

هجمات DOS و DDOS في الشبكات المعرفة بالبرمجيات

د. مهند عيسى*

سلفانا علي**

سمارة سليمان**

ملخص

ان هجمات رفض الخدمة DOS أو رفض لخدمة الموزعة DDOS هي عادةً محاولات صريحة لاستنفاد النطاق الترددي أو تعطيل وصول المستخدمين الشرعيين الى الخدمات .البنية التقليدية للإنترنت عرضة لهجمات DDOS وتوفر فرصة للمهاجم للوصول الى عدد كبير من أجهزة الكمبيوتر معرضة للخطر من خلال استغلال نقاط الضعف الخاصة بها لإعداد شبكات هجوم.

هجوم حجب الخدمة DOS هو هجوم الهدف منه جعل الضحية خارج الخدمة وذلك عن طريق إغراقه بعدد كبير من الطلبات يصبح فيها غير قادر لاستجابة طلبات المستخدمين العاديين.

هجوم حجب الخدمة الموزعة DDOS مشابه لهجوم حجب الخدمة من حيث الهدف إلا أنه يختلف عنه بآلية العمل حيث يتم فيه أكثر من جهاز لإنجاز الهجوم على ضحية واحدة ويتم التحكم بهذه الأجهزة التي تقوم بالهجوم عن طريق برنامج من قبل المهاجم.

الكلمات المفتاحية: الشبكات المعرفة بالبرمجيات، هجوم حجب الخدمة، هجوم حجب الخدمة الموزعة

* الهيئة التدريسية -كلية الهندسة الميكانيكية والكهربائية قسم هندسة الاتصالات والالكترونيات -جامعة تشرين.

**طلاب سنة خامسة -كلية الهندسة الميكانيكية والكهربائية قسم هندسة الاتصالات والالكترونيات -جامعة

تشرين.

DOS & DDOS Attacks in Software-Defined Networks

Dr. Mouhnad Essa*

Selvana Ali**

Samara suliman**

ABSTRACT

Dos and DDOS attack

Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks are usually explicit attempts to exhaust bandwidth or disrupt legitimate users' access to services. The traditional architecture of the Internet is vulnerable to DDOS attacks and provides an opportunity for an attacker to gain access to a large number of vulnerable computers by exploiting their weaknesses to set up attack networks

DOS Denial of Service attack

It is an attack aimed at making the victim out of service by flooding him with a large number of requests in which he becomes unable to respond to the requests of ordinary users

Distributed Denial of Service (DDoS) attack

Similar to the denial-of-service attack in terms of the target, but it differs from it in the mechanism of action, in which more than one device cooperates to accomplish the attack on one victim. These devices that perform the attack are controlled by a program by the attacker.

Key Words: Software-Defined Networks , DOS – Denial Of Service Attacks, DDOS – Distributed Denial Of Service Attacks

*Education Institution –Mechanical and Electrical Engineering Department of Communications and Electronics Engineering – Tishreen University.

**Fifth year students–Mechanical and Electrical Engineering Department of Communications and Electronics Engineering – Tishreen University.

مقدمة:

الشبكات المعرفة بالبرمجيات هي من أكثر المواضيع المطروحة للنقاش في السنوات الأخيرة ،فقد قدمت العديد من المميزات وساهمت في حل العديد من المشاكل التي عانت منها الشبكات التقليدية.

تعتمد الشبكات المعرفة بالبرمجيات على فصل عمليات توجيه البيانات عن عمليات التحكم واتخاذ قرارات التوجيه لجعل التحكم بالشبكة مركزياً وبالتالي تقليل الأخطاء التي من الممكن أن تتعرض لها الشبكات.

يعتبر بروتوكول OpenFlow هو الأكثر شيوعاً واستخداماً في متحكمات الشبكات المعرفة بالبرمجيات للتواصل والتحكم بالمبدلات . باستخدام هذا البروتوكول ،يتعلم المبدل معلومات التوجيه من المتحكم ومن ثم تمرير حزم البيانات بالاعتماد على هذه المعلومات .

أهمية البحث وأهدافه:

التعريف بالشبكات المعرفة بالبرمجيات وأمنها ودراسة هجمات حجب الخدمة الموزعة وأثرها على الشبكة، فقد فتحت الشبكات المعرفة بالبرمجيات (SDN) فرصاً جديدة لعشاق الشبكات لتجريب ونشر طرق مبتكرة لإدارة الشبكات والتحكم ديناميكياً في توجيه حزم البيانات في شبكاتهم .

طرائق البحث وموارده:

تم تنفيذ الهجمات باستخدام أدوات خاصة على المحاكى mininet حيث تم الكشف عنها وإيقافها .كان هدفنا من تحليل هذه الهجمات في بيئة SDN هو تحديد فئة الهجمات التي قد تشكل تهديدات خطيرة لوحدة التحكم .

لقد ساعدنا ذلك على اكتشاف بعض الميزات التي قد تكون مفيدة لنا في اكتشاف هذه الهجمات.

النتائج والمناقشة:

بروتوكول OpenFlow هو بروتوكول التواصل بين طبقة التحكم والطبقة التي تليها (طبقة البنية التحتية) فيقوم بإنشاء قناة التواصل بين control plane والذي يمثلها المتحكم controller والـ data plane والتي يمثلها المبدل switch .

تم إنشاء هذا البروتوكول ليكون حلاً للتعامل مع المبدلات بشكل مفتوح كي يتم استقبال الطلبات من المستوى الأعلى نظراً لكم الهائل من الخدمات التي يتم تحديثها يومياً.

الفوائد التي قدمتها الشبكات المعرفة بالبرمجيات:

1. قابلة للبرمجة والتحكم بالشبكة بشكل مباشر .

2.يستطيع مهندس الشبكة التحكم في الشبكة بشكل كامل من مكان واحد حيث يقوم بعمل الإدارة والتحكم بها وصيانتها.

3.تحسين عملية إرسال البيانات في الشبكة من ناحية التوجيه وتوزيع الحركة.

4. توفير عدد كبير من الأجهزة حيث أنه نستطيع عمل أجهزة شبكة افتراضية ولكن غير موجودة في الواقع.

5.توفر وحدة مركزية للتحكم الكامل في الشبكة مما يسهل صيانة ومراقبة الشبكة.

المميزات التي تقدمها الشبكة لتحقيق الحماية:

تم مؤخراً إجراء الكثير من الأبحاث لتوفير الأمان للشبكة وقاموا بتقييم خصائص شبكة SDN والتي تؤثر على الأمن الذي توفره الشبكة وكانت نتائج التقييم:

1-إدارة الشبكة :

تم تقييم ادارة شبكات SDN على أنها ايجابية حيث توفر رؤية مركزية وبالتالي فإن إدارة SDN أبسط من إدارة الشبكات التقليدية .

وتكون الصيانة أكثر مرونة مما يوفر التكاليف والوقت لمعالجة الأخطاء كما توفر بيئة أمان طبيعية لمواجهة التحديات.

كما ان دمج تطبيقات الأمان الجديدة (مثل جدار الحماية) أسهل في شبكات SDN نظراً للمرونة .

2-التكاليف :

تم تقييم هذا المعيار على أنه ايجابي نظراً لتوفير تكاليف الصيانة وكذلك من ناحية تكاليف الموظفين ، لأن معالجة الأخطاء أسهل وأقل جهد ، علاوةً على ذلك يمكن أن يؤدي نشر شبكات SDN الى تقليل استهلاك الطاقة للأجهزة .

من ناحية ،لم تعد المبدلات مسؤولة عن مهام حساسة وقوية . ومن ناحية أخرى ،إذا كان من الممكن تخفيض الأجهزة فإن استهلاك الطاقة يتناقص أيضاً.

3-كشف الهجوم وتخفيفه:

لا تزال SDN قيد التطوير ولا يتم نشرها على نطاق واسع ،مما يسمح لمشغلي الشبكات بدمج عملية الكشف عن هجمات الشبكة والتخفيف منها حسب التصميم.

