

نوع ربع عمل اعي قوت ال ميريقت : snort 3 مهف BYTE_JUMP الالاح

تايوت حمل

[قم دقمل](#)

[قيساس ا تامول عم](#)

[دي دجل ا ام](#)

[قم و عد مل ا قيساس ال ا قم ظن ال](#)

[قيساس ال ا قم ج ال او ج مار بل بل ين د ال ا دجل](#)

[قزي مل ا لي صا فت](#)

[قي في طول ا قزي مل ا ف ص و](#)

[لم عت في ك](#)

[ك رت ش مل ا د ع ا ق ل ا م ي ي ق ت](#)

[ق ت ق ق م ل ا IPS ن ن ا خ م و ت ا ن ا ي ب ل ا ق ف د ت](#)

[د ع ا ق ل ا ر ا ر م ت س ا](#)

[م د خ ت س م ل ا ت ا ن ي و ك ت](#)

[ا و ا ل ص ا و ا ط ا خ ال ا ف ا ش ك ت س ا](#)

[ق ن ي ع ل ا ق ل ك ش م](#)

[ف ص و ل ا : ق ل ك ش م ل ا](#)

[ل ج ل ا : ق ل ك ش م ل ا](#)

[ق ع ئ ا ش ل ل ا ل ك ا ش م ل ا و د و ي ق ل ل ا ل ي ص ا ف ت](#)

[ع ر خ ال ا ت ا ر ا ب ت ع ال ا و د و ي ق ل ل ا](#)

قم دقمل

ادعاصف 7.4 نم Snort 3 في اهتفاض ا تمت يتي ال ا ديدجل ا تاي نقت ال ا ققي ثول ا هذ ه فصت

قيساس ا تامول عم

- اءال ا في قزي م ي ط ع ي ج ه ن ال ا ا ذ ه ن ا م غ ر و . ر ط ح ل ا ع ض و ي ف Snort 3 ف ا ش ت ك ا د ح و ل م ع ت ف ش ك ي ل ع د و ي ق ل ا ض ع ب ي ل ع ي و ط ن ي ه ن ا ف ، (ا ي ب س ن) ذ ي ف ن ت ل ا ي ف ة ط ا س ب و . د د ع ت م ت ا ن ا ي ب ل ت ك ر ب ع د ت م ت ي ت ل ا ت ا ع ي ق و ت ل ا
- ي ه و ، Snort ، في ت ا ن ي س ح ت ل ا ض ع ب ذ ي ف ن ت ل ع ف ل ا ب م ت ، م د خ ت س م ل ا ة ب ر ج ت ل ي ه س ت ل و ة ك ب ش ل ا ق ف د ت ي ل ع ة م ا ل ع ع ض و د ع ا ق ل ا ب ت ا ك ل ب ا ي س ن ا ل ا ت ب ت ا د ح و ح ي ت ت 1 . ا ه ت ي ف ص ت و ة ي ص ا خ ل ا ك ل ت ن ي ي ع ت ن ك م ي و ، م د خ ت س م ل ا ل ب ق ن م ة ف ر ع م ة ي ص ا خ ر ب ك ا ع ي ق و ت ل و ح ج ا ت ن ت س ا ل ل ق ي ر ط ل ث م ي ا م م) ق ف د ت ل ا ن م ة م ز ح ي ا ي ل ع ا ه ر ا ب ت خ ا و (م ز ح ل ا ي ل ع
- ر ب ك ا ق ل ت ك ن و ك ت ي ت ل ا و ، ا ه و ا ن ب د ا ع م ة م ز ح ي ف ك ا ل س ا ل ا م ز ح س ي د ك ت ب ق ف د ل ا د ح و م و ق ت ر ف و ي ا ه و ا ن ب د ا ع م ل ا ة م ز ح ل ا ل ب ا ق م IPS د ع ا و ق م ي ي ق ت ن ا ا م ك ، م ا خ ل ا ة م ز ح ل ا ن م ة ي م ه ا ر ث ك ا و (ع ي ق و ت) ر ب ك ا ط م ن ة ق ب ا ط م و ا ه ل م ك ا ب ة ر و ص ل ا ة ي و ر ل ص ر ف ل ا ن م د ي ز م ل ا
- ن م ض ت ت ا ه ن ك ل ، ط ق ف ة د ي د ج ت ا ن ا ي ب ا ه و ا ن ب د ا ع م ل ا ة م ز ح ل ا ل ث م ت ا ل ت ا ل ا ح ل ا ض ع ب ي ف

قرم؛ فشكلا ةطساوب لعفلاب اهتجالعم تمت يتلا ةقباسلا تانايبلا نم عزج ضعب
ىلا دتمت يتلا تاعيقوتلا فاشتكاب حمست ةمكارتملا تانايبلا ةعومجم نأ ىرخأ
(ام دح ىلا) قفدتلا ىلع فلخللا

