

مادختساب عب تتل او مزحل اضيف تالاح زيمي مت Cisco تاهجوم

تايوت حمل

[عمدق مل](#)

[سيس اس أل تابل طت مل](#)

[تابل طت مل](#)

[عمدختس مل تانوك مل](#)

[تالاح الطصال](#)

[اعويش \(DoS\) عمدخال اضيفر تامجه رثكأ](#)

[\(DoS\) عمدخال اضيفر فصول لوصول عمئاق](#)

[Smurf لئاهنل فدهل](#)

[يروفنس سكاغ](#)

[لازه](#)

[تاناضيفل او زلي س](#)

[يرخأ تامجه](#)

[ليجستل او دادعل تاريذحت](#)

[افش تس](#)

["لجسل لالخال" بعب تتل](#)

[دوولف نيس](#)

[روفنس هبنم](#)

["لجسل لالخال" نودب عب تتل](#)

[قلص تاذا تامولعم](#)

عمدق مل

درلل اهمدختست يتل لولوالا ووطخال. تنرتن لال لعل عمئاش (DoS) عمدخال اضيفر تامجه ربتعت عمدخال اضيفر تامجه نم ديدعل دمعتتو. موجهل وه ام طبضلاب فرعت نأيه موجهل اذه لثم لعل لعل وأيلال يددرتل قاطنل تاذا مزحل تاناضيف لعل عمئاش لكشب عمدختس مل (DoS). مزحل ليرخالا قرركت مل تاقفدتل.

موقت ام دنع (DoS) عمدخال اضيفر موجه تاقفدت نم ديدعل يف ءدوجومل مزحل لزع نكمي ءيفصتل ميقرم اذه نل Cisco IOS® جم انرب لوصول عمئاق تالخال لباقم اهتقباطمب موقت ام دنع لو، ءفورعم ريغ تامجه فيصوتب موقت ام دنع اضيفر هنافم. تامجهل. ءيقي قحل اهرداصم لال اعوجر "لحنتن مل" عمزحل تاقفدت عب تتب

ضارغال IP ءب ساجم وءاطخال ليجست لثم Cisco هجوم تازيم مادختس ل نالخال ضعب يف نكمي نم ءريخال تارادصلال مادختساب، كلذعمو. ءيداعل ريغ وأ ءديدجل تامجهل عم ءصاخو، ءلثامم ديدحت دن ل لولوالا تازيم لوصول عمئاق ليجست و لوصول مئاقو دعت، Cisco IOS جم انرب اهعبتتو عمئاشل تامجهل.

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 اعطخ امدختست
اهم ادختس انكمي ةكبشال ربع اهالاسرا نكمي IP ةمزح يا نا يه ةقويقحلال لظت ،اي بسن
امئاد ركفت نا بجي ،موجه تحت نوكت ام دنع .ضي في يذال (DoS) ةمدخلال ضفر موجه ذي فننتل
ةداتعمل تافينصتلا نمض جردني ال عيش وه هارت ام نا ةينام ي

ةريثك تامجه نا ركذتن نا اضيا اديجال نم ف ،رابتعال ني عب ريذحتلا اذه انذخا اذا نكلو
ريغ اهنا ل وا ،صاخ لكشب ةلاعف اهنا ل ةعئاشال تاقحالمال نومجهامال راتخي و .ةهباشتم
نابلط ةكرح" ييجمجهام نم ديدعل رقتفي و .ةحاتم تاودال نا ل وا ،صاخ لكشب بقعتلل ةلباق
يلع ةدوجومال جماربال م ادختساو ،ةصاخال مهتاودا عاشنال زفاحال وا ةراهمال يلا "ناتسكاب
اهنم جورخال وا ةضومال يلا لوحتلا يلا تاودال هذه لي مت و .تنرتنالا

