بخادم SSH فإنك أولاً تقوم بطلب تأسيس اتصال جديد وهنا تكون صيغة الباكيت هي NEW ، عندها يقوم الخادم بالرد عليك وتكون حالة الباكيت هنا هي ESTABLISHED وهي المرحلة الثانية ، بعدما تقوم بالموافقة على رد الخادم ترسل له باكيت بالحالة RELATED وهنا يتم الاتصال .

هذا يعني انه لا ينبغي عليك استقبال باكيت بهيئة NEW على البروتات التي تعمل فيها خدماتك ، ولهذا قمت هنا بتحديد هيئة الباكيت بـ NEW . ولكن كيف يستقبل جهازك الرد من الخادم بقبول الطلب (المرحلة الثالثة) ؟

هنا عليك وضع قاعدة تستخدمها دوماً وهي :

```
iptables -I INPUT 1 -m state –state ESTABLISHED,RELATED -j ACCEPT
```

لاحظ هنا اني اخترت I بدل A لأني اريد وضع هذه القاعدة في بداية سلسلة الإدخال INPUT .

عليك دوماً التأكد بأنه لا توجد منافذ مفتوحة لخدمات لا تريدها.

استخدام XINETD :

xinetd هي خدمة مسؤولة عن خدمات اخرى مثل swat,tftp,telnet وغيرها . طريقة عملها هي كالتالي:

Client --> XINETD --> Service

ملف اعداد xinetd هو /etc/xinetd.conf والذي بدوره يقوم بتحميل كل الملفات الموجودة في الدليل /etc/xinetd.d/ .

ملف اعداد xinetd يظهر لنا الخيارات التالية :

```
#
# Simple configuration file for xinetd
#
# Some defaults, and include /etc/xinetd.d/

defaults
{
        instances               = 60
        log_type                = SYSLOG authpriv
        log_on_success          = HOST PID
        log_on_failure          = HOST
        cps                     = 25 30
}

includedir /etc/xinetd.d
```

حيث :

instances هي أقصى عدد من الخدمات التي تقوم xinetd بتشغيلها . أي في حال تحديد الرقم بـ 2 فإنك تستطيع الوصول الى هذه الخدمة عن طريق جهازين (IP 2) .

log_type وهي المستوى الذي يتم به تسجيل ملفات log وفي العدد القادم بمشيئة الله سنتناول log بمزيد من التفصيل .

log_on_success صيغة ملف log عن تسجيل دخول ناجح ، وفي هذه الحالة سيتم تسجيل عنوان الجهاز الذي قام بتسجيل الدخول ، وكذلك رقم ID لهذه العملية أي ما يسمى بـ PID.

log_on_failure تسجيل محاولات الدخول الفاشلة في ملفات log ولكن هنا سيتم تسجيل عنوان IP فقط .

Cps وهي اختصار لـ connection per Second حيث يأخذ هذا الخيار مدخلتين ، الأولى هي عدد الاتصالات التي تستطيع الخدمة التعامل معها في الثانية الواحدة وهي هنا 25 . المدخلة الثانية هي عدد الثواني التي تتوقف في الخدمة عن العمل في حال تجاوز العدد المحدد في المدخلة الأولى . أي أنه في حال وصول أكثر من 25 اتصال في ثانية واحدة فإن الخدمة ستتوقف عن العمل لمدة 30 ثانية .

لاحظ آخر خيار هو تحميل كل الملفات الموجودة في الدليل /etc/xinetd.d .

لنلقي نظرة سريعة على ملف اعداد خدمة swat الموجود تحت الدليل السابق .

```
# default: off
# description: SWAT is the Samba Web Admin Tool. Use
swat \
#               to configure your Samba server. To use SWAT, \
#               connect to port 901 with your favorite web
browser.
service swat
{
        port            = 901
        socket_type     = stream
        wait            = no
        only_from       = 127.0.0.1
        user            = root
        server          = /usr/sbin/swat
        log_on_failure  += USERID
        disable         = yes
}
```

قد تكون أبرز الخيارات التي يتم تغييرها هي port أي المنفذ ، only_from وهي كما تلاحظ هنا تعمل على الجهاز المحلي localhost ، إذا أردت الوصول الى هذه الخدمة عبر الشبكة أو جهاز معين فحدد عنوان IP الخاص به مثل 192.168.1.1 لعنوان واحد فقط أو 192.168.1.0/24 لشبكة معينه . ويمكن وضع أكثر من قيمة مثل 127.0.0.1 192.168.1.1 192.168.1.100 . يمكنك أيضاً تفعيل الخدمة وتعطيلها عن طريق تغيير قيمة disable ، لاحظ هنا أن الخدمة لا تعمل ، غير القيمة الى no لتعمل الخدمة لديك . يمكنك أيضاً تحديد IP الذي تعمل عليه الخدمة (في حال وجود أكثر من NIC) عن طريق الخيار bind = 192.168.1.1 . كما يمكنك استخدام كلمة interface بدلاً من bind ولكلاهما بنفس العمل . يمكنك أيضاً تحديد وقت الوصول الى هذه الخدمة عن طريق access_times = 8:00-15-00 وذلك لتحديد وقت الوصول الى هذه الخدمة في ساعات العمل الرسمي (لاحظ هنا استخدام نظام 24 ساعة) .كما يمكنك أيضاً تحويل الطلبات القادمة الى جهاز آخر أو حتى على خدمة اخرى فمثلاً