- عطقلا ةطقن نوكت نأ لم تحملا نم نكلو، لتك ىلا قفدتلا عطقب رايتلا قرفم موقى
ىدل يلاتلابو، طامألا فاشتكاب بنجتلا اهمادختسا مجاهملل نكمي فعض ةطقن
ديزي اذهو. ؤبنتلل ةيلباق رثكأ ماسقنالا لعجل اهقيبطت متي حاجترا ةيلا تروشللا
مجاهملا ليلحت ديقعت نم

ديدجال ام

موقت. ةمئاقلا ىلا هتفاضلا نكمي ديدج بولسا وه ةلاحلا ددحي يذلا عيقوتلا ميقوت
ناف اذه ىلعو. ةددعتم لتك ربع IPS ةدعاق ميقوت نيكمت قيرط نع فشكلا تاردق عيسوتب
اهنكلو، تانايبلا ىلا رقتفت ةيلاحلا ةلتكلا تناك اذا روفلا ىلع مءالتت ال ةدعاقلا
لوصولل تانايبلا نم ديزملا كلذ نم الادب رظنت

ةمومدملا ةيساسالا ةمظنالا

ةيساسالا ةزهجال او جماربلا ىندالا دحل

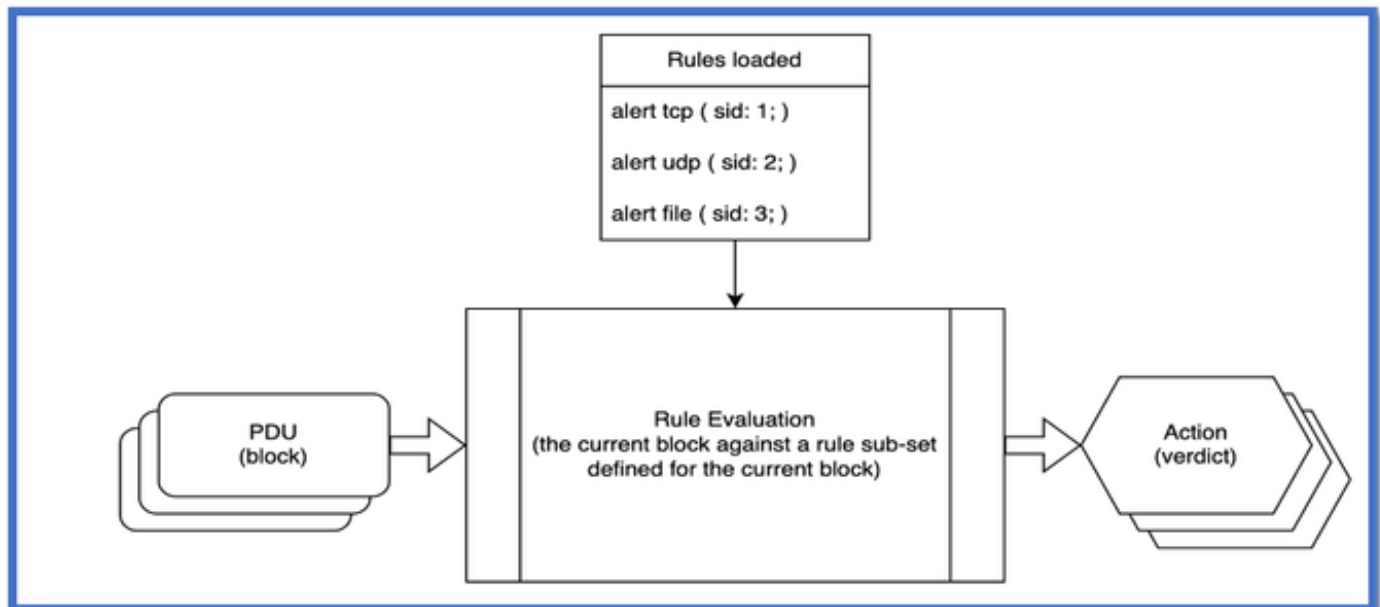
رادصلا ىندالا دحل Supported Manager	ةرادملا ةزهجال	رادصلا ىندالا دحل مومدملا رادملا زاهجال بولطملا	تاطحالما
Management Center 7.4.0	Firepower Threat Defense (FTD) ماظن	7.4.0	طقف 3 ترون
7.4.0 زاهجال ريديم	معددي FTD جمارب ي ةرادلا FDM	7.4.0	طقف 3 ترون

ةزيملا لىصافت

ةيفيظولا ةزيملا فصو

لمعت فيك

ةكرح ةجالعم ةلحرم في. يطيظختلا مسرلا في ةيظمنلا فشكلا ةدحولمع ريس فصومت
لبقت اهنأ امك، اهليمت مت دعاوقلا عيمج ىلع لعفلاب ةيظمنلا ةدحول يوتحت، رورملا
ةلتكل اهذاختا بجي يتلا تاءارجالا فرعتو، دعاوقلا ميقتو، ةيدرف ةقيرطب تانايبلا تاعومجم
ةيلمعلاب ةصاخلا ةلاحلا عيقوت ميقوت