يلع لوصحلل ةالمعل تابلط مظعم تناك ، 1999 زومت/ويروي في ،لاقمال اذه ةباتك تقوي في
لسري . "سكاع" و "يئاهن فده" :ناتحضي موجهال اذه . "smurf" موجه نمضتت Cisco ةدعاسم
ةكبش سكاعال نم ثبال ناو نع يلا ("pings") بلط يدص ICMP نم هي بنت قفدت مجهامال
ةمزح لكل .يئاهنال فدهال ناو نع نوكتل مزحلال هذهل ردصمال نيوانع ريوزت متي .ةيعرف
ةيعرفال ةكبشال يلع ةفيضممال تائيبلال نم ديدعل بيحتسي ،مجهامال نم ةلسرم
اياحضال نم لكل يددرتلا قاطنالا راده او يئاهنال فدهال قارغ يلا كل ذي دوي و .سكاعلل

هنكلو ،ةقيرطال سفنب ةهجومال ثبال تاي لعم ، "قبيضتلا" يسمي ،لثامم موجه مدختسي و
تنرتنالا في مكحتلا لئاسر لوكوتورب يدص تابلط نم ال دب UDP يدص تابلط مدختسي
ةيبعش لقا هنا امك ،روفنس نم لقا ميحضت لماع لالخال اذه ققحي ام ةداع و .(ICMP)
ريثكب

فصو دجوي .دئاز لكشب القثم حبصي ةكبشال طابترال نا ل smurf تامجه ةظحالم ةداع متي
[ةمدخلال ضفر تامجه تامولعم ةحففص](#) في ،ةيعافدل ريبادتلالو ،تامجهال هذهل لماك

متي .TCP لاصتلا تابلط هب فده زاهج قفدت متي شيح ،SYN نافوط وه رخآ عئاش موجه كانه
رابج او ضرغلا .ايئاشوع لاصتالا بلط مزحل ردصمال TCP ذفانم و ردصمال نيوانع ميسقت

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

(SMTP مداخل أو HTTP نوكي ام ابلاغ) فدهال فيضملال نأل SYN ناضيف تامجه ةظحالم ةداع متي
نم عجرت يتل رورملا ةكرحل اضيا نكمملا نم . لقطعتي وأ لقطعتي وأ ةياغلل ائيطب نوكي
رورملا ةكرح نأل عجري اذهو . تاهجوملا ىلع ةلكشم ثودح يف ببستت نأ فدهال فيضملال
ىل رقتفت يهو ، ةيلصلال مزحلل ةيئاوشعل رصملا نيوانع ىل بهذت هذه ةدئاعلا
تاهجوم يف . راسملا نزاخم زواجتت نأ نكميو ، "ةيقيقحلال" IP رورم ةكرحل ةيلحملال صئاصخلال
هنم ةركاذل تدفن يذل هجوملا يف اهسفن ةلكشملا هذه رهظت ام ابلاغ ، Cisco

(DoS) ةمدخلال ضفر تامجه نم يمظعلال ةيبلغالال اع م SYN و Smurf تاناضيف تامجه لكشت
فرعتل نكمي . ةيمهالال غلاب ارمأ دعى ةعرب اهيلع فرعتل نأ امك ، اه Cisco غالاب مت يتل
رابتخ تاناضيف لثم ، "ةيناثلال ةقبطلال" تامجه ضعب كلذكو) ني موجهال الك ىلع ةلوهسب
Cisco نم لوصلال مئاوق مادختسا دنع (لاصتالال

(DoS) ةمدخلال ضفر فصو ىل لوصولال ةمئاق

دوزم وأ ةكرش يف ةيلخاد LAN ةكبش ب Ethernet 0 لصتي . نيتهجاو مادختساب هجوم ةروص
متي . ليمحتلل ISP ربع تنرتن ل لاصلتال Serial 0 رفوي . ريغصلال (ISP) تنرتنالال ةمدخ
امك ، طابترالال لمالكلا يدرتلال قاطنلال ىلع 0 لسلسللال يف لاخلالال ةمزح لدعم "تېبثت"
وأ قيلعت وأ لقطع وأ عطب لمعلال ةيلحملال ةكبشلال ىلع ةدوجوملا ةفيضملال ةزهجالال موقت
هب لصتي يذل ريغصلال عقوملا يوتحي ال . (DoS) ةمدخلال ضفر موجهل ىلأ تامالع راهظا
ةمودعم وأ ةليلق ةربخ مهيدل كانه ني دوجوملا صاخشالال نأ امك ، ةكبش للحم يأل ىلع هجوملا
ةرفوتم عبتتلال تنالك اذا ىتح للحم راثأ ةءارق يف

