تأمين خدمات لينكس

يكتبها – محمد عبدالله

تحدثنا في الاعداد السابقة عن كثير من الخدمات مثل NFS,SAMBA,SSH,FTP . وسأحاول هنا الحديث عن تأمين هذه الخدمات ، تغيير البرورتات المستخدمة ، استخدام xinetd لتنظيم بعض الخدمات والحد من الوصول لها ، استخدام TCP Wrappers لمزيد من الحماية وكذلك تستخدام iptables لمزيد من الأمان .

NFS :

هي خدمة تقوم على مشاركة الملفات بين أنظمة Linux and Unix تقوم على مبدأ أن يقوم الجهاز الخادم بتصدير ملفات لتقوم الأجهزة الاخرى بالاستفادة منها . على فرض أن لديك جهاز NFS في الشبكة يقوم بتصدير ملفات للتثبيت (تثبيت لينكس من خلال الشبكة) فما هي المنافذ التي تحتاج اليها لإتمام عملية التثبيت ؟

لكي تعمل هذه الخدمة يجب أن تكون خدمة portmap تعمل لديك وهي تستخدم البورت 111 ، NFS يستخدم البورت 2049 . إذاً كل ما تحتاجه هو فتح هذه المنافذ . عن طريق iptables ضف الرولز التالية :

```
iptables -A INPUT -p tcp -s 192.168.1.0/24 -m multiport –dport 111,2049 -j ACCEPT
```

و

```
iptables -A INPUT -p udp -s 192.168.1.0/24 -m multiport –dport 111,2049 -j ACCEPT
```

الآن قم بمحاولة عمل mount من أي كلاينت وستجد بأنه ليس بإستطاعتك الوصول الى هذه الملفات !!!

السبب في هذه أن هناك خدمات مثل rquotad و mountd و statd تأخذ البروتات بطريقة عشوائية ، وللتأكد من ذلك قم بعمل restart للخدمة وفي كل مره تأكد من منافذ rpc.mountd و rpc.rquotad عن طريق الأمر netstat -tunap .

الآن سنقوم بتثبيت هذه القيم عن طريق انشاء الملف التالي :

```
/etc/sysconfig/nfs
```

تأكد من أن صلاحية الملف 644 ثم ضع فيه القيم التالية :

```
RQUOTAD_PORT=875
MOUNTD_PORT=800
STATD_PORT=662
```

الآن قم بإعادة تشغيل الخدمة لترى أن هذه القيم لا تتغير . إذاً عدل على الرولز الخاصة بـ iptables لتكون كالتالي :

```
iptables -A INPUT -p tcp -s 192.168.1.0/24 -m state --state NEW -m multiport --dport 111,2049,800,875,662 -j ACCEPT
```

و

```
iptables -A INPUT -p udp -s 192.168.1.0/24 -m state --state NEW -m multiport --dport 111,2049,800,875,662 -j ACCEPT
```

SSH :

وهي خدمة للوصول الى الأجهزة عن بعد و تعمل الخدمة على المنفذ 22 . ملف اعدادها هو .

```
/etc/ssh/sshd_config
```

أهم النقاط التي ينبغي تغييرها هي جعل الخدمة تعمل على الإصدار الثاني Protocol 2 لما فيه من أمان . أم الأخر وهو تحديد الـ IP الذي تعمل عليه الخدمة وذلك في حال احتواء الجهاز على أكثر من NIC ويمكنك ذلك عن طريق ListenAddress 192.168.1.1 مثلاً .

من المهم أيضاً تعديل الخيارات التالية :

```
LoginGraceTime 1m
PermitRootLogin no
MaxAuthTries 3
```

وهي اعطاء المستخدم مهله دقيقة لكتابة كلمة المرور كما قمنا بمنع المستخدم root من الوصول للخدمة بطريقه مباشرة ، وكذلك قمنا بتحديد عدد مرات المحاولة لكتابة كلمة المرور بثلاث مرات .

ولوضع قاعدة في iptables نفذ الآتي :

```
iptables -A INPUT -p tcp –dport 22 -s 192.168.1.0/24 -m state --state NEW -j ACCEPT
```

توضيح على حالات الإتصال (state)

الاتصال عبر بروتوكول TCP يمر بثلاث مراحل هي :

SYN ---> SYN/ACK ---> ACK

المرحلة الأولى تكون الحالة فيها NEW وهي عندما يقوم أي جهاز (client) بطلب تأسيس اتصال جديد ، مثلاً عندما تطلب الإتصال