نتيجةً لذلك ، تقييم امكانية اكتشاف او تخفيف الهجوم في SDN هو ايجابي .

وأبرز آليات الدفاع عن تهديدات الشبكة هي التشفير والجدران النارية وأنظمة كشف التسلسل نظراً لأننا نعتبر SDN وسيلة لنقل حركة مرور الشبكة .

الأمن في الشبكات المعرفة بالبرمجيات :

هناك توقع هائل أن تحل الشبكات المعرفة بالبرمجيات SDN محل ادارة الشبكات التقليدية .ومع ذلك ، فإن SDN ليست محصنة ضد الثغرات الأمنية الموجودة حالياً او التي تنشأ حديثاً بسبب التغيير في تصميم الشبكة .

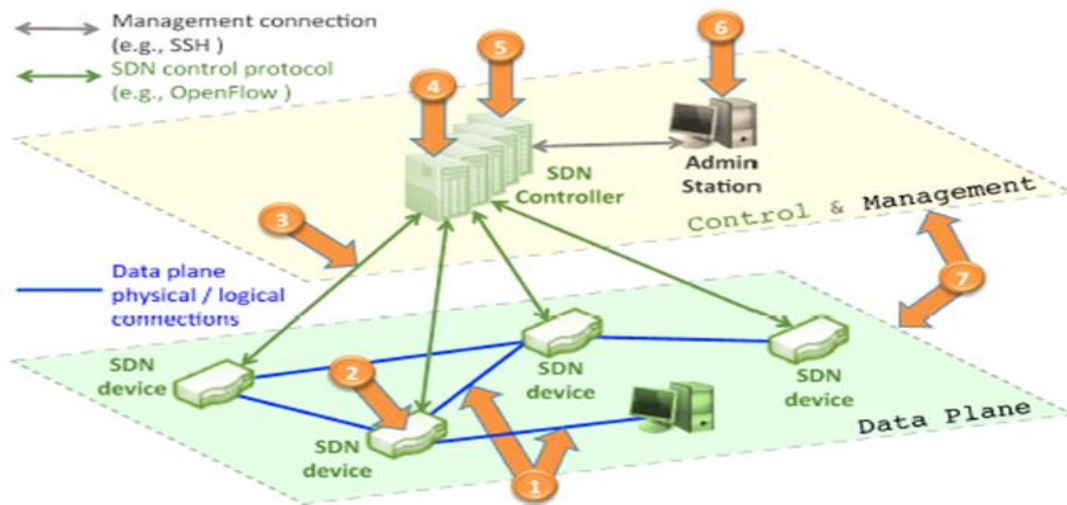
منذ بداية تطوير SDN كان التركيز الأساسي للأبحاث على فصل مستوى التحكم عن مستوى البيانات عن طريق الحفاظ على الأداء والمرونة التشغيلية دون تغيير .

في الوقت المناسب لتحقيق ذلك ، اتخذت الجوانب الأمنية لشبكة SDN مقعداً خلفياً. على الرغم من ان فصل مستوى التحكم عن مستوى البيانات يعد خطوة كبيرة نحو تبسيط ادارة الشبكة ، فإنه يخضع الشبكة إلى هدف محتمل ثنائي الاتجاه للمتسللين للحصول على السيطرة.

نظراً للتصميم المركزي لشبكات SDN ، فإن أمن وحدة التحكم قد يؤدي الى تعريض أمن شبكة كاملة للخطر .

مواضع الهجمات في شبكات SDN :

طالما أن شبكات SDN مقسمة إلى ثلاث طبقات فإن كلاً من هذه الطبقات قد تكون موجودة في موقع مختلف من الشبكة، كما أنه من الضروري الاتصال بين هذه المكونات وبشكل متكرر ، لذلك ومقارنة مع الشبكات التقليدية فإن SDN تقدم العديد من نقاط الهجوم .



الشكل (1) مواضع الهجمات في شبكات SDN

يبين الشكل (1) ٦ نقاط للهجمات الممكنة في بنية شبكات SDN وهي :

- مبدل SDN

إن مبدل SDN هو جهاز منفصل يتألف من عتاد صلب وبرمجيات مما يجعله قابلاً للهجوم .

- الوصلة بين مبدلات SDN

إن رزم البيانات المرسلة بين مبدلات SDN تكون غير مشفرة وقد تحتوي على معلومات حساسة للمستخدمين، إن هذه الرزم يمكن اعتراضها من قبل المهاجمين بسهولة خصوصاً عندما تكون الوصلة بين المبدلات لاسلكية .

- متحكم SDN

إن المتحكم هو النقطة الأكثر جاذبية للمهاجمين بسبب الانفتاح لقابلية البرمجة وتعقيد وظائفه، فإن برمجيات المتحكم حتماً قابلة للطعن وهذا قد يتم استغلاله من قبل المهاجمين الخبيثين .

- الوصلة ما بين المتحكم والمبدلات :

إن كل قواعد تمرير المعطيات يتم حقنها في المبدلات عن طريق المتحكم. إن رزم المعطيات التي تحتوي على هذه القواعد قد يتم التلاعب بها من قبل المهاجم من خلال التتصت على الوصلة ما بين المتحكم والمبدل، والذي قد يتسبب بحقن قواعد زائفة أو تعديل على القواعد الأساسية. إن وجود قاعدة واحدة مخادعة في المبدل قد يؤدي إلى أن رزم البيانات لن تمر بالشكل الصحيح .

- الوصلة بين المتحكمات:

إن الاتصالات بين المتحكمات في البيئات متعددة المتحكمات يعد أمراً ضرورياً من أجل المحافظة على استقرار كامل الشبكة. إن رزم البيانات المتبادلة ما بين المتحكمات يمكن أن تتم مقاطعتها مما قد يعطي للمهاجمين أفكار من أجل مهاجمة المتحكمات .

- برمجيات التطبيقات :

إن برمجية التطبيق تبنى مباشرة في المتحكم وهي تتوضع في نفس الجهاز الفيزيائي مع المتحكم، عندما تحقن برمجية التطبيق وظائف المتحكم من خلال الواجهة الشمالية، فإنه قد يتم إضافة برمجيات خبيثة إلى المتحكم ، لذلك تعد برمجية التطبيق هي أكثر نقاط المهاجمة المستخدمة من أجل السيطرة على المتحكم .

أهم التهديدات في شبكات SDN :

- حقن معطيات مزورة أو مزيفة:

حيث يمكن مهاجمة المبدلات والموجهات من خلال وجود أجهزة معطلة في الشبكة أو من خلال مهاجم خبيث يستخدم أحد مكونات الشبكة (موجه ، مبدل ، خادم.....) وذلك لإطلاق رزم بأعداد كبيرة من أجل تحقيق هجوم حجب الخدمة DOS: Denial of Service والتي قد تكون ضد المبدلات التي تعمل باستخدام البروتوكول Open Flow وذلك من أجل استهلاك جميع الذاكر الموجودة ضمن المبدل.

الحل المقترح: استخدام أنظمة كشف التسلل IBS: Intrusion Detection System مدعومة بأنظمة معرفة السبب الحقيقي المسبب للمشكلة، وذلك لكشف السلوك غير الطبيعي لعناصر الشبكة، إضافة إلى آليات التحكم الديناميكي بسلوك المبدل.

- الهجوم على نقاط الضعف الخاصة بالمبدلات:

حيث أن الهجوم أو السيطرة على مبدل واحد يعني إمكانية تجاهل طرد ما أو إعادة توجيه طرد ما إلى وجهة خاطئة أو نسخ طرود معينة، أو إبطاء توجيه الطرود ضمن الشبكة أو حتى حقن معطيات أو طلبات وهمية في الشبكة وذلك لإسقاط المتحكمات أو المبدلات المجاورة.

الحل المقترح: استخدام آليات من أجل إجراء عمليات المصادقة على البرامج أو استخدام آليات المراقبة أو كشف السلوك الغير طبيعي لأجهزة الشبكة.

- الهجوم على نقاط الضعف في المتحكم:

وهي أشد التهديدات خطورة في شبكات SDN ، حيث إن خلل وحدة تحكم واحدة أو إصابتها بهجوم خبيث يمكن أن يسقط الشبكة بأكملها، كما أن استخدام نظام كشف التسلل IDS قد لا يكون كافياً لأنه من الصعب إيجاد التجميع الدقيق للأحداث الذي قد تؤدي إلى توليد سلوك معين، والشئ الأكثر أهمية هو معرفة أن هذا السلوك هو سلوك خبيث، وأيضاً يمكن للتطبيقات الخبيثة في الشبكة أن تفعل ما يحلو لها في الشبكة.

الحل المقترح: يمكن استخدام العديد من التقنيات مثل التكرار أو النسخ (لكشف ازالة أو إخفاء السلوك غير الطبيعي (وإعادة التهيئة أو الاسترداد) والتحديث الدوري للنظام للوصول إلى الحالة الموثوقة و السليمة وأيضاً من المهم تأمين كل العناصر الحساسة داخل المتحكم مثل مفاتيح التشفير.

- الهجوم على نقاط ضعف محطات الإدارة:

والتي عادة تكون موجودة ضمن الشبكات التقليدية، تستخدم هنا أيضاً في شبكات SDN للنفاذ إلى المتحكم في الشبكة، لكن الفرق في أنه إذا تعرض جهاز أو محطة إدارة فقط للخطر فإن هذا الخطر سوف يزداد في شبكات SDN حيث سيكون من السهل إعادة برمجة الشبكة وذلك من مكان واحد.

الحل المقترح: استخدام البرتوكولات التي تتطلب التحقق المزدوج (مثال على ذلك طلب النفاذ إلى المتحكم يتطلب تفويضاً من قبل شخصين اثنين)، أيضاً استخدام آليات استرداد مضمونة لضمان حالة موثوقة بعد إعادة التشغيل.

هجمات الحرمان من الخدمة (Denial of Service Attacks):

هذه الهجمات هي من أكثر الهجمات خطورة على شبكة الانترنت تهدد الدول والحكومات ،وكل الشبكات عرضة لهجوم الحرمان من الخدمة وانهيار أجهزتها.

هذه الهجمات تصنف الى قسمين:

١- هجمات الحرمان من الخدمة (DOS – Denial Of Service Attacks)

٢- هجمات الحرمان من الخدمة الموزع (DDOS – Distributed Denial Of Service Attacks)

هجمات DOS :

إن هجوم منع الخدمة DOS في شبكات SDN ينطوي على موارد بحيث يتعذر على المبدلات SW إعادة توجيه الحزم كما هو متوقع ، ويتضمن الهجوم الناجح إرسال عدد كبير من الحزم إلى المبدل وربما إنشاء تدفقات جديدة.

هجمات DDOS :

تعد هجمات منع الخدمة الموزعة DDOS محاولة خبيثة لاستنزاف موارد الحاسب أو الشبكة عن طريق إرسال أعداد ضخمة من الطرود، كما يمكن للمهاجم زرع العديد من التطبيقات الخبيثة في الشبكة للقيام بمثل هذه الهجمات. يتم هذا الهجوم من عدة مهاجمين في نفس الوقت أو باستخدام Botnet . (حيث أن BOTNET هو شبكة من أجهزة الحاسوب الخاصة ،والمصابة ببرامج ضارة ويتم التحكم فيها كمجموعة دون علم المالكين لإرسال رسائل عشوائية) .

حيث يكون لدى المهاجم هدفين أساسيين وهما:

ا. استخدام كامل عرض الحزمة Band Width

اا. استنزاف الموارد.

يبدأ الهجوم من خلال زرع المهاجم لكود برمجي خبيث في أجهزة الحاسوب والتي يشار إليها باسم Botnet ، وعند بدء الهجوم يتم تشغيل هذه البرمجيات ويتم توجيه سيل من الطرود نحو الهدف ، كما يوجد نوع معقد أكثر لهذه الهجمات حيث يقوم المهاجم باستخدام عدد من الحواسيب المصابة بالفايروس ونسميها handler للتحكم بعدد ضخم من الحواسيب نسميها zombie إذ تعد الحواسيب المصابة مسؤولة عن توليد حركة مرور المهاجم وباستخدام Botnet يكون المهاجم أكثر تركيزاً ويحافظ على نفسه متخفياً عن برمجة الكشف.

الفرق بين DOS و DDOS :

هجوم منع الخدمة DOS : هو هجوم يهدف إلى جعل الضحية خارج الخدمة ، وذلك عن طريق إغراقه بعدد كبير من الطلبات بحيث تجعله غير قادر على الاستجابة لطلبات المستخدمين العاديين .

هجوم منع الخدمة الموزع DDOS : مشابه لهجوم منع الخدمة من حيث الهدف ؛ إلا أنه يختلف عنه من حيث آلية العمل ، حيث يتعاون أكثر من جهاز لإنجاز الهجوم على هدف واحد ، ويتم التحكم بالأجهزة التي تقوم بالهجوم عن طريق برنامج من قبل المهاجم .

أنواع هجمات DDOS :

يتطلب البدء بأية هجوم النفاذ إلى الشبكات الفرعية للضحايا لاستخدامها مثل Zombie ، ويقوم المهاجم بإجراء عمليات مسح لإيجاد الحواسيب الضعيفة في الشبكة ، وتكون عملية المسح هذه عشوائية أو اعتماداً على قائمة معينة ، أو عملية مسح للشبكة المحلية الفرعية ، أو من خلال خوارزمية يقوم المهاجم بتصميمها .

- ❖ يمكن تصنيف الهجمات بناءً على التطبيق أو المضيف أو المورد أو الشبكة أو هجمات البنية التحتية:
- (a) التطبيق : يتم استهداف التطبيق في المضيف لمنع استخدامه .
- (b) المضيف : يتم جعله غير متاح .
- (c) الموارد : يتم من خلال اشغاله بمعالجة تدفق ضخم من الطلبات المزيفة.
- (d) الشبكة : يتم استنزاف عرض حزمة الشبكة من خلال ارسال احجام ضخمة من المعطيات إلى الشبكة.
- (e) البنية التحتية : يتم استخدام مخدم DNS : Domain name server بشكل متزامن من عدة أماكن.

❖ يمكن تصنيف هجمات DDOS على SDN إلى ثلاث فئات :

١. هجمات DDOS لطبقة التطبيقات .
 ٢. هجمات DDOS لطبقة التحكم .
 ٣. هجمات DDOS لطبقة البنية التحتية .
- (١) هجمات DDOS لطبقة التطبيقات :

هناك طريقتان لإطلاق هجمات DDOS لطبقة التطبيقات:

مهاجمة التطبيقات أو مهاجمة واجهة برمجة التطبيقات الشمالية ، نظراً لأن عزل التطبيقات أو الموارد في SDN لم يتم حله جيداً.

يمكن أن تؤثر هجمات DDOS على أحد التطبيقات على التطبيقات الأخرى .

(٢) هجمات DDOS لطبقة التحكم :

من المحتمل النظر إلى وحدات التحكم على أنها نقطة خطر تسبب حدوث فشل للشبكة ، لذا فهي هدف جذاب بشكل خاص لهجمات DDOS في بنية SDN.

يمكن للطرق التالية التسبب في هجمات DDOS لطبقة التحكم :

مهاجمة وحدة التحكم أو واجهة التطبيقات الشمالية أو الجنوبية أو واجهة برمجة التطبيقات الغربية أو الشرقية .

(٣) هجمات DDOS لطبقة البنية التحتية :

هناك طريقتان لظهور هجمات DDOS لطبقة البنية التحتية :

مهاجمة المبدلات أو مهاجمة واجهة برمجة التطبيقات الجنوبية .

❖ هجمات الحرمان من الخدمة Denial Of Serves Attack : هذا النوع من الهجمات يدعى في بعض الأوساط ((إيدز الانترنت)) بسبب أنه ليس له علاج حتى الآن ، مهما بلغت مواصفات الهدف وسرعته وقدرته على المعالجة واستقبال الطلبات يبقى ضمن رقم محدود من الطلبات مهما كان كبيراً، حيث لا يستطيع أن يستقبل طلبات أكثر من ذلك العدد ، فتبقى هذه الهجمات أكثر الهجمات خطورة على شبكة الانترنت .

أنواع هجمات DOS و DDOS :

يمكن تقسيم هجمات DDOS لطبقة التطبيقات إلى ثلاثة أنواع :

A. الهجمات على أساس الحجم :

يتضمن فيضانات UDP وفيضانات ICMP وغيرها من فيضانات الحزم المخادعة .
هدف الهجوم هو تشبع النطاق الترددي للموقع المهاجم ، ويتم قياس الحجم البت بالثانية BPS .

B. هجمات البرتوكول :

يتضمن فيضانات SYN وهجمات الحزم المجزأة و ping of Death و Smurf DDOS يستهلك هذا النوع من الهجوم موارد المخدم الفعلية أو تلك الخاصة بمعدات الاتصال الوسيطة مثل جدران الحماية وموازنة الحمل ويتم قياسه بالحزم في الثانية PPS.

C. هجمات التطبيق :

يتضمن الهجمات المنخفضة والبطيئة ، وفيضانات GET/POST ، والهجمات التي تستهدف نقاط ضعف Apache أو windows أو .
OpenBSD

وتتألف من طلبات تبدو مشروعة وبريئة والهدف من هذه الهجمات هو تعطيل مخدم الويب ، ويتم قياس الحجم بالطلبات بالثانية RPS.

هجمات DDOS الشائعة :

١. UDP flood
٢. ICMP flood
٣. SYN flood
٤. Ping of Death
٥. Slowloris
٦. تضخيم NTP
٧. فيضان HTTP
٨. Fragmentation

❖ الهدف الأساسي للمهاجمين هو :

- a. الايديولوجيا : يستخدم الهاكرز هجمات DDOS كوسيلة لاستهداف مواقع الويب التي يختلفون معها ايديولوجياً.
- b. الابتزاز : يستخدم الجناة هجمات DDOS ، او التهديد بهجمات DDOS كوسيلة لابتزاز الأموال من أهدافهم.
- c. الحرب الالكترونية : يمكن استخدام هجمات DDOS المصرح بها من قبل الحكومة لتعطيل مواقع الويب الخاصة بالمعارضة والبنية التحتية لدولة معادية.

أدوات الهجوم :Attacking tools:

يقوم المهاجم بزرع أدوات في الأجهزة المعدة للهجوم ليقوم باستخدامها في تنفيذ هجوم حجب الخدمة . وكما قلنا فإن هنالك العديد من الأدوات ، فلا حاجة لأن يقوم المهاجم بتطوير أدوات خاصة به .

Trin00 و Tribe Flood Network (TFN) اول ظهور كان

ثم توالى بعدها ظهور أدوات أخرى مثل TFN2K و Stacheldraht و Eggdrop وغيرها من التي تنتوع في المواصفات وإمكانيات الهجوم.

اكتشاف ومنع أدوات الهجوم :

يجب التأكد من أن الجهاز غير مصاب بثغرة أمنية ولا توجد به أي من أدوات الهجوم المستخدمة لحجب الخدمة.

الخطوات المهمة دائماً هي: استخدم برامج مكافحة الفيروسات والجدران النارية وجميع البرامج محدثة باستمرار

إن الكثير من هذه الأدوات تستخدم طرقاً متقدمة للتخفي، فلا يشعر المستخدم بوجودها.

وأيضاً تستخدم التشفير في ترسل البيانات بينها. أمر آخر يجعل ملاحقة مصدر الهجوم أكثر صعوبة ، هو أنها ترسل حزم البيانات بعنوان مصدر مزيف لذلك ينصح مدراء الشبكات بعمل إعدادات خاصة للموجهات routers بحيث لا تقوم بالسماح بمرور حزم البيانات التي عنوان المصدر الخاص بها ليس ضمن الشبكة ولكنها ستساعد في تخفيفها وتجعل تعقبها أمراً ممكناً .

- أيضاً هنالك أدوات مساعدة خاصة تساهم في اكتشاف ما إذا كانت أجهزة الشبكة تستخدم في تنفيذ هجوم حجب الخدمة. من هذه الأدوات find_ddos31 من national international protection center و ddos_scan و rid وغيرها من الأدوات.

مقاومة هجوم حجب الخدمة:

منذ بداية ظهور هذه الهجمات حاول الكثيرون اتخاذ اجراءات للدفاع ضدها لكن وبالرغم من بذل الكثير من الجهود في هذا المجال يبقى خطر هذه الهجمات قائماً .. ولقد حاول الخبراء تصنيف طرق الدفاع والتي تقسم إلى طرق وقائية وطرق تفاعلية.

الطرق التفاعلية: حيث يتم التقليل من احتمال التعرض لهجوم حجب خدمة او على الاقل جعل الضحايا

المستهدفين يستمرون في تقديم الخدمات للمستخدمين الشرعيين بالرغم من تعرضهم للهجوم

الطرق الوقائية: حيث يتم محاولة اكتشاف الهجوم مبكراً والاستجابة له بالحال. مما يخفف تأثير الهجوم على الضحية. لكن هنالك خطر من امكانية تصنيف طلب مستخدم شرعي على انه هجوم حجب خدمة وهو ما يدعو الى الحذر الشديد في تصنيف الحزم على انها حزم هجوم.

يمكن اكتشاف الهجوم بعدة طرق منها:

١- يمكن اكتشاف الهجمات التي لها طابع مميز او نموذج معين وهو ما يسمى توقيع (signature) حيث يتم مقارنة كل حزمة مع قاعدة بيانات تحوي نماذج لهجمات معروفة .

٢- احيانا يتم اللجوء الى طريقة اخرى لاكتشاف الهجوم : تكون هذه الطريقة بمراقبة مرور البيانات ومقارنتها مع نموذج للمرور الطبيعي للبيانات في الاوضاع العادية ، تسمى هذه الطريقة Anomaly وإذا زاد حجم البيانات بشكل مميز عن النموذج الطبيعي يتم اعتبار الشبكة تحت حجب خدمة.

٣- يمكن دمج الطريقتين اعلاه واستخدامهما في وقت واحد.

بعض الحلول لهجوم DDoS:

الهجمات على اساس الحجم:

الحل لهذه الهجمات يتم من خلال استيعابها بشبكة عالمية من مراكز التنظيف التي تتوسع حسب الطلب لمواجهة هجمات DDoS متعددة الجيجابايت.
هجمات البروتوكول:

الحل لهذا النوع من الهجوم منع حركة المرور "السيئة" حتى قبل وصولها الى الموقع والاستفادة من تقنية تحديد هوية الزائر التي تميز بين زوار الموقع الشرعيين(البشر ومحركات البحث وما الى ذلك) والعملاء الآليين او الخبثاء

هجمات طبقة التطبيقات:

الحل لهذه الهجمات يتم من خلال مراقبة سلوك الزائر ، وتحدي الكيانات المشبوهة او غير المعترف بها باستخدام اختبار JS وتحدي ملفات تعريف الارتباط وحتى اختبارات CAPTCHA

نصائح للتعامل مع هجوم حجب الخدمة:

إضافة الى ما ذكر فيما يخص اكتشاف ومنع ادوات الهجوم فانه ينصح القيام بالأمر التالية للتعامل مع هجوم حجب الخدمة:

- التدريب للطوارئ: يجب ان يكون المسؤولون عن الشبكة مؤهلين و مدربين جيدا
- تقوية البنية التحتية للشبكة والانظمة الموجودة بها
- التأكد من وضع اعدادات مناسبة لأجهزة الشبكة وبالخصوص الموجهات routers
- استخدام المرشحات filters وهي ادوات قادرة على الغاء حزم البيانات اي تكون مطابقة لنماذج او شروط معرفة مسبقا يمكن وضع هذه المرشحات في عدة اجهزة مثل :
- الموجهات : routers عادة يتم استخدام Access Control list (ACL) قائمة ضبط الوصول في الموجهات وهي غير كافية لمواجهة هجوم حجب الخدمة .ذلك لأنها لا تقوم بفحص ترويسة header كل حزمة قادمة لكن في المقابل فان تركيب المرشحات على موجه يسبب ذلك تأثيراً كبيراً في الاداء وقد لا يكون من مهام الموجه فحص ترويسة كل حزمة قادمة
- الجدران النارية : firewalls وتركيب المرشحات هنا افضل لان جدار النار يقوم بفحص كل حزمة تمر من خلاله

- أجهزة مخصصة لمكافحة الهجوم : وهي بالطبع الافضل فهي تجمع طرق مختلفة للدفاع وانماط متعددة للترشيح .وتكون مهمتها متخصصة للتصدي لهجوم حجب الخدمة فقط. ولأنها تقوم بفحص كل حزمة وعمل مقارنات متعددة فإنها يجب ان تكون قادرة على تحمل معدل كبير لمرور البيانات
- اتباع سياسات امنية قوية: بعد وقوع هجوم حجب خدمة لا بد من القيام بتحليله (معرفة نوع البروتوكول المستخدم، مصادر الهجوم، نوع حزم البيانات ، الطرق المتبعة في الهجوم ...الخ) ومن ثم الاستفادة من نتائج التحليل لزيادة الامن وتحديث المرشحات وضبط الاعدادات.
- load balancing:

توزيع الحمل بين الاجهزة التي تقدم الخدمات.

- الحصول على سعة حزمة bandwidth اكبر واستخدام اجهزة اكثر .

التطبيق العملي :

التطبيق العملي عبارة عن تنفيذ هجوم DDOS على المتحكم ليكشف حدوث الهجمات وحظر IP المهاجم .

وتم التطبيق العملي باستخدام المحاكى mininet وهو محاكي ينشئ شبكة من المضيفات الظاهرية والمبدلات والمتحكمات والروابط .

تستطيع مضيفات mininet تشغيل برامج Linux القياسية كما تدعم مبدلاته البروتوكول openflow لتحقيق توجيه مخصص للرزق عالي المرونة .

يدعم mininet البحث والتطوير والتعلم والنماذج الأولية والاختبار وتصحيح الأخطاء وأي مهام أخرى من خلال تقديم شبكة كاملة على الكمبيوتر المحمول أو أي جهاز آخر.

والمتحكم POX هو من المتحكمات الهامة والشهيرة في SDN وقد تمت برمجته بلغة البايثون كما أنه يوفر منصة برمجية سهلة ومرنة لكتابة التطبيقات التي يمكن تنفيذها في الشبكة والمتحكم POX مكتوب بلغة البايثون لذلك للتعامل مع هذا المتحكم نكتب Python Script ليقوم بالوظائف البرمجية المطلوبة (تنفيذ هجوم ، اكتشاف هجوم ، التصدي للهجمات)

تنفيذ الهجوم:

لتحقيق هجمة DDOS استخدمنا الأداة hping3 وهي أداة شبكة قادرة على إرسال حزم TCP/IP مخصصة وعرض الردود .

يمكن كتابتها في سطر الأوامر في Linux مع تحديد البارامترات المناسبة لتحقيق الهجمة منها البارامترات:

• S-Syn

تحديد لإرسال SYN tcp .

• V-verbose

تمكين الإخراج المطول ستظهر ردود TCP كما يلي :

Len=46 ip=192.168.1.1 flags=RADF seq=0 ttl=225 id=0 win=0 rtt=0.4ms

tos=0 iplen=40 seq=0 ack=1380893504 sum=20 urp=0

• I-interval

انتظر العدد المحدد من الثواني بين إرسال كل حزمة الزمن الافتراضي

• -p-destport[+][+]dest port

عَيّن منفذ الوجهة القيمة الافتراضية هي 0 إذا كان الحرف "+" يسبق رقم منفذ النقل فستتم زيادة منفذ الوجهة لكل رد يتم استلامه.

- C-count

توقف بعد إرسال وتلقي حزم استجابة العد

- --spoofhostname

استخدم هذا الخيار لتعين عنوان IP مزيف ، يضمن هذا الخيار ألا يكتسب الهدف عنوانك الحقيقي

.ومع ذلك سيتم إرسال الردود إلى العنوان المخادع لذلك لن تتمكن من رؤيتها.

لتحقيق الهجمة تم كتابة ال script التالي :

```
def _timer_printer():
    cout_ip=random.randint(0,80)
    rand_time_loop=random.uniform(1,3)
    pack='.'.join(['%s'%random.randint(0, 200), '%s'%random.randint(0, 255) for i in range(3)])
    os.system("hping3 -S -V -p 80 -i u1 -c %s --spoof %s 10.10.1.3 " %(cout_ip,pack))
    print "hping3 -S -V -p 80 -i u1 -c %s --spoof %s 10.10.1.3 " %(cout_ip,pack)

threading.Timer(rand_time_loop,_timer_printer).start()
```

اكتشاف الهجوم:

يتم تشغيل المتحكم POX مع هذا ال script DDOS الذي يحوي على التعليمات اللازمة لاكتشاف الهجوم وقد تم الاعتماد على فكرة مراقبة عدد ال packets القادمة من ال IP وعددها .

في المقطع البرمجي التالي يتم احصاء عدد ال packets القادمة :

```
# Get number of bytes/packets in flows for web traffic only
web_packet = {}
last_Packet_count=0
for f in event.stats:
    if f.match.tp_dst==80:
        if web_packet.has_key(str(f.match.nw_src)):
            last_Packet_count= web_packet[str(f.match.nw_src)]
            web_packet[str(f.match.nw_src)] = last_Packet_count + f.packet_count
            last_Packet_count=0
        send_packet(event,str(f.match.nw_src),web_packet)
```

التابع send-packet يختبر أولاً اذا ال IP ضمن قائمة ال IPs المحظورة ليتجاوز اختبار عدد ال Packets .

إيقاف الهجوم :

ضمن التابع send-packet عندما يتم استقبال packet من الـ IP بمعدل أكبر من حد يتم تحديده بالبرنامج ويتم حظر هذا الـ IP كما هو موضح في المقطع البرمجي التالي :

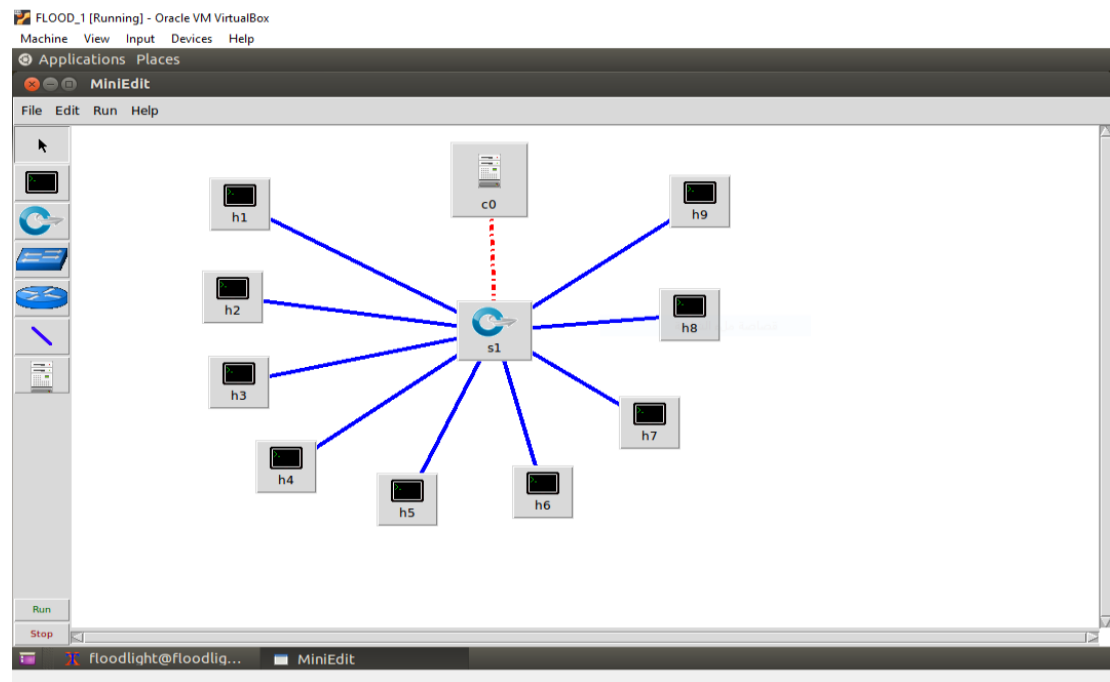
```
def send_packet(event,src_ip,web_packet):
    global srcip_count
    global srcip_blocked
    global rate_limit
    skip_loop=0
    if srcip_blocked:
        for i in srcip_blocked:
            if i==src_ip:
                skip_loop=1
    if skip_loop==0:
        srcip_count[src_ip]=web_packet[src_ip]
        global tmp_src_ip
        tmp_src_ip=None
        srcip_count1=srcip_count

    # If an user exceeds the threshold
    for i in srcip_count:
        if srcip_count[i]>rate_limit:
            tmp_src_ip=i
            log.debug("packet-rate exceeded for %s. redirect the packets.",i)

    # Add a flow to block the user
    for connection in core.openflow._connections.values():
        connection.send( of.ofp_flow_mod(match=of.ofp_match(
            nw_proto=6,d1_type=0x800,nw_src=i,nw_dst="10.10.1.0/24",tp_dst=80 )))
    log.debug("Host %s blocked and removed from the list",i)
    if tmp_src_ip :
        srcip_blocked[tmp_src_ip]="Blocked"
        print "Host %s blocked and removed from the list"%(tmp_src_ip)
        srcip_count[tmp_src_ip]="Blocked"
        tmp_src_ip=None
```

الآن أصبح لدينا مقطع برمجي لتنفيذ الهجوم يتم تشغيله من أحد المضيفين في الشبكة ومقطع برمجي لكشف وصد الهجوم يتم تشغيله على المتحكم POX .

لتنفيذ التطبيق تم انشاء شبكة مكونة من متحكم ومبدل و 9 مضيفين باستخدام المحرر miniedit :

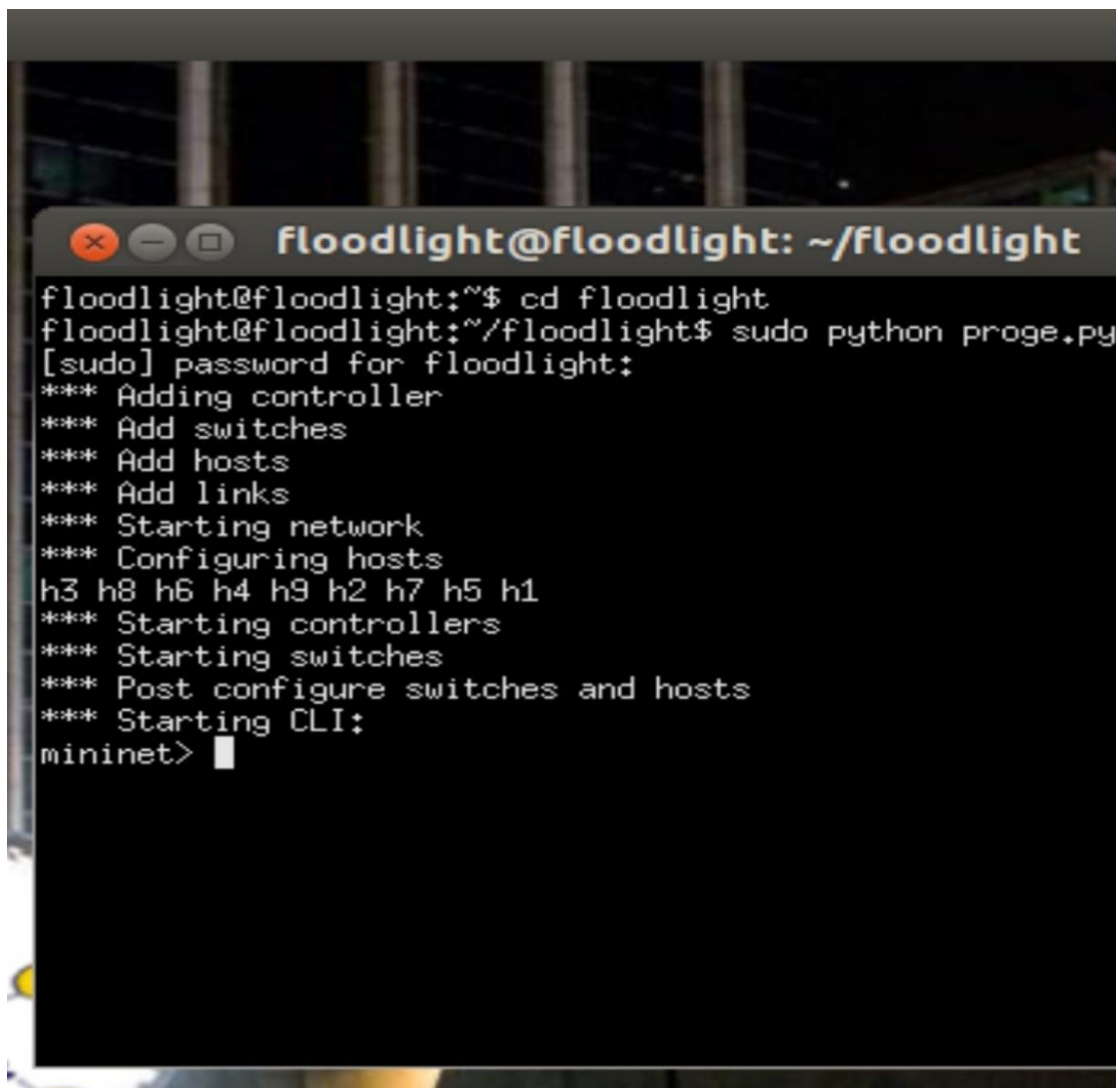


عند الضغط على الزر run يتم تشغيل الشبكة و إنشاء العقد:

```
Applications Places

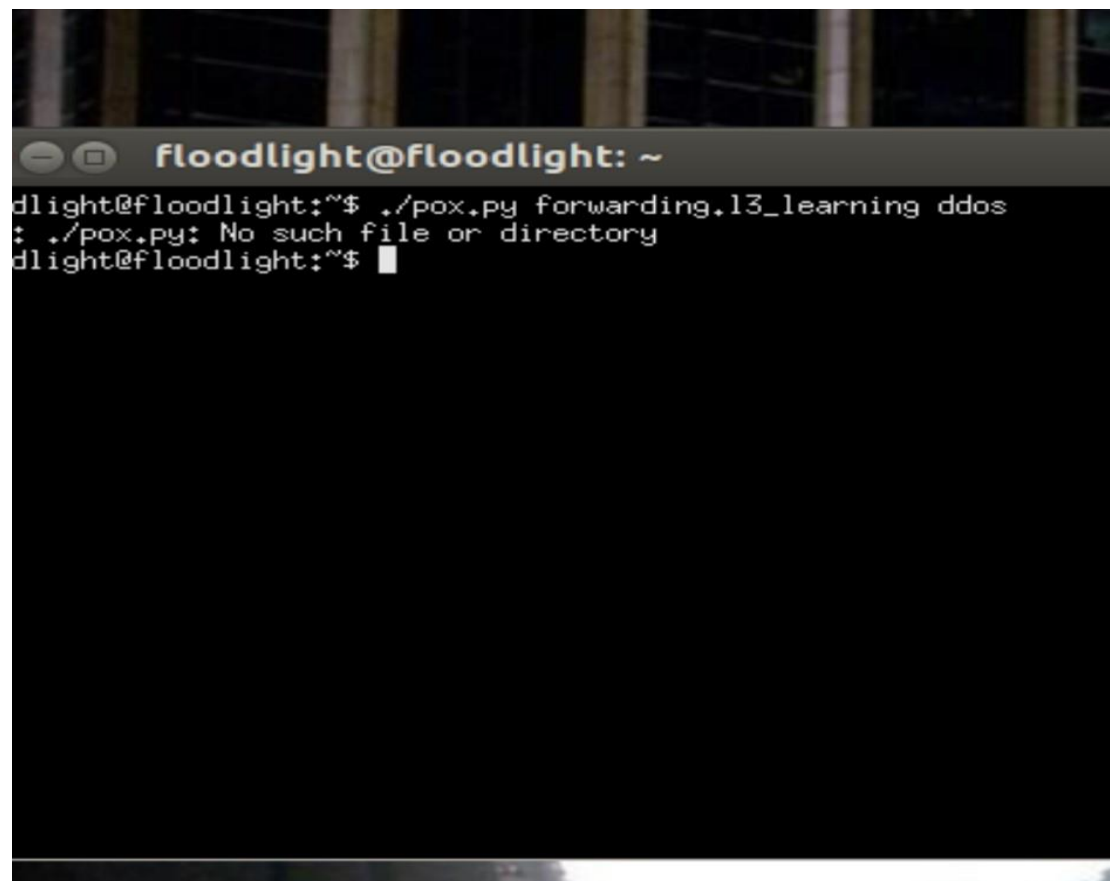
floodlight@floodlight: ~/floodlight

floodlight@floodlight:~/floodlight$ sudo python miniedit.py
[sudo] password for floodlight:
topo=None
Getting Hosts and Switches.
Getting controller selection:ref
Getting Links.
*** Configuring hosts
h3 h8 h6 h4 h9 h2 h7 h5 h1
**** Starting 1 controllers
c0
**** Starting 1 switches
s1
No NetFlow targets specified.
No sFlow targets specified.
*** Stopping 1 controllers
c0
*** Stopping 9 links
*****
*** Stopping 1 switches
s1
*** Stopping 9 hosts
h3 h8 h6 h4 h9 h2 h7 h5 h1
*** Done
□
```

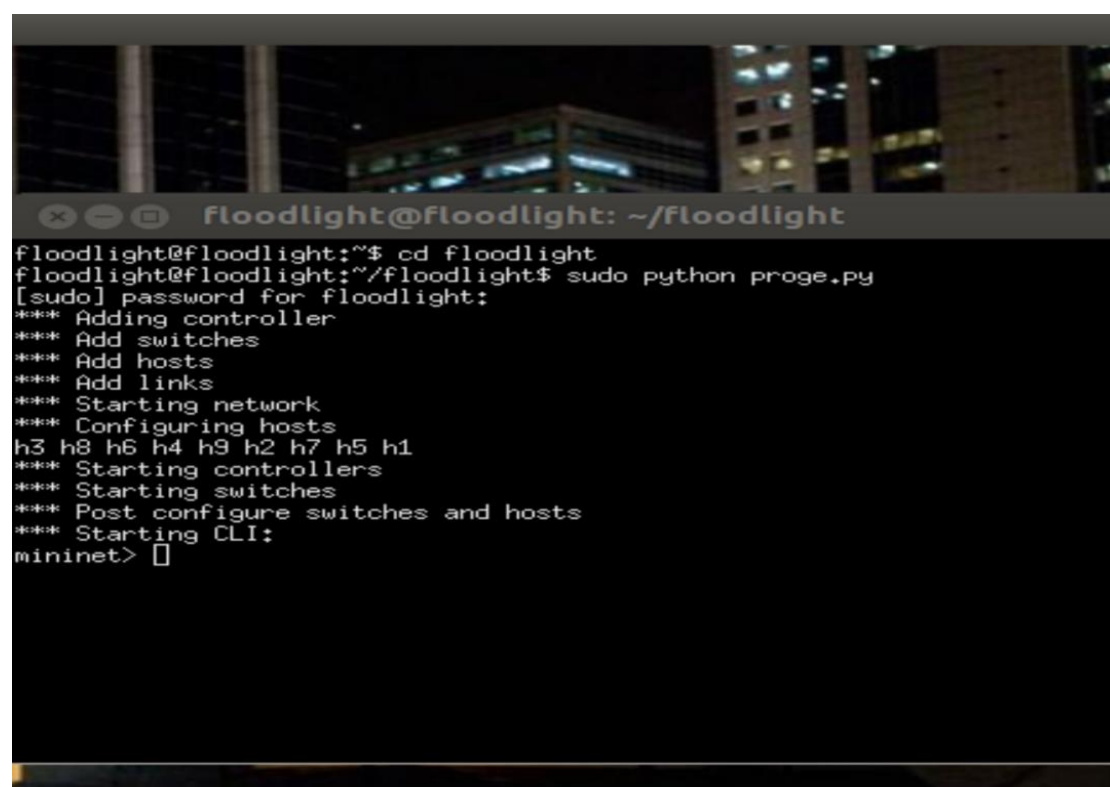
A terminal window titled 'floodlight@floodlight: ~/floodlight' is shown. The user enters 'cd floodlight' and then 'sudo python proge.py'. After entering the password, the script runs several commands: 'Adding controller', 'Add switches', 'Add hosts', 'Add links', 'Starting network', 'Configuring hosts', 'Starting controllers', 'Starting switches', 'Post configure switches and hosts', and 'Starting CLI:'. The output shows a list of hosts: 'h3 h8 h6 h4 h9 h2 h7 h5 h1'. The prompt changes to 'mininet>'.

في Terminal جديدة نكتب الأمر اللازم لتشغيل المتحكم POX مع برنامج DDOS من خلال التعليمة :

./pox.py forwarding.l3_learning ddos

A terminal window titled 'floodlight@floodlight: ~' with a dark background and a window icon on the left. The terminal shows a user attempting to run a command, which fails with an error message.

```
floodlight@floodlight: ~  
floodlight@floodlight:~$ ./pox.py forwarding.l3_learning ddos  
: ./pox.py: No such file or directory  
floodlight@floodlight:~$
```

A terminal window titled 'floodlight@floodlight: ~/floodlight' with a dark background and window icons on the left. The terminal shows a user navigating to a directory and running a script with sudo, followed by a series of status messages and a CLI prompt.

```
floodlight@floodlight: ~/floodlight  
floodlight@floodlight:~$ cd floodlight  
floodlight@floodlight:~/floodlight$ sudo python proge.py  
[sudo] password for floodlight:  
*** Adding controller  
*** Add switches  
*** Add hosts  
*** Add links  
*** Starting network  
*** Configuring hosts  
h3 h8 h6 h4 h9 h2 h7 h5 h1  
*** Starting controllers  
*** Starting switches  
*** Post configure switches and hosts  
*** Starting CLI:  
mininet>
```

من خلال التعليمات السابقة يجب تشغيل متحكم POX وفتح Host4 ذو الـ IP: 10.0.1.5

لتشغيل الهجمة من أحد المضيفين نفتح Terminal في المضيف ونكتب الأمر التالي :

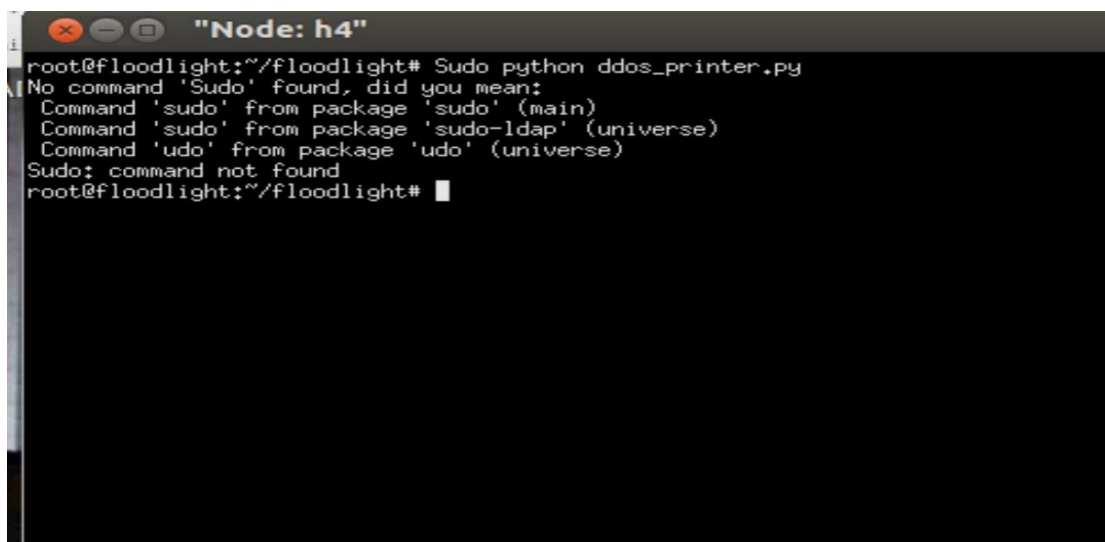
Sudo python ddos_printer.py

حيث **ddos_printer.py** هو اسم الـ Script الذي كتبناه :



```
floodlight@floodlight:~$ cd floodlight
floodlight@floodlight:~/floodlight$ sudo python proge.py
[sudo] password for floodlight:
*** Adding controller
*** Add switches
*** Add hosts
*** Add links
*** Starting network
*** Configuring hosts
h3 h8 h6 h4 h9 h2 h7 h5 h1
*** Starting controllers
*** Starting switches
*** Post configure switches and hosts
*** Starting CLI:
mininet> xterm h4
mininet>
```

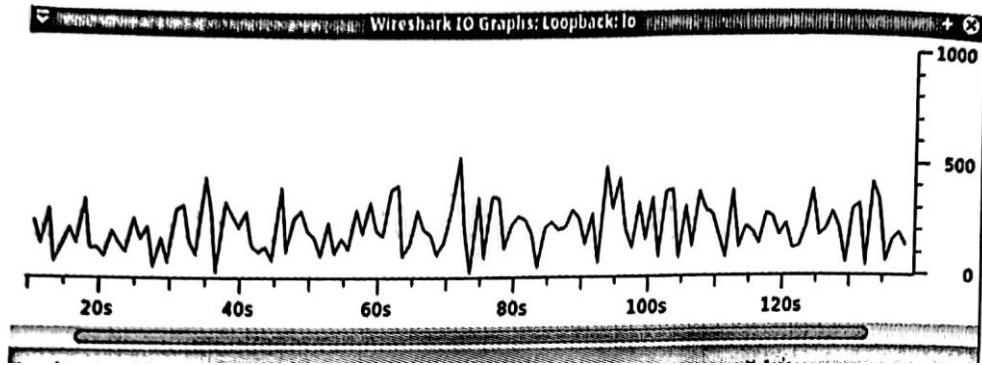
وواجهنا هذا الخطأ:



```
root@floodlight:~/floodlight# Sudo python ddos_printer.py
No command 'Sudo' found, did you mean:
Command 'sudo' from package 'sudo' (main)
Command 'sudo' from package 'sudo-ldap' (universe)
Command 'udo' from package 'udo' (universe)
Sudo: command not found
root@floodlight:~/floodlight#
```

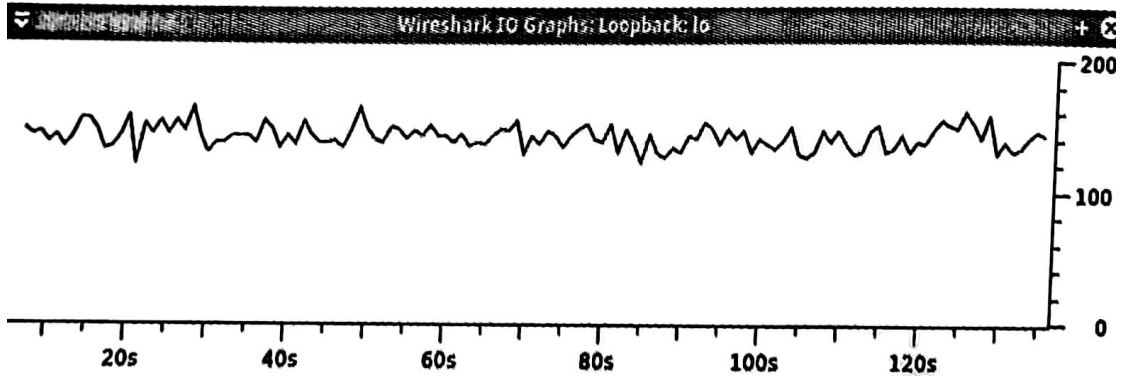
لاختبار فعالية هذه الطريقة في اكتشاف وصد الهجوم تم تنفيذ الهجمة في كل المضيفات ومراقبة الحمل الحاصل على المتحكم في حالتين :

1 - تشغيل المتحكم بدون برنامج كشف وصد الهجمة:



نلاحظ أن معدل الـ Packets يتراوح بين الـ 200—500 Packet/sec مع وصول للقيمة (0)، في بعض الأحيان بسبب فقدان الرسائل المرسله وعدم وصولها للمتحكم .

2 - تشغيل المتحكم مع برنامج كشف الهجوم وإيقافه :



نلاحظ أن معدل الـ Packet يتراوح بين الـ 240--260 Packet/sec ولا نلاحظ أبداً وصول للقيمة للصفر ويعود السبب الى أن الـ Script كشف الهجمة .

الاستنتاجات والتوصيات :

للإجابة على السؤال هل SDN آمن ؟ في هذه المرحلة من المرجح أن تكون الإجابة غير حقيقية.

قد يكون من الممكن الحصول على شبكة SDN آمن دون أي اتصال خارج حدود الثقة المحددة ، ووفقاً لأشد مبادئ الأمان تشدداً، ومع ذلك لن يعكس هذا النشر سوى مجموعه فرعيه من خصائص SDN وعلى هذا النحو سيكون محدوداً مقارنةً بإمكانيات SDN وأنه من الممكن تحسين أمان الشبكة باستخدام خصائص بنية SDN .

الاستنتاج هو ان العمل على تحسينات أمان الشبكة عبر SDN هو أكثر نضجاً يتضح هذا من خلال التطبيقات المتاحة . ومع ذلك، فقد تم تقديم حلول بحثية لمعالجة بعض المشكلات الأمنية التي طرحها SDN ، على سبيل المثال كيفية الحد من الضرر المحتمل من تطبيق ضار .

المراجع :

- 1-Ahmad Sonba , Hassan Abdalkreim "Performance Comparison Of the state of the state of the art Openflow Controllers ".
- 2-Nick Feamster , Jennifer Rexford , Ellen Zegura,"The Road to SDN :An Intellectual History of Programmable Networks".
- 3-F . D . O .Silva , j .H.d.S.Perrira ,p.F . Rosa, and S.T.Kofuji,"Enabling Future internet Architecture Research and Experimentation by Using Software Defined Networking".
- 4-H.Kim and N.Feamster."improving Network Management with Software Defined Networking "