جارخالال اذه حضوي امك لوصولال ةمئاق قيبطتت 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 تالاخلالال عيمج ، قاطلالال ىلع رورم ةكرح يأل ةيفصتت ةمئاقلال هذه موقت ال
عاونا عيمج صيخشتل ةمئاقلال مادختسا نكمي ، ةديفم قرطب مزحلال فنصت اه نأل ارظن ، كلذ
بعالالالال ، SYN لويسو ، smurf : يضا رتفا لكشب ةثالثلال تامجهال

Smurf ل يئاهنلال فدهال

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


```
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.59
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.82
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.56
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.84
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.15
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.33
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
```

و 192.168.212.0/24 و 172.16.x.x و 192.168.x.x تاكبش يف ةصاخلا نيوانعلا). 172.16.132.0/24 و 192.168.45.0/24 روصملاو، روفنسلال موجه نم ادج ةمس اذه (ربتخم لل يحيضوت مسر اذه؛ تنرتنإلا يلع نوكت ةبسانملا تانايبلا دعاوق يف نيوانعلا هذه باحصأ نع تثحب اذا. روفنس سكاكال نم ناووع يف مهتدعاسم بلطو تاكبشلا هذه يلوؤسم يلع روثلعال كنكمي، "WHOIS" تنرتنإلا يلع موجهلا عم لماعتلا.

ءاقفراي احض مه ءالؤه سكاكال نأ ركذن نأ ةرركتملا ثداوحلا نم ةلحرملال هذه يف مهملال نم IP مزح يلع مهب ةصاخلا روصملا نيوانع مادختسا نيماجاهم لل ادج ردانل نم. نيماجاهم سيلاو موجه يف كلذب مايقلا مهل ةبسنلاب ليحتسملال نمو، (DoS) ةمدخلال ضفرل قفدت ي يف، امامت اروزم نوكي نأ اما هنأ ضارفتا يغبني ناضي يف ةمزح يف ناووع ي أو. ةقئاف ةعرسب متي ةيانه يف روفنسلال موجه فدهل ةيجاتنإ رثكالأل جهنملا. ام عون نم ةيحصلا ناووع نوكي نأ أو، موجهلا فاقيايإل مهتاكبش نيوكت ةدعاب مهتباطملا اما، نيسكاكالاب لاصتالا وه فاطملا زيفحتلا رايت عبتت يف مهتدعاسم بلطل.

ةدئازلا ةلومحلل ببسب نوكي ام ةداع روفنس موجهل يئاهنلا فدهللا بيصي يذلا ررضلا نأل لاصتالا ريغ ةباجتسا ي اكانه نوكي ال ام ابلاغ هنإف، تنرتنإلا نم مداقلا طبارلا يلع دق نوكي، فدهللا يف مكحتلا تحت زاهج ي ايل مزحلا هي ف لصلت يذلا تقولا يف. تاسكاكالاب لعللاب ررضلا مطعم ثدح.

دودر لك أو، ICMP ي دص دودر لك يف صي نأ عب نملال ةكبش دوزم نم بلطي نأ سايقم تقوم دحاو هعضوم يف ةيفصتلا لماع نم عونلا اذه كرتب ي صوي ال. نيعم سكاكال نم ICMP ي دص مزح يمج سيلاو، طقف دادترالا دودر ةيفصت بجي، تقوم ةيفصت لماعل يتح. مئاد لكشب

للدعم الذي دعتو مداخل دودج تازيم مداخلتساب ثبلا رفوم موقوي نأيه يرخأة نيكم ICMP. قاطنلا ضرع يلعل لوقوعم دويق كرت نكمي. يدص دودرل حاتملا يدرتلا قاطنلا ديقتل عبنملا تامدخ مدقم تادعم يلعل نيجهنلا الك دمتعي. يمسم ريغ لجال انهالكم يف يدرتلا. حاتم ريغ وردقلا هذه نوكت نايجال ضعب يفو، مزاللا وردقلا اهيدل يتلا

يروفنس كاع

ناك اذا، رخأ ينعمب) دادترالا دودر نم الدب echo تابلط نم فلأتت دراولا رورملا كرح تنك اذا نكمي امم رثكأ تاقباطتلا نم ديدعل بسحي، ةيناثلا نم الدب، يلاوأل لوصولا ةمئاق لاخدا، س كاعك ةكبشلا مداخلتسا هي متي smurf موجه شودح يف كشت دقف، (لوقوعم لكشب هعقوت متنأف، ةمجهلا تحجن اذا، نيتهلحلا اتلك يف. اطي سب لاصتالا رابتخا ناضي يف نوكي امبر وأ ببسب، عقاولا يف. مداقلا بناجلا كلكذو، يلسلسلتلا طخال نم جراخلا بناجلا قرغ نوعقوتت مداقلا بناجلا نم رثكأ المرحم جراخلا بناجلا نوكي نأعقوتت كنإف، ميخضتلا لماع

طيسبلا "جنيب" ضيفو "روفنسل" موجه نيبي زيمي تليل قرط ةدع كانه

- نيح يف، يدخال ثبلا ناووع نم الدب، هجوم ثب ناووع يلا Smurf هي بنت مزح لاسرا متي ةيؤر كنكمي. ةيدخال لحوسل ابي رقت امئاد ةيدعلا ping تاناضي ف مدختست لوصولا ةمئاق لاخدا يف لحوسل لاخدا ةيساسالا ةمكلا مدختست يتلا نيوانعلا بسانملا

- يف جراخلا ثب تاي لمع نم بسانتم ريغ ددع كانه ف، Smurf س كاعك مدختست تنك اذا نم بسانتم ريغ اددع نوكي ام ةداعو، ماظنلا يف تثرثيالا بناج يلعل show ةهجاوولا ضرع لاصتالا رابتخا ضيف ديزي ال IP. رورم ةكرح ضرع ةشاش يف ةلسرمل ثبلا تاي لمع ةيفللخا يف ثبلا تانايب رورم ةكرح يساي قلا

- نم تثرثيالا يلا ردصي رورم ةكرح ريثك كانه، smurf س كاعك تلمعتسا تنأ نوكي نا لاخدا مزح نم تاجرحملا مزح نم ديزملا كانه، ماع لكشب. تثرثيالا نم مداق رورم ةكرح، لمالك لكشب لاخدا ةهجاوب زيفحتلا قفدت ألتما اذا يتح. ةيسلسلتلا ةهجاوولا يلعل طاقسا تاي لمع باسح متيو، زيفحتلا قفدت نم ربكأ نوكي ةباجتسالا قفدت نإف مزحلا

فاقي س كاعلا راتخا اذا Smurf موجهل يئاهنلا فدهلا نم رثكأ تاراخي يلعل Smurf س كاع يوتحي نم كلذ لداعي ام وأ) ثبلا هي جوت مدعل بسانملا مداخلتسالا ةداعي فكيفي، موجهلا ليغشت طشن موجه كانه نكي مل اذا يتح، نيوكت لك يلا رماوأل هذه يمتنت. (IOS فالخب رماوأل [نامألا نيسحت](#) يلا عجرا، smurf موجه يف Cisco ةزهجأ مداخلتسا عنم لوح تامولعمل نم ديزم لوح تامولعملو، ماع لكشب smurf تامجه لوح ةماعلا تامولعمل نم ديزم. [Cisco تاهجوم يلعل](#) [ةمدخل اضفرتامجه تامولعمل ةحفض](#) يلا عجرا، Cisco ةكرشل ةعباتلا ريغ تادعمل ةيماح

عضو يف وهف يلاتلابو، يئاهنلا فدهلا نم رثكأ مجاهملا نم برقا ةوطخ وه روفنس س كاع نا ةمدخ يدوزم عم لمعلا يلا ةجاحب كنإف، موجهلا بقعت تثرثا اذا. موجهلا عبتت للصفأ لمعلا ةجاحب كنإف، عبتتلا لامك دنع عارجا يا ذاختا يف بغرت تنك اذا. نيي نعمل تثرثيالا موقت ناب يصوي، ام موجه عبتتلا يعست تنك اذا. ةبسانملا نوناقلا صرف تالكوعم لوح ةينف تامولعمل يلعل لوصول [عبتتلا](#) مسق عجار. نكمم تقو برقا يف نوناقلا صرفب تاناضي فل تامجه بقعت

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

تاناضي فالو زليس

يه لوصول عمئاق نم سداسل او سماخل رطسالا

```
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 لوا قباطتي TCP SYNs نوكت يتل مزحل يثالث رطسالا قباطي و. TCP ماظن تسيل ةمزي ي قباطت اهنا. هذه عمئاقلا تالخد ي ةدوجوملا تاداعل نم SYN قفدت يلع ةلوهسب فرعتل نكمي. طقف ةداعو، لقالا يلع نينثا لماعم ب SYN ددع SYN ريغ TCP مزج زواجتت، ةيداعل رورملا ةكرح يف تارم ةدع SYN ريغ TCP مزج ددع ةداع SYNs قوفي، SYN نافوط يف. ةسمخ وأ ةعبرأ نم رثكأ

تابطل 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. ةيلصالا لاصتالا يلع يوتحت ام ابلاغ SYN تاناضي ف نأ امك. يقيقحل SYN ناضي ف لثم SYN مزج نم ديدعل نم، لجسلا لخد ةيساسالا ةملا ل مادختساب؛ امامت ةححص ريغ ردصم نينوانع تاذ مزج نينوانعل هذه نم يتأت لاصتالا تابطل تناك اذا ام ةفرعم نكمملا

موجه يف. ماظنل ناضي فب هبشلا ضعب لمحي ي ذللا "تاي لمعل لودج موجه" يمسي موجه كانه ديزم نود ةينمزللا ةلهملا اهتتاب اهل حمسي مئ نم و، TCP تالاصتالا لامكلا متي، ةيلمعل لودج ةيلوالا لاصتالا تابطل لاسرا متي، SYN قفدت يف امنيب، لوكوتوربل رورم ةكرح نم هقالطاب جي ف، ةيلوالا TCP ةحفاصم لامكلا بلطتي ةيلمعل لودج موجه نأل ارظن. طقف ةداع) هيلل لوصولل مجاهملا 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 ةدوجوملا SYN رصانع عيمج يتأت. مزحل ليجست مادختساب. ةيعرف تاكبش ةدع وأ ةيعرف ةكبش نم رثكالا يلع وأ، نينوانع ةدع وأ دحاو

ي ذللا ماظنل او. ةيغلل ةدودجم ةيناجرملل باعشلل 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، ةيامل رادجو تاهجوملا تاجت نم نم ديدعل يوتحت يلع دمتعت تازيملا هذه ةيلعاف نكلو. SYN تاناضي ف ريثأت نم دحلل اهمادختسا نكمي Cisco لال قيثوتل، ةعومجم ةيامل رادج Cisco ios لال قيثوتل، ةمولعم ريثكلا ل تلحأ. ةئيبلل. [ديدخت جاحسم Cisco يلع نامالا نيسحتو](#)، ةمس ضارعتا ios TCP

ي مدقم نم لك ةدعاسم بلطتت بقعتل ةيلمعل نكلو، ةكبشلا تاناضي ف عبتت نكمملا نمو نم نافوط بقعت ةلواجم تررق اذا. ةيحضلا ل مجاهملا نم قيرطلا لوط يلع تنرتنالا 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

ىرخأ تامجه

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

لجستلاو دادعلا تاريذحت

اذإ. لاخدا اذو لباقم تاقباطتلا عيمج باسحب لوصولو ةمئاق لاخدا ىلع دوجوملا دادعلا موقى. ةيعيمجت دادعأ يه اهارت يتلا ماقراو انا، نيتهجاو ىلع لوصولو ةمئاق قيبطتت تمق

ببنتل لدعلا دودحم 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 عاضوا يف طقف لوصولو ةمئاق لجستت لمعي، جماربل تارادصا ضعب يف حسم لواحف، عيشي لاجسي ال هنكلو، تاقباطتلا نم ريثكللا دعى لوصولو ةمئاق لاخدا ناك تمق اذإ اردح نك. ةيولمعلل اهليوحت متي نأ ىلع مزحل رابجل راسم لل تقوملا نيذختلا ةركاذ طاقس انكمي. تاهجاو لا نم ديدعلا مادختساب ةدشب اهليوحت متي يتلا تاهجوملا ىلع كلذب هيوجللا ةداع مادختساب. تقوملا نيذختلا ةركاذ ةداع اناثا رورملا ةكرح نم ريثكللا. كلذ نكمأ 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 يف 80 نع ديزت ةبسنب لمعت يتلا. ةعسرلا 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 يف ةديفم ريغ يهف، يلاتلابو. مهسفنأ نيجمجاهملا ب. ةكبشلا نم يف لخلل بنجال ىلع هعبتت يه موجهلا ردصم ىلع فرعتلل ةقووثوملا ةديحو لا عيمج نواعت مزليو. لجال تامولعم صرغو تاهجوملا نيوكت ةداع ىلع ةيولمعلل هذه لمشتتو نواعتلا ك لذ نيئات بلطتيو. ةيحصلا ىل مجاهملا نم قيرطلا لوط ىلع ةكبشلا يلغشم دض ءارجا يذاختا دي را ام اذيا اضيا كراشت نأ بجي يتلا، نوناقلا ذافنا تالكو ةكراشم ةداع مجاهملا

ىمسي) هجوم نم ءادتا. اي بسن ةطيسب دفننتسملا دوقولا تاناضيف راثا ءافتقا ةيولمعو يذلا ("B" ىمسملا) هجوملا عرمل ددحي، تاناضيفلا رورم ةكرح لمح يهنا ب فورعم ("A" يذلا ("C" ىمسملا) هجوملا دحيو، b ىل ك لذ دعب دحاو لخد ي. رورملا ةكرح A هنم لبقتسي. يئاهنلا ردصملا ىلع روثلعل متي ىتح اذكه لاجل رمتسيو. رورملا ةكرح B هنم ملتسي.

:ةمئاقلا هذه اهفصت يتلاو، ةقيرطلا هذه يف تاديقت ةدع كانه

- يف هنكلو، مجاهملا لبقي نم رطخلل ضرعت ابوساح "يئاهنلا ردصملا" نوكي نأ نكمي و

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 ةيعرشلل مزحلا نم قفدتلا مزح زيميتم نكمملا نم ،نايحلأا ضعب يف .رخصم MAC ناوانع ةمزح يأ نوكت نأ لم تحملا نم .ةحلل اص ريغ رخصم نيوانع اهل نوكي نأ 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 ناوانعل ةهجوملا مزحلا إلى هسفن ديقي ال لوالا لاخدإلا نأ ظحال فدهلا عم لاصتا إلى نكت مل اذا .ةددعتم سكاع تاكبش مدختست smurf تامجه مطعم 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 دؤي 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 ةقيرطال 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 ةدحم 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 ديدعلال نم صلختلا كنكمي ،ةمئاقلا هذه لالخنم بترتقت يذلا تقولا يف زيفحتلا نم ةيفاضا تاقفدت ةدهاشمل 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 معددي ال .ةمدخلال دوزم
قيبطتلل ةلباق تاراخي ةثالث كي دلف ،ةميدق

- رورم ةكرح قباطت تالاخلإ مادختساب نكلو ،لوخدلا ليجست نود لوصو ةمئاق عاشنإب مق
يف ةهجاو لكل لاخلإال بناج ىلع ةمئاقلا قيبطتب مق .اهيف هبتشملا تانايبلا
هذه زيمتت .ةيلاع 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 ردصم 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 تالاخلإ عاشنإب مق
ال .اهرودب ةهجاو لكل دراوول بناجلا ىلع ةمئاقلا قيبطتب مق ،يرخأ ةرم .(لجسلا لاخلإ
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 ليبس 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 ريظخ ريثأت اهل نوكي نأ نكمي نكلو ،MAC
نم دكأتف ،ةقيرطلا هذه مدختست تنك اذا .مادختسالل لباق ريغ هجوملا لعجو ةقيرطلا
مدختسأ .لثمألا وأ يثاذلا وأ عيرسلا عضولا يف تامجهلا رورم ةكرح لوح هجوملا نأ
مق .طقف اهيلإ جاتحت يتلا تامولعمل ىلع اعطأال حيحصت ديقتل لوصو ةمئاق
مق نكلو ،يلحملا لجسلل تقوؤملا نزخمل 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 - تادنتس مل او ي نقتلا معدلا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة 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 دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل