمملا

موجه يف. ماظنل ناضي فب هبشلا ضعب لمحي يذلا "تايلمعل لودج موجه" يمس ي موجه كانه ديزم نود ةينمزللا ةلمل اهتتاب اهلمسي مثنمو، TCP تالاصتال لامكإ متي، ةيلمعل لودج ةيلوال لاصتال تابلطل لاسرا متي، SYN قفدت يف امن ي ب، لوكتوربلا رورم ةكرح نم هقلاطإ بجي ف، ةيلوال TCP ةحفاصم لامكإ بلطتي ةيلمعل لودج موجه نأل ارظن. طقف ةداع) هيلل لوصول مجاهم لل نكمي يقيقح زاهج صاخلا IP ناونع مادختساب ماع لكشب SYN تاناضي ف نم ةلوهسب ةيلمعل لودج تامجه زييمت نكمي كذلذ. (قورسمل لوصول ناونع نم ةيلمعل لودج موجه يف ةدوجومل SYN رصانع عيمج يتأت. مزحل ليحست مادختساب. ةيعرف تاكبش ةدع وأ ةيعرف ةكبش نم رثكأل يلع وأ، نينوانع ةدع وأ دحاو

يذلا ماظنل او. ةيغلل ةدودجم ةيناجرمل باعشل تاناضي ف اياحضل ةباختسالا تاراخي مجاهملا هديري ام ماظنل لوصول عمئاق ققحي ام ةداعو، ةمهه ةمدخ ةداع وه موجهل لضرعتي تازيم يلع Cisco، تاجت نم كذلذ يف امب، ةيامحل رادجو تاهجومل تاجت نم نم ديدعل يوتحت يلع دمتعت تازيملا هذه ةيلاعف نكلو. SYN تاناضي ف ريثأت نم دحلل اهمادختسإ نكمي Cisco لال قيثوتل، ةعومجم ةيامح رادج Cisco ios لال قيثوتل، ةمولعم ريثك ل تلحأ. ةيئيبلا. [ديدخت جاحسم Cisco يلع نامأل نيسحتو](#)، ةمس ضارعتا ios TCP

ي مدقم نم لك ةدعاسم بلطتت بقعتل ةيلمع نكلو، ةكبشلا تاناضي ف عبتت نكمملا نمو نم نافوط بقعت ةلواجم تررق اذا. ةيحضلا يل مجاهملا نم قيرطال لوط يلع تنرتنل تامدخ عبنملا ةمدخ رقوم عم لمعاو، ركبم تقوي ف نوناقلا ذافن تاطلسب لصاتا، SYN ماظن عبتتلا لوح ليصافت يلع لوصول دنسمل اذه يف [عبتتلا](#) مسق عجار. كب صاخلا

يرخأ تامجه

نيوانع مادختساب موجهلا ك لذ فصو ىلع ارداق تنك اذإو، موجهل ضرعتت كنأ دقتعت تنك اذإ لوصولا مئاق مادختساب كنكمي ف، ذفانملا ماقراو تالوكوتوربلا ماقراو ةهوجلواو IP ردصم، اهيف هبتشملا رورملا ةكرح قباطت لوصولو ةمئاق لاخدا عاشناب مق. كتيضرف رابخال رورملا ةكرح لجس وأ ةقباطملا تاداع بقارامو، ةبسانم ةهجاو ىلع اهتقبطو

لجستلاو دادعل تاريذحت

اذإ. لاخدا اذله لباقم تاقباطتلا عيجم باسحب لوصولو ةمئاق لاخدا ىلع دوجوملا دادعل موقوي. ةيعيجمت دادعأ يه اهارت يتلا ماقراو انا ف، نيتهجاو ىلع لوصولو ةمئاق قيبطتت تمق

ببنتل لدعمل دوجم لجستلا. لاخدا قباطت ةمزح لك لوصولو ةمئاق لجستت ضرعي ال نكلو، ةلوقعم ةيوليثمت ةنيع وه لجستتلا هرهظي ام. ةيزكرملا ةجلالعمل ةدحول دئازلا لمحلا اهارت ال مزح كانه نأ ركذت. لمك ةمزح عبتت سيل

اذإ. ةنيعم ليوحت عاضو ايف طقف لوصولو ةمئاق لجستت لمعي، جماربل تارادصا ضعب ي ف حسم لواحف، عيشي ل جسي ال هنكلو، تاقباطتلا نم ريثكللا دع لوصولو ةمئاق لاخدا ناك تمق اذإ اردح نك. ةيولمعلل اهليوحت متي نأ ىلع مزحل رابجال راسم لل تقوملا نيزختلا ةركاذ طاقس انكمي. تاهجاو لا نم ديدعل مادختساب ةدشب اهليوحت متي يتلا تاهجوملا ىلع كلذب هيوجللا ةداع مادختساب. تقوملا نيزختلا ةركاذ ةداع اناثا رورملا ةكرح نم ريثكللا. كلذ نكم امك Cisco Express Forwarding عيرسللا

تاهجوملا نم اردح نك. اريبك سيل نكلو، ةادألا ىلع ريثأت لجستتلاو لوصولو مئاقول نوكي دنع وأ، (CPU) ةيزكرملا ةجلالعمل ةدحو لمح نم ةئامل ايف 80 نع ديزت ةبسنب لمعت يتلا. ةعرسللا ةيلع تاهجاو لا ىلع لوصولو مئاق قيبطت

ءافشتسا

اهل ةقالع ال ميق ىلع ابيرقت امئاد (DoS) ةمدخلل ضفر مزحل ردصملا نيوانع نييعت متي ةقيرطلا. نيجمجاهملا ةيوه ديدحت ي ف ةديفم ريغ يهف، يلاتلابو. مهسفنأ نيجمجاهملا ب. ةكبشلا نم يفلخلل بانجال ىلع هعبتت يه موجهل ردصم ىلع فرعتلل ةقووثوملا ةديحو لا عيجم نواعت مزليو. لجسل تامولعم صحفو تاهجوملا نيوكت ةداع ىلع ةيولمعلل هذه لمتشتتو نواعتلا ك لذ ني مات بلطتيو. ةيحصلا ىل مجاهملا نم قيرطلا لوط ىلع ةكبشلا يلغشم دض ءارح ايف اذخا دي را ام اذ اضا كراشت نأ بجي يتلا، نوناقلا ذافن تالكو ةكراشم ةداع مجاهملا

ىمسي) هجوم نم ءادتا. ايبسن ةطيسب دفننتسملا دوقولا تاناضيف راثا ءافتقا ةيولمعو يذلا ("B" ىمسملا) هجوملا ءرملا ددحي، تاناضيفلا رورم ةكرح لمح يهنا ب فورعم ("A" يذلا ("C" ىمسملا) هجوملا دحيو، b ىل ك لذ دع ب دحاو لخدي. رورملا ةكرح A هنم لبقتسي. يئاهنلا ردصملا ىلع روثلعت متي يتح اذكه لاجل رمتسيو. رورملا ةكرح B هنم ملتسي

:ةمئاقلا هذه اهفصت يتلاو، ةقيرطلا هذه ي ف تاديقت ةدع كانه

• ي ف هنكلو، مجاهملا لبق نم رطخلل ضرعت ابوساح "يئاهنلا ردصملا" نوكي نأ نكمي و

سإ ودة ففحص ناضف عبتت نإف ،ةلأال هذه فف و.سأ ؤفحص هرفدو هكل مفا عقالا
سألوال ؤوطالأس سسل

- إلمهتامه نولصاؤف ام ؤءاع مهو ،مهتا ففلخ عبتت نكمفا ال هنأ نومجاهملا كرفدو
إلعلف نافوطال عبتتل فاك تقوكلالنه نوكفا ال دق .ةدودحم ؤرتفل
- نمو .إفسن اروطتم مجاهملا ناك إذا اصوصخو ،ةدءتم رءاصم نم تامهال فأت نا نكمفا و
رءاصملا نم نكمم دء ربكأ دفءء ؤلواحم مهملأ
- رءكأ وأ دحاو سدل نوكفا ال نأفأال نم رفءك فف .عبتتل ؤفلمع ؤطبت لاصءال لكاشم
بسانم لكشب نولهؤم نوظوم نففنعملا ؤكبشال فلغشم نم
- ول سء نففمجاهملا دص لمعل بعصلال نم ؤفساؤسلال ؤفنوناقال لغاوشال لءءء دقو
ءءو

(DoS) ءنءءنإل ؤمدخ فلوئسم فءهءسء فءل تامهال عبتت سل ؤفمارال ؤهال بلغأ نإ
اونوكفا مل ام موه بقءء سء ؤكبشال فلغشم نم دفءل لولأف ال ،بسال اءهل و .لشفء
فالءءأم ،"ةدفءل" تامهال أس نففنأل نم دفءل عبتءل ال امنفب .طغضال ءء
نوناقال ذافن ناك إذا ال رءأ سلل روءل فف نوءعاسف ال ضعبالف . "رفطء" وه ام ءافرفءء
الومشم

"لءسلال لءءء" ب عبتتل

فه كلذب مافلل ؤفلل ءءكأال ؤفرطال نإف ،Cisco ءوم ربع رمف موه عبتء ءءءء إذا
لءءل ؤفساأل ؤمكلال قافراو ،موهال رورم ؤكرق باطف فءل لوصول ؤمءاق لءءل ءاشن
لاسرا هلأل نم مءل فءل ؤهال سلل ؤرءاصال لوصول ؤمءاق قفبءو ،هفل لءسلال
ؤمءاق ؤطساوب اءءن مءل لءسلال ءالءءل فرءء .ففءهال هفءه وءن موهال قفءء
لاصلال نع ؤرابع ؤهال ءنالك إذا ،هلأل نم رورملا ؤكرق لصلل فءل ءوملا ؤهال لوصول
دعب نكمف .هنم هلل باقتسا مءل فءل ذلأ زاهلل 2 ؤقبطال ناونع ءاطع لكفلل ف ،طاقنل دءءم
سلل ،مءءءساب ،ؤلسلسال فف فءل ءل ءومال ففرءل 2 ؤقبطال ناونع مءءءسلكل ذ
show ip arp mac address رمال ،لاءملا لفس

ءوول ففس

اءهل ؤلءام لوصول ؤمءاق ءاشن نكنكمف ،SYN قفءء عبتتل

```
<#root>
```

```
access-list 169 permit tcp any any established  
access-list 169 permit tcp any host
```

```
victim-host
```

```
log-input  
access-list 169 permit ip any any
```

SYN ؤمظنأ كلذ فف امب ،فءل ففضملل ؤهال لSYN مزء ءفمء لفسءءب اءه موقف
لءسلال ءالءءل صءفب مق ،مجاهملا وءن اءفءء رءكأال فلعلال راسملا دفءءل .ؤفرشلل

مزحلا نم ددع ربكأ لصي هنم يذلا رخصملا وه ناضي فل رخصم ،ماع لكش ب .ليصفتلاب نيوانعو رخصم تاهجاو نع شحبت تنأ .ائيش ينعت ال اهسفن رخصملا IP نيوانع .ةقباطملا مزح نأل ةيعرشلا مزحلا نم قفدتلا مزح زيميتم نكمملا نم ،نايحلأا ضعب يف .رخصم MAC ناوانع ةمزح يأنوكت نأل لم تخملا نم .ةحلل اص ريغ رخصم نيوانع اهل نوكي نأل نكمي قفدتلا قفدتلا نم اعزج حلل اص ريغ اهب صاخلا رخصملا

إلى ةبسنلاب اي بسن يداع ريغ كلذنا عم ،ةددعتم رصاصم نم نافوطلا يتأي نا نكمي .نافيشلا تاناضي ف

روفنس هب نم

لثم لوصو ةمئاق مدختسا Smurf، تاهب نم قفدت عبتتلا

```
access-list 169 permit icmp any any echo log-input
access-list 169 permit ip any any
```

نأ اذه يف ببسلا .سكاعلا ناوانعلا ةهجوملا مزحلا إلى هسفن ديقى ال لوالا لاخدإلا نأ ظحال فدهلا عم لاصتا إلى نكت مل اذا .ةددعتم سكاع تاكبش مدختست smurf تامجه مظعم يف أدبت دق ،موجهلا رخصم نم كبقعت بارتقا عمو .سكاعلا نيوانع لك فرعت ال دق ،يئاهنلا .ةديج ةمالع هذهو ،رثكأو رثكأ تاهجو إلى بهذت دادترالا تابلط ةيؤر

ردق ديروت إلى كلذ ي دوي دق ،ICMP رورم ةكرح نم ريبك ددع عم لماعتلاب تمق اذا ،كلذ عمو تنأ ،اذه ثدح اذا .ةلوهسب ةءارقلال نم نكمتت يتح كل ليحسنتلا تامولعم نم ادج ريبك .تلمعتسا نوكي نأ فورعم نوكي نأ سكاعلا نم دحاو نوكي نأ ناوانع ةيغال تديق عيظتسي ةكبشلا ةعنقأ نأ ةقيقح نم ديفتسي لخدم مادختسا وه رخآ ديفم كي تكت كانهو .تاسكاع نيماجاهملا اهب دجي يتلا ةقيرطلا ببسبو .تنرتنإلا يف ادج ةعئاش 255.255.255.0 اذه ةقباطملا الامتحا رثكأ يه smurf تامجهل لعفلاب ةمدختسملا سكاعلا نيوانع نإف ،smurf ،كلذل .تنرتنإلا يف ادج ةعئاش ريغ 255.0 .يف يهتنت يتلا فيضملا نيوانع .عانقلا جتانلا اذه حضوي امك روفنس زفاوح تارايتل اي بسن ةدحمت فيرعت ةادأ انب كنكمي

```
access-list 169 permit icmp any host known-reflector echo log-input
access-list 169 permit icmp any 0.0.0.255 255.255.255.0 echo log-input
access-list 169 permit icmp any 0.0.0.0 255.255.255.0 echo log-input
access-list 169 permit ip any any
```

ال نيح يف ،كلجس يف "ءاضوضلا" مزح نم ديدعلا نم صلختلا كنكمي ،ةمئاقلا هذه لالخنم بترتقت يذلا تقولا يف زيفحتلا نم ةيفاضا تاقفدت ةدهاشملا ةديج ةصرف كي دل لازت مجاهملا نم هي ف

"لجسلا لاخدإ" نودب عبتتلا

Cisco IOS جم انرب نم 11.2 تارادصإلا يف لجسلا لاخدإلا لجسلا لاخدإلا ةيساسألا ةملكلا دجوت قوسل اصيصخ اهؤاشنإ مت يتلا 11.1 إلى ةدنتسملا جماربالا ضعب يفو ،ثدحألا تارادصإلاو

جمارب عم هجوم مدختست تنك اذا .ةيسيئرلا ةملكلا هذه مدقأال جم انربل معدى ال .ةمدخلال دوزم
قيبطتلل ةلباق تاراىخ ةثالث كي دلف ،ةميدق

- رورم ةكرح قباطت تالاخلدا مادختساب نكلو ،لوخدلا ليجست نود لوصو ةمئاق عاشناب مق
يف ةهجاو لكل لاخلدا بناج ىلع ةمئاقلا قيبطتب مق .اهيف هبتشملا تانايبلا
هذه زيمتت .ةيلع قباطت تالدعم تاذ تاهجاو نع ثحبا .تادادعلل بقارم ث ،لباقملا
نإ .ردصملا تاهجاو ىلع فرعتلل ةديفم اهنأ امك ،ةيغلل ةضفخنم عادأ ةميقب ةقيرطلا
اديفم نوكي يلاتلابو ،طابترالا ةقبط رصم نيوانع يطعي ال هنأ يه هل ةبقع ربكأ
ةطقن ىلإ ةطقن نم لاصتالا طوطخل بلاغل ي ف

- لباقم ي ف) لجسلا ةيساسألا ةملكلا مادختساب لوصولا ةمئاق تالاخلدا عاشناب مق
ال .اهرودب ةهجاو لكل دراوول بناجلا ىلع ةمئاقلا قيبطتب مق ،يرخأ ةرم .(لجسلا لاخلدا
ضرعل ةديفم نوكت نأ نكمي نكلو ،ردصم لل MAC نيوانع رفوت ال ةقيرطلا هذه لازت
موجه نم عزج لعفلااب وه ةمزحلا قفدت نأ نم ققحتلل ،لاثملا لىبس ىلع .IP تانايب
لكشب لمعت ثدحأال جماربلاو ،عفترم ىلإ طسوتم نم نوكي نأ نكمي عادأال ريثأت
مدقأال جماربلا نم لصفأ

- نيوانع ةقيرطلا هذه رفوت .مزحلا لوح تامولعم عمج debug ip packet detail رمألا مدختسأ
هذه عم أطخ باكترال لهسلا نم .عادأال ىلع ريثأت اهل نوكي نأ نكمي نكلو ،MAC
نم دكأتف ،ةقيرطلا هذه مدختست تنك اذا .مادختسالا لباق ريغ هجوملا لعجو ةقيرطلا
مدختسأ .لثمألا وأ يثاذلا وأ عيرسلا عضولا يف تامجهلا رورم ةكرح لوح هجوملا نأ
مق .طقف اهيل جاتحت يتلا تامولعمل ىلع اعطأال حيحصت ديقتل لوصو ةمئاق
مق نكلو ،يلحملا لجسلل تقوؤملا نزخملا ىلإ اعطأال حيحصت تامولعم ليجستب
ةدحو ىلإو Telnet لمع تاسلج ىلإ اعطأال حيحصت تامولعم ليجست ليغشت فاقيب
،ايلعف هجوملا نم برقلاب ادوجوم ام صخش نوكي يكل بيترتلاب مق ،نكمأ نإ .مكحتلا
ةرورضلا بسح ةقاطلا ريودت نكمي يتح

جاتحت تنأ .ليوحتلا ةعيرس مزحلا لوح تامولعم ضرعي ال debug ip packet رمألا نأ ركذت
وأ ةمزح كي طعي حضاو رمأ لك .ةمولعم ضبق ىلع in order to clear ip cache ل ردصي نأ
اعطأال حيحصت جارخا نم نيثنثا

ةلص تاذ تامولعم

- [Kerberos](#)
- [Cisco Systems - تادنتسمل او يثقتلا معدلا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نء مء دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إلمءءء ءوچرلاب ةصوء و تاملرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزىل ءنل اءل دن تسمل