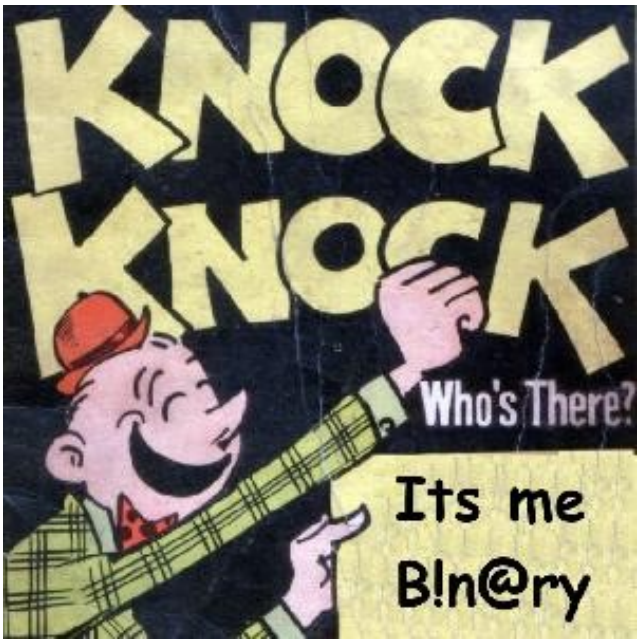
Port Knocking – using Knockd

السلام عليكم ورحمة الله وبركاته



اليوم في حياتنا الواقعية حين ترجع الى منزلك بعد العودة من الخارج تقوم بالدق على الباب لمنزلك لكي يقوم من في المنزل من أهلك (**حفظهم الله لك**) بفتح الباب لك بعد سؤالهم: من أنت؟ وتجيب أنا فلان وتدخل ...

حين تذهب لزيارة صديق تدق على الباب الخاص ببيته ... وربما يرد عليك سائل: من أنت؟ ... وستقول أنا فلان الفلاني ... ومن ثم يفتحون لك الباب وتدخل ...

بعض الأحيان تكون بينك وبين أخوك/صديقك/زميلك بالعمل إشارة معينة بينكما ... وعلى ضوء هذه الإشارة تقوم بعمل تصرف معيين ... يعني مثلاً:
تقوم بالدق على الباب ثلاث مرات متتالية وبسرعة ... هنا يفهم الطرف الآخر بإن الذي على الباب هو أنت وليس شخص آخر ...

أو
تقوم بالدق على الخشب دقة معينة ... هنا يعرف الطرف الآخر بإن على سبيل المثال هناك من جاء ولا تريدوه أن يسمع كلامكم ...

والأمثلة كثيرا ...

هذه الإشارة التي بينك وبين الآخرين هي إشارة لا يفهم ما الغرض منها سواكم ... أي لن يفهمها سواك أنت والطرف الآخر (أخوك/صديقك/زميلك بالعمل) من الهدف منها ...

من هنا جائت فكرة الـ Port Knocking ... جميع السيناريوهات التي أخذناها هي من واقع حياتنا ... الآن لنأخذ كيف تم تطبيق هذه الفكرة على الحياة التكنلوجية وبالتحديد الحواسيب ...

لنفرض بإن هناك مدير شبكة/مدير أنظمة (**Admin**) وهو خارج العمل وأحتاج الى الوصول الى جهازه بداخل العمل ... والمشكلة بإن جميع المنافذ من الخارج مغلقة ... يعني جميع الـ **packets** التي ستصل الى الجدار الناري الخاص بالشركة/العمل يتم عمل **BLOCK** لها من ثم **DROP** ... طيب حتقول لي مهو يعمل **DROP** لكل شيء بإستثناء الـ **IP** الذي يدخل منه المدير هذا ؟ الجواب وماذا لو كان المدير هذا في مكان آخر (مسافر) غير الذي يتصل من خلاله كل مرة ... كيف سيدخل الى الداخل ؟

هنا يأتي دور الـ Port Knock ... حيث يتم تركيب برنامج **daemon** على احد الأجهزة التي تريد أن تتصل بها من الخارج ... لنفرض هو نفسه الـ **GW** ... الآن هذا البرنامج يقوم بقراءة الـ **LOG** وحين يرى بإن هناك مثلا عملية مسح **SCAN** على منافذ معينة يقوم بإضافة rule الى الـ **iptables** تفتح منفذ وممر لهذا الشخص للدخول الى النظام ... مثلا يقوم بالدق على المنافذ 3000 5000 7000 والتي سيقوم الجدار الناري بستجيلها في الـ **LOG** والبرنامج بما إنه يقرا هذه الـ **LOG** سيقوم على ضوئها بإضافة الأمر الذي يتيح للشخص الذي عمل هذه الدقات بالدخول الى النظام ... طبعا هذه هي الطريقة التقليدية للـ Port Knock هناك طرق أكثر متقدمة من هذه لكنها خارج نطاق هذا الشرح ...

الآن لنقم بعمل تجربة بسيطة أوضح لكم الفكرة بطريقة عملية ... حيث سنقوم بعمل دق على السيرفر الذي عليه برنامج الـ **PK** وحين يتعرف على الدقات الخاصة بنا يسمح لنا بإستعمال الـ **SSH** أي سيفتح لنا ممر أو منفذ للوصول الى خدمة الـ **SSH** من خلال المنفذ رقم 22 ... اول شيء سنقوم بتركيب برنامج الـ Knockd على النظام جنو/لينوكس (توزيعة فيدورا/أوبنتو)

لتركيبه على فيدورا قمت بعمل بناء للحزم وذلك لأنه الموقع الرسمي لا يقدمها بشكل جاهز ولهذا قم بتحميلهم من الروابط التالية:
Server
Client
Debug

لتركيبه على توزيعة أوبنتو قم بعمل التالي:
كود:

```
apt-get install knockd
```

الآن لنقم بعمل إعدادات للجدار الناري عندك لعمل التجربة:
كود:

```
iptables -F
iptables -X
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -t nat -F
iptables -t nat -X
```

الآن تأكد من إعداداتك الجدار الناري:
كود:

```
iptables -L -n
```

الآن لنفتح ملف الإعدادات الخاص بالخدمة:
كود:

```
vi /etc/knockd.conf
```

وتأكد من وجود الإعدادات التالية:
كود:

```
[options]
        UseSyslog

[opencloseSSH]
        sequence      = 2222:tcp,3333:tcp,4444:tcp
        seq_timeout   = 15
        tcpflags      = syn,ack
        start_command = /sbin/iptables -I INPUT 1 -s %IP% -p tcp --dport ssh -j ACCEPT
        cmd_timeout   = 10
        stop_command  = /sbin/iptables -D INPUT -s %IP% -p tcp --dport ssh -j ACCEPT
```

لمستخدمي أوبنتو عليك تحرير ملف آخر ولهذا قم بفتح الملف التالي:
كود:

```
vi /etc/default/knockd
```

وتأكد من وضع رقم 1 بدل من 0 في المتغيير START_KNOCKD كما يلي:
كود:

```
START_KNOCKD=1
```

الآن قم بتشغيل السيرفر Knockd هكذا:
كود:

```
 /etc/init.d/knockd start
```

الآن لنقم بتشغيل خدمة SSH هكذا:
كود:

```
/etc/init.d/sshd start
```

الحين كل شيء جاهز لعمل التجربة ...

الآن قم بمحاولة الإتصال بالسيرفر الـ SSH:
كود:

```
ssh 192.168.0.44
```

لن تستطيع وذلك لأنه جميع المنافذ للوصول للخدمة SSH مغلقة ... الآن من جهاز لينوكس آخر قم بتركيب برنامج الـ Client عليه (يوجد واحد للويندوز لكني لم اقم بتجربته) وقم بتنفيذ التالي:

كود:

```
knock -v 192.168.0.44 2222 3333  4444
```

ما قمنا به هو عمل دق على المنافذ 2222 و 3333 و 4444 التي حددناها في إعدادات السيرفر knockd ...

الآن قم بالإتصال مرة أخرى بخدمة SSH كالتالي:
كود:

```
ssh 192.168.0.44
```

ستلاحظ إنه أصبح الآن بإمكانك الإتصال بالخدمة وكل الأمور تمام ...

الآن لنرى ماذا حدث على الجدار الناري:
كود:

```
iptables -L -n
```

سترى هناك شي شبيه بالتالي:
كود:

```
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.0.44         0.0.0.0/0           tcp dpt:22
```

أي تم إضافة **rule** جديدة الى الجدار الناري يفتح منفذ 22 لكي يتم إستعماله بالإتصال بخدمة SSH ...

آخر حاجة هي ان نغلق الإتصال هذا وتقوم خدمة knockd بغلق المنفذ هي بعمل التالي:
knock -v 4444 3333 2222

وهنا قمنا بعكس الدق على الخدمة والتي يفهمها الـ knockd على إنها طلب بغلق المنفذ كما هو محدد في ملف الإعدادات الخاص بخدمة knockd ... طبعا تستطيع تغيير كل من المنافذ الخاصة بفتح المنفذ أو غلقها وذلك من ملف الإعدادات التي ذكرناه بالاعلى ...

الى هنا ينتهي هذا الموضوع ولمن يريد معرفة المزيد عن هذه التقنية PK يمكنه متابعة المواقع التالية:
موقعي الشخصي لرسالة الدكتوراه
موقع الـ Knockd الرسمي
موقع PortKnocking.org العالمي

ودمتم بود جميعاً