موظنن لول تاطحالم:

1. ةءاق لك مئقق مئق؁ ةئلالل تانائبل ةللل ةئرف ءءاق ءءومءم ءئءل ءرءم ب. ىرأ الل ءءاقول نع لقللسم لكشب انه م.
2. ىرأ للل نع لقللسم لكشب تانائبل ةللل لك مئقق مئق.
3. اهمئقق مئق ئلل او IPS ل ءلؤلؤل نزلؤل نم ءءومءم ءئرف ئه تانائبل ةللل ءلللال ءلللال.
4. مءلل ءئءل مئقو؁ ةئلالل ءمزللل اهمئقق مئق ئلل تالل تاءارءلابل ءمئلل وه ءارءلل ءعب امئق ئئاهللل.

IPS ءءاق مئقق ةئففك ىل ءرطن قلأ؁ ءلالل وء ءققولل مئقق لم ءئففك مهفل اءل ءانائبل للل لكشب نأ نكمئ فئفك وء ءرلشملل.

ءرلشملل ءءاقول مئقق

ءءوملل اءه فئ IPS ءءاق مئقق نكمئ:

```
action protocol source → destination ( option_1: parameters; option_2: parameters;
option_3: parameters; gid: 1; sid: 1; meta_option_1; meta_option_2; meta_option_3; )
```

لئ:

ءءاقول لئءشئ مئ اءل ءمزللل ىل IPS ءارءل - ءارءل

ءقباطملل لوكولورب - لوكولورب

ءنملل او IP ناولع - ءءولل وء رءصملل

ءءاقول مئقق نم ءرء ءئل لل IPS تارائء - option_1 و option_2 و option_3

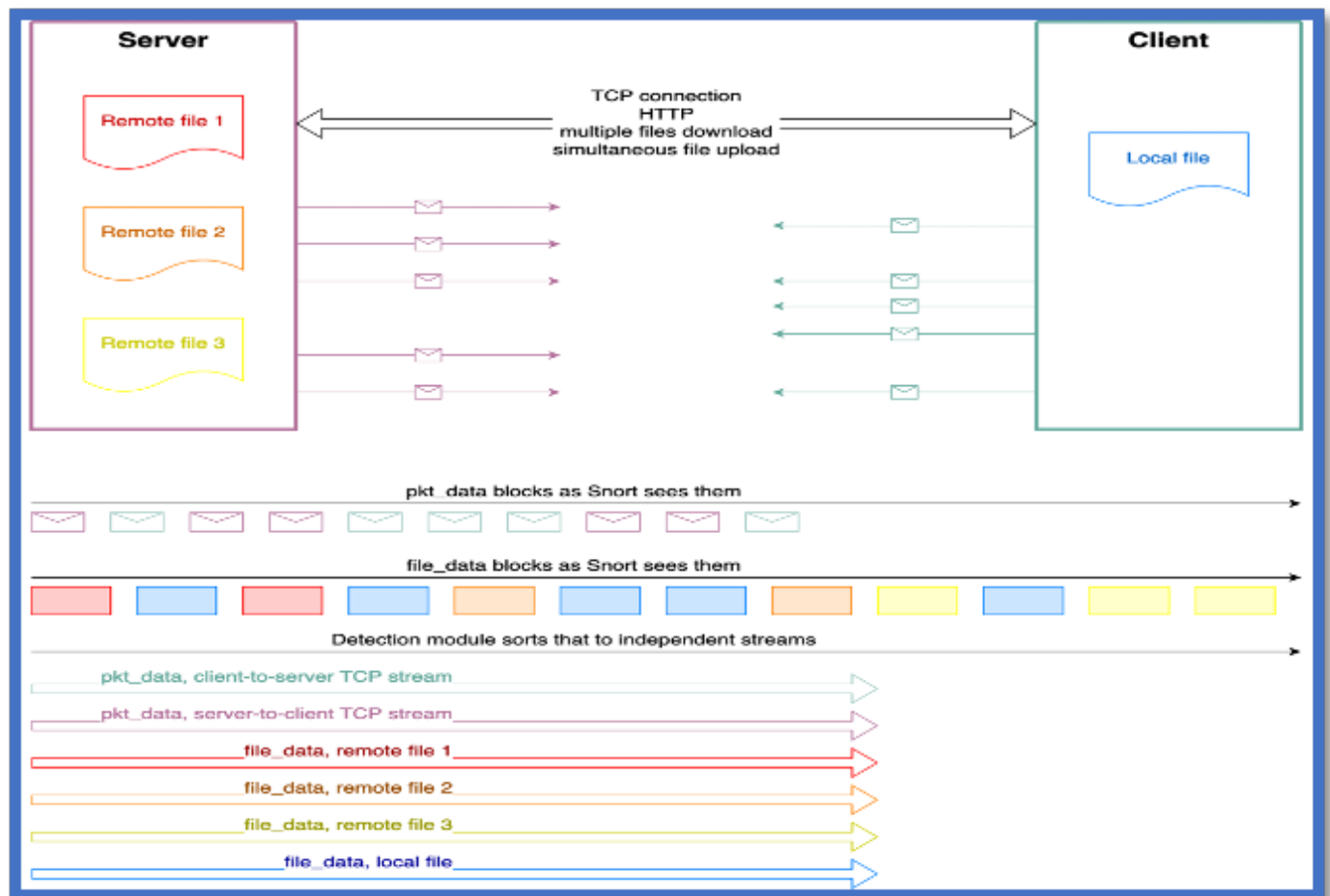
(ةيولوالا تانايبال تاراخي لثم) ةدعاقال فرعي ديرف جوز - sid و GID

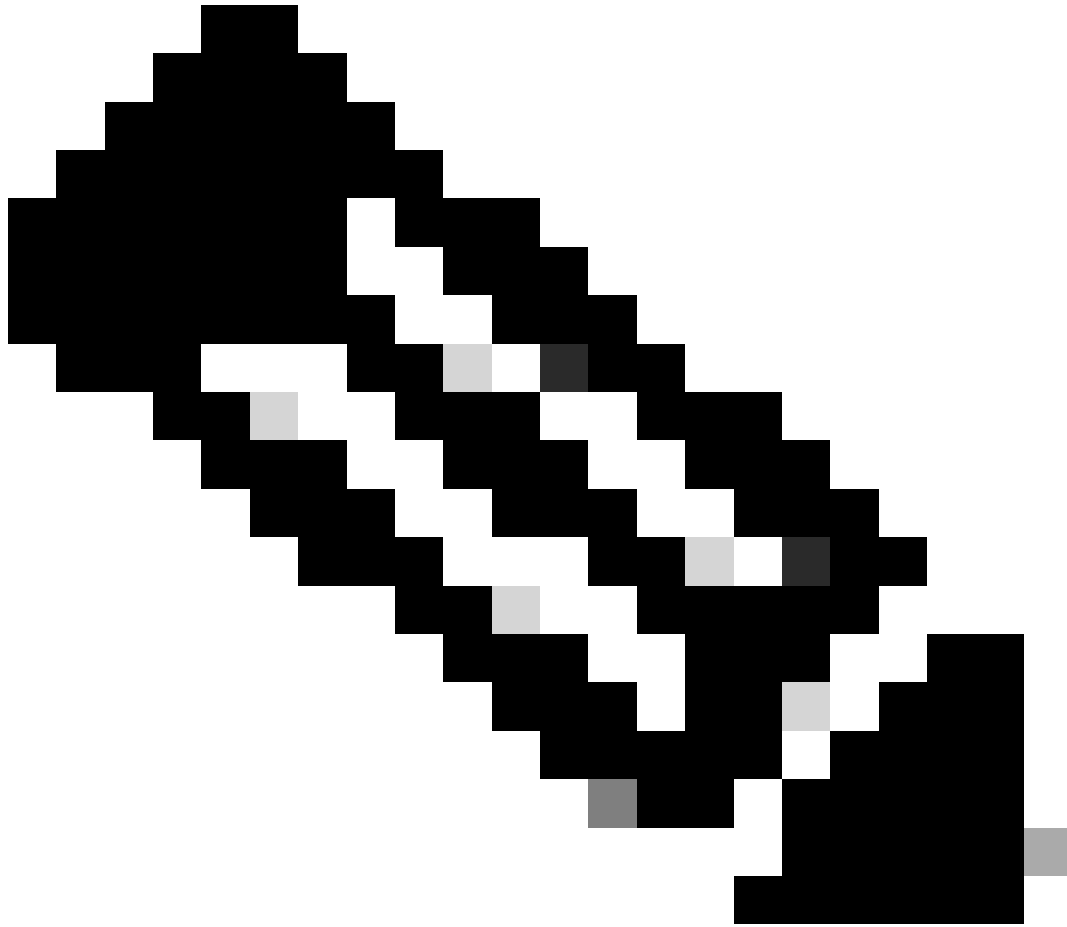
عون ،ةلاس رلثم ةيولوالا تانايبال ري طست - meta_option_1، meta_option_2، meta_option3
ةدعاقال مبيقت يفي كراشت ال تاراخيال كلت ،عجرم وأ ،فنص

- ةكبشال قفدتل ةيفصت لماعك لمعي .ةدعاق سار ةهجولاول ردصملاو لوكوتوربال جذومن IPS تاراخي .ةدعاق ةئيه وه نيسوق نيب عيش لك .(مبيقتلل هلوبق متي يذال) اهمبيقت متي يتل كلت يه ةدعاقال صن نم (ةدعاقال فيرعت تانايب اناثتساب) :تارابعال هذلل لثتمت يهف .تانايبال ةلتكل
- .نيميلا لراسيلا نم ةقذب تاراخيال مبيقت متي
 1. .نيسيساسا نيعون دحا نوكي نا نكمي
 2. .ةيلالحا ةمزحلل تقوؤم IPS نزخم راخيال دحي ،تقوؤملا نزخملا نيعم
- (قفدتل ةيلمع ،رشؤملا ةجالام ،باسحلا ةيلمع ،شقنلا نع ثحب) رخا
- .ددحمال IPS ل تقوؤملا نزخملا يفي عوضوملا بقعتل رشؤملا مادختسا متي
- :اما تاراخيال دحا نوكي نا نكمي
 1. رشؤملا عضو لىل دمتعي ال ي ،'قلم'
 2. رشؤملا عوضوم نم اهمبيقت ادبي ينع ي'بسن'
- نلولش فيسف ،ددحمال IPS ل تقوؤملا نزخملا جراخ رشؤملا نييعة تاراخيال دحا لواح اذا (تانايبال صقن ببسب) اهلمكأب ةدعاقال قباطت
- لىل رفوتت نا نكمملا نم ناك اذا .ةيطمنلا فشكلا ةدحو ديدحت يه ةريخال ةطقنلا دعاوقال مبيقتل اهتيؤر متي يتل تانايبال لك نيزخت متي فوسف ،ةدودحم ريغ دراوم (كالسألا مزح نم ديزملا لصي) ةحاتم تانايبال حبصت ام دنع رخا دعب ةرم

ةتقوؤم IPS نزخمو تانايبال قفدت

- .وهو .ردصملا سفن نم عباتتم جذومن يفي تيبال تادحو نم قفدت وه تانايبال قفدت نيب ةدعاقال مبيقت عارجا بجي .ةلاحال دحي يذال مبيقتل معدل مدقي ديدج موهفم صن وأ يقن TCP قفدت وأ فلم ناك ءاوس) ةيقتنملا تانايبال سفن نمض لتكل (JavaScript).
- :نكمي فشكلا ةدحو ةطساوب اهيقلت مت يتل تانايبال ةلتك ،ماع لكشب
 - اسيل file_data و pkt_data ،لاثملا ليبس لىل) فلتخم تقوؤم IPS نزخم نم نوكي نا (نيلثامتم)
 - رخا قفدىل يمتنا
 - (ماخ ةمزح نم اهؤاشنا مت يتل ةتقوؤملا نزخمال) قفدت لكشي ال
 - (ICMP ، UDP) الصتم اقفدت لكشي ال
 - (ةيئزجال HTTP ةباجتسا) ببيترتللاب نوكت ال
 - وأ http_inspection.script_detection لثم ،ةمكارتم ةلتك) ةرركتم تانايب لىل يوتحي (ةمسقملا HTTP ةباجتسا)
- نإف ال او ،طقف قفدل سفن نم لتك ببيترتل ءايشألا زرف فشكلا ةدحول نكمي ةلخادتم لتك نم هي فبوغرم ريغ لخادت ىرتس مبيقتل ةيلمع





تافلم لي زنتو لي محتب HTTP ليمع اهيف موقوي ةلاح انه لاثملا مدقي: ةطحال م
تقولا سفن يف ةدعتم

- شيح، file_data و pkt_data: قفد IPS ل طقف نادصم لثمي نأ نكمي، ايلاح
ىلا مداخل او مداخل ىلا ليمعلا تاداشرا) TCP لوكوتوربل نيروود جذومن PKT_DATA
(للمعلا)
2. تانايب و MIME تاقفرم وأو تافلملل جذومن تاقفد file_data نوكي نأ بجي
(رخأ ىوتحم عون وأو HTML HTTP ةحفص لثم) رخأ لوكوتورب
• تانايبلا قفدت لخاد مراض لكشب ةلاحلا ددحي يذلا ميعيقتلا عارجا متي

ةدعاقلا رارمتسا

- نيعيتب ماق اذا قباطتم ريغ IPS راخي نأ ىلا ريشت ةلمجب مدقألا مسقلا يهتني
قفدت IPS ل تقوؤملا نزخملا لكشي امदन نكلو. يلاحلا IPS تقوؤملا نزخملا جراخ رشؤملا
ةدعاقلا ميعيقت قايس لخدت ةلاحلا نع ربعملا عيقوتلا ميعيقت ةزيمناف، تانايب
رارمتسا (ةلاحلا) ظوفحملا ميعيقتلا قايس ىمسي. Snort قفدت نئاك يف هظفحتو
رفوتي نأ ىلا ةدعاقلا لئاهنلا مكحل ةلاحلا ددحي يذلا عيقوتلا ميعيقت لجؤي. ةدعاقلا

ت. تاناي ببل نم دي زمل

- ردصم IPS ل تقوؤم لنزخم لمسا: ةيسيئر ءانجأ ةثالث ىلع ةدعاق ل ةعباتم يوتحت اديرف افرعم تقوؤم لنزخم لمسا (ردصم دع) فدهتسم لمسا رشوؤم لمسا رشوؤم لنزخم لمسا (تاناي ببل قفدتل تاءارجال ثدحت، ةيظمننل فشك ل ةدحو ةطساوب تاناي ببل ةلتك ةجالعم متت ام دنع :-ةقلا تال
- اذا قفدتل اب اهطبري و ةدعاق ل رارمتسا ةلاحل ددحي يذلل عي قوتل ميريقت ئشن ي
• عضو شي دحتب موق ي رخأ عيش ي أو pcre أو content أو byte_jump IPS راخي لمعي
• ةلاحل IPS ل تقوؤم لنزخم لمسا دع رشوؤم لنزخم لمسا نبيعت ىلع (رشوؤم ل
• تاناي ببل قفدتل ةلاحل IPS ل تقوؤم لنزخم لمسا معدي
• ةطحلل هذه ي ف تاناي ببل قفدتل ةلاحل IPS ل تقوؤم لنزخم لمسا لكشي
- نم هليزيو وتلل اهؤاشن مت يتل ةدعاق ل رارمتسا ةلاحل و ذ عي قوتل ميريقت بحسي
اذا قفدتل:
• نكامأ عم ةدعاق ل قباطت) ةلاحل تاناي ببل ةلتك ىلع IPS ةدعاق ليغشت مت
(ةلتك ل نم رخأ)
- قفدتل نم اهليزيو ةقل عمل ةدعاق ل رارمتسا ةلاحل يطمع لمسا عي قوتل ميريقت صفري
اذا:
• يوتحت، لاثم ل لبس ىلع) الصتم اقفدت IPS ل تقوؤم لنزخم لمسا لكشي ال
نأ و تاناي ببل نم عزج دق ف مت) ةوجف كانه و، اهلاخادب ةرركتم تاناي ببل ىلع تادحول
(ببترتلاب تسي ل ةلتك ل
- فدهتسم لمسا رشوؤم لمسا عضو شي دحت ىلع ةلاحل ددحي يذلل عي قوتل ميريقت لمعي
ام دنع ةرفوتم لمسا ةديجل تاناي ببل اب:
• ددحم ل تقوؤم لنزخم لمسا ردصم س فن وه ةدعاق ل رارمتسا نم تقوؤم لنزخم لمسا ردصم
• لصتم قفدت IPS ل تقوؤم لنزخم لمسا لكشي
- IPS ةدعاق كرحم ىل رخأ ةرم ةدعاق ل رارمتسا ةلاحل ددحي يذلل عي قوتل ميريقت لسري
ام دنع:
1. اهنأ ينعي ام) ددحم ل IPS ل تقوؤم لنزخم لمسا لخاد ةفدهتسم لمسا رشوؤم لمسا عضو طاقن
(ةدعاق ل ميريقت لامك ل ةمزالل تاناي ببل عي مج اريخأ تقلت

مدختسم ل تاناي وكت

- كانه. اهنم دودحم ريغ ددع نيزخت Snort ل نكمي الف، ةركاذل ذخأي دعاوق ل رارمتسا نأ امبو
دحل ي ف مكحتلل نيزوكت راخي:
1. detection.max_continuations_per_flow = 1024: دحل { 0:65535 } قفدتل ىلع دحاو نأ ي ف ةننخمل
لدبتسي هنإف، هب حومسم ل دحل ىل ةلاحل نع ربعم لمسا عي قوتل ميريقت لصي ام دنع
ديج رخأ ةدعاق ل رارمتسا مدقأ
- يفت ال اهنأ ينعي ام، ادج ةليوط ةرتفل قفدتل ىلع ةدوجوم رارمتسا ةدعاق مدقأ دجوت
ةدعاق ل ميريقت فانئتسا طرشب
- ةقذب IPS دعاوق طبضل ةرفوتم لمسا peg دع تاي لمع نم ريثك ل كانه، كلذ ىل ةفاضل اب
(رمأل مزل اذا) دحاو (يسيئرل زيكرتل نوكت نأ بجي يتلوا)
1. detection.cont_creations: (عومجم ل) اهؤاشن مت يتل راركتل تاي لمع ددع يلامج
2. DETECTION.cont_RECALLS: (عومجم ل) اهؤادتسا مت يتل تارارمتسا ل ددع يلامج
3. detection.cont_flow: (عومجم ل) رارمتسا ل مدختست يتل تاقفدتل ددع يلامج
4. detection.cont_evals: (عومجم ل) طرشل ءافيتسا رارمتسا تارم ددع يلامج
5. detection.cont_match: (عومجم ل) قباطتم ل راركتل تاي لمع ددع يلامج

6. detection.cont_mismatch: (عومجملا) ةرارمتسالا قباطت مدع تارم ددع يللامج: (ىصقأ دحك)
7. detection.cont_max_num: قفدت لك ةنمازتملا رارمتسالا تايلمع نم ددع ىصقأ (ىصقأ دحك)
8. detection.cont_match_distance: اهيل زفقل مت يتلا تيابل تادحو ددع يللامج: (عومجملا) ةقباطتملا راركتلا تايلمع ةطساوب
9. detection.cont_mismatch_distance: اهيل زفقل مت يتلا تيابل تادحو ددع يللامج: (عومجملا) ةقباطتم ريغ ةعباتم تايلمع ةطساوب

اهحالصا وءاطخالا فاشكتسا

اهحالصا وءاطخالا فاشكتسا نكمي ال كلذل ، ةدوجوملا فاشكتسا ةي لمعل نيسحت يه ةزيملا وأ نيوكتلا وأ دعاوقلا صحف بجي ، فاشكتسا يف لشف تالاح ي ءاودح ةلاح يف . جيريص لكشب رورملا ءكر .

ةنيعل ءلكشم

فصولا : ءلكشملا

- تقولا سفن يف هبنذو فلملا ةيادب نم ققحتت نأ بجي عي قوتلا نأ لوقن انعد .
- (فيرعت تانايب ، صن ، سأر) لك يهلا اذه نم فدهتسم فلم يف ، لاثملا لبيس ىلع 0. ةميق هب ةصاخلا فيرعتلا تانايب نم يأل ناك اذا ام ةفرعم ىلا جاتحن
- شيج e1 f3 22 03 7f ff xx xx ... xx 01 00 02 00 : تافللملا تيابل تادحو
 - فلملا عون فرعي يذلا ، يرحسلا مقرلل تيابل 4 - e1 f3 22 03
 - مسجل مجحل تيابل 2 - 7f ff
 - تانايب للضعب نم تيابلوليك 32 - xx xx xx ... xx
 - تيابل 1) ةمالعلا ةميقي قيسنتب ، ةيفصولا تانايب نم تيابل 4 - 01 00 02 00 (اهنم لكل
- file_data : (هي بننتلا فلم : يلي امك IPS ةدعاق ودبت فوس : اي بسن 4 : لخد ، "00" : ىوتحملا ، fast_pattern : byte_jump : 2.0 ، relative : "e1f32203" : ىوتحملا sid : 1)
 - شيج
 - (ال) طقف اهؤانب داعملا مزحل لبقت ةدعاقلا نأ فلملا لوكوتورب نمضي (ةلاحلل دعملا عي قوتلا مييقت يف ماخلا مزحلا كراشت
 - اقفدت نوكتي نأ نكمي يذلاو ، تقوؤم فلم تانايب نزخم 'file_data' رايلخا ددحي
 - لكذ ناك اذا) يرحسلا مقرلا نم ققحتت ويرس جذومن وه لوألا ىوتحملا رايلخ (دوصقملا فلملا عون وه
 - فلملل ياساسالا صنلا قوف لقتنيو فلملا صن مجح byte_jump رايلخ أرقبي
 - تانايبلا ميقل يئاهنلا ققحتلا ذيفنتب يئانثلا ىوتحملا رايلخ موقي
 - بيسن رايلخلا لعجي و شحبلا قمع دح لماعملا نمض ، ةيفصولا

لحلا : ءلكشملا

ةةقيرطلا هذهب ةدعاقلا ميريقت متيس

يساسأل صنللا نم عزجو فلم سأل لمحت يتلاو، (تيا ب وليك 8 مجحب) لولال ةمزلال لعل

1. رشاعلا تيا بل لىل رشؤملا ريشي IPS buffer file_data ديحت مت
2. اريشم، ةرشابم يرسلال مقرلا دعب رشؤملا عوضوم نييعو عيرسلال شقنللا رايخ قباطي 7f. تيا بل لىل
3. تيا بل نيताهب رشؤملا شيحت متي. فلملا صن مجح نم نيताب byte_jump رايخ أرقى. تيا ب 32768 نم رثكال ةزف ق باسحب BYTE_JUMP موقى م
4. 24578 لىل جاتحت شيح، ةدعاقلا رارمتسا ةلاحلا ددحي يذلا عيقوتلا ميريقت ئشنى (مسلال مجح نم تيا ب 2 - سألل نم تيا ب 4 - تيا ب وليك 8) - 32768) رثكال تيا ب
5. لىل رشؤملا عوضوم نييعت في لشفى byte_jump رايخ نأل، قباطتت ال اهل مكأب ةدعاقلا. دحلل اذه

فلملا صن عزج لمحت يتلاو، (تيا ب وليك 16 مجحب) ةيناثلا ةمزلال لعل

1. ةقلعملل ةدعاقلا رارمتسا ةلاحلا ددحي يذلا عيقوتلا ميريقت رهظى.
2. وه ديدجل تانايبلا مجح نأو رفوتم file_data نأ ىريو همساب تقؤملا نزخمل ددحي وه. 16384.
3. (16384 - 24578) تيا ب 8194 لىل لازت ال ةجالحا نأ ثدحمل رشؤملا رهظى
4. ةدعاقلا فانئتسا متي مل.

فيعرعتلا تانايبو فلملا نتم عزج لمحت يتلاو، (ماجأ 8198 نم) ةثلاثلا ةمزلال لعل

1. ةقلعملل ةدعاقلا رارمتسا ةلاحلا ددحي يذلا عيقوتلا ميريقت رهظى.
2. وه ديدجل تانايبلا مجح نأو رفوتم file_data نأ ىريو همساب تقؤملا نزخمل ددحي وه. 8198.
3. 8194 وه رشؤملا عوضوم، ةيفاك تانايب هب تقؤملا نزخمل نأ ثدحمل رشؤملا رهظى.
4. ةدعاقلا رارمتسا فذحب ةلاحلا ددحي يذلا عيقوتلا ميريقت موقى.
5. يناثلا يوتحمل رايخ نم ةدعاقلا ميريقت ةلاحلا ددحي يذلا عيقوتلا ميريقت فئاتسى. 01. تيا بل لىل رشؤملا ةراشا عم
6. هنع ثحبلا مت يذلا يناثلا تيا بل لىل قباطت نع يوتحمل رايخ ثحبى.
7. اريخأ قلطنت اهلك ةدعاقلا.

ةعئاشلا لكاشملاو دويقلا ليصافت

ىرخال تارابتعالاو دويقلا

- تايللمع عي مج طاقساب Snort موقى، ةلاحلا ددحي يذلا عيقوتلا ميريقت ذيفنتل ارطن ةدعاقلا رارمتسا نأ طحال. هب صاخلا نيوكتلا ليمحت ةداعا دنع ةقلعملل دعاوقلا ةعباتم تانايبلا ةلتك لاسرا متي تحت Snort ةركاذ لغشى لازي ال اهاطاقسا نم مغرلا لعل فشكلا ةدحو لىل ةيلاتلا
- ميريقت تناك ول امك ةلاحلا ميريقت في IPS ةدعاقلا ةدعاقلا لاقتنا نمز ةزيم لمعت. ةفلتخمل تانايبلا لتك في ةدعاقلا عاجأ ميريقت تقو صيخلت متي. ةكرتشم ةدعاق لبق ءاهنال متي، ةريصق ةرئاد ربع متي ةدعاقلا ميريقت ناف، دحلل تقولا زواجت اذا كلذ
- "ةتباتلا" تارايخلل لثم يذوت لازت ال اهنأ مغر، اهانعم ببايسنال تايللمع ظفتحت

مت اذا، كذلك. ايلاح فورعم قاييس نمض ةي بايسنا رابتخا/حسم/نيي عت ةيلمع عارجا متي
ةيلاح ةئيبل رابتعالا ي ذخايس هناف، ةدعاق رارمتسا ي بايسنال راخي مبيقت
اهي اهمبيقت ةدعاقا تادب يتلا ةئيبل سيلو، (بايسنال تبت ادحو ةومجم)

عيرسلا طمنلا عقوم يلا هبتني نأ دعاقا لبتاك يلع بجي، اضيأ

طمنلا راخي مبيقت متي هناف، ةدعاقا نم عزج يأي ف نوكتي نأ نكمملا نم ناك اذا يتح
ةدعاقا للة بسنلاب. ةدعاقا مبيقت ليغشتب موقت. اهلماكب ةدعاقا لبق عيرسلا
رارمتسا ةطقن نأ ينعي اذهف، ةلاحلا يلا ريشي ذل عيقوتلا مبيقت يلا ةدنتسملا
عيرسلا طمنلا راخي دعب نوكت نأ بجي ةدعاقا

اهمبيقت يي دعاقا ةرارمتسا تايلمع ةدع IPS ةدعاقا نوكتي نأ نكمي، كذلك يلا ةفاضلاب
رمتسي نأ نكمي ةدعاقا صن نم راخي يأي نأ امب. (تقول سفن يي سيلو، يرخأا دعب ةدحاو)
تانايبل قفدت نم ةفلتخم نكاما يي ةيفاضا تاققحت عارجاب ةدعاقا لبتاكل حمسي هناف
IPS ةدعاقا سفن

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م ج ر ت
م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م ج ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م م ج ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م ج ر ت ل ا ع م ل ا ح ل ا و ه
ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م ج ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems
(ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا