بسم الله الرحمن الرحيم

الجبهة الإعلامية الإسلامية العالمية

سرية الأمن التقني

تقدم

البوابة الآمنة

(بإذن الله)

شرح لإنشاء و تركيب سيرفرات التخفي الآمنة و تشفير البيانات باستخدام نظام اللنكس و تقنية

OpenVPN

إهداء ...

إلى مجاهدينا الأشاوس...

و شهدائنا الأبطال...

إلى الشباب الموحد الذي قضى بسبب تتبع من هنا و إختراق من هناك...

إلى الشهيد المجاهد يوسف العييري رحمه الله الذي عمل ليلاً و نهاراً بدون توفر أبسط المعايير الأمنية المتوفرة لنا في هذا اليوم مضحياً بنفسه في سبيل الله....

إلى الرعيل الأول من المجاهدين الإلكترونيين الذين سقوا شجرة الجهاد المباركة بدمائهم فأثمر زرعهم شجرة أصلها ثابت و فرعها في عنان الويب !

إلى شيخي و حبيبي الشيخ المجاهد أسامة بن لادن حفظه الله و رعاه و من سار على منهجه....

إلى إخواننا الذين سبقونا بالجهاد الإلكتروني و لهم علينا السابقة و الفضل في الجبهة الإعلامية الإسلامية العالمية و غيرها من منظمات العمل الجهادي المخلص....

إليهم جميعاً ، أهدي هذا العمل

خادم المجاهدين

سرية الأمن التقني

مقدمة :

عندما تتصل بموقع من المواقع تمر بياناتك على العديد من الجهات قبل وصولها الهدف ، و مبدئياً يحمل ذلك بعض المخاطر مثل تجسس الجيران او الشركة المزودة للخدمة – sniffing - و غير ذلك ، بالإضافة إلى تسجيل الآيبي الخاص بك على سيرفر الشركة المستضيفة مما قد يقود إليك مباشرة لا سمح الله في حال حدوث اختراق للموقع الذي تتصفحه ...

البروكسيات الموجودة حالياً لا تحل المشكلة ، ففضلاً عن كونها غير موثوق بها (لأنك لا تدري السبب الحقيقي لتقديم هذه الخدمات مجاناً !) فهي لا تشفر البيانات الخارجة و الواردة من جهازك ، بالإضافة إلى أن أكثرها لا يقدم تخفي حقيقي بل إن استعمال أكثرها يتسبب في ظهور الآي بي الخاص بك لدى المواقع التي تهدف لفتحها و ان اردت الدليل فافتح احد المواقع التي تظهر معلومات كاملة عن مصدر الطلب مثل هذه الصفحة :

/www.sptechs.com/ip

بعد بحث مستفيض و دراسة و ما شابه قمت بحمد الله بالتعرف إلى خدمة ممتازة في هذا المجال ، و هي خدمة OpenVPN

و تعتمد على إصدار شهادات للطرفين بحيث تكون آمنة من محاولات التقمص و ما شابه و هو ما يسمى

MITM (Man In The Middle Attack)

و تدعم هذه الخدمة درجات تشفير متعددة ، و المدى العام لها 384 بت - 4096 بت !

و لقد استشرت أخونا أبو مصعب مبرمج برنامج أسرار المجاهدين حول هذه الخدمة فكتب إلي أنها ممتازة و يمكن إستخدامها

هذه الطريقة من فكرة المهندس James Yonan و هو مهندس أمريكي و كما قرأت على موقعه فإن سبب تفكيره في هذه الخدمة هو عندما كان في رحلة عمل إلى شرق آسيا و انه احتاج للدخول لشبكة الشركة التي يعمل فيها في أمريكا فخشي أن يتنصت الروس على المعلومات المتبادلة بينه و بين شركته (يبدو أن مجال عمله حساس) و عندما لم يجد حلاً متوفراً في مجال الإنترنت لهذا الأمر قام ببرمجة هذا البرنامج و توفيره مجاناً مع الكود المصدري على موقعه (مما يدل أن البرنامج عند درجة تشفير معينة يستحيل حتى على الدول فك تشفيره)
فإذا قلنا أن أعلى درجة تشفير في التصفح الآمن هي 256 بت فكيف لو وجدنا أن البرنامج يبدأ من 384 بت ؟

المتطلبات :

الآن لتركيب الخدمة يلزمنا ما يلي :

1- سيرفر لنكس (لقد كنت اعمل على الفيدورا) .
2- تركيب خدمة البروكسي squid .
3- تركيب خدمة openvpn .
4- إنشاء و استصدار الشهادات لمن ترغب في ان يعملوا على الخدمة .
5- إنجاز ملف إعدادات للزبائن .
1- إعداد لنكس على الفيدورا ليس أمراً صعباً ، لذلك لن أشرحه
إن كنت تنوي انشاءه بنفسك فقم باستئجار سيرفر windows 2003 مع كمية كبيرة من الرام ثم قم بتنصيب برنامج vmware server باستخدام التحكم بالسيرفر عن بعد

و من ثم قم بتنزيل الفيدورا 6 نسخة الديفيدي حتى لا تتعب أثناء تبديل الأسطوانات (بشكل وهمي طبعاً !)
و قم بتنزيل الفيدورا و إليك رابط الشرح (إنجليزي)

http://howtoforge.net/installing_a_l..._fedora_core_6

و نظراً لأنك قد تتعامل مع سرعات مختلفة ، فكلما زادت قوة التشفير كلما احتجت لخط إنترنت أسرع

سنفترض اننا سننشئ شبكات وهمية لزبائننا بالسرعات التالية :

192.168.11.0/8 لقوة التشفير 384
192.168.22.0/8 لقوة التشفير 512
192.168.33.0/8 لقوة التشفير 1024
192.168.44.0/8 لقوة التشفير 2048
192.168.55.0/8 لقوة التشفير 4096

2- إعداد البروكسي:

إليكم الأوامر الخاصة بذلك :

أولاً نقوم بتنصيبه بكتابة الأمر التالي في الشل shell عندما تكون روت root :

```
yum -y install squid
```

الآن نقوم بتحرير ملف الإعدادات :

```
nano /etc/squid/squid.conf
```

نقوم بتعديل السطر التالي :

```
http_port 3128
```

إلى بورت بديل لتجنب العثور عليه من قبل الفيروسات التي تجوب النت طوال الوقت ، و ليكن :

رمز:

```
http_port 33128
```

الآن نذهب للسطر الذي يحتوي على هذه الجملة كما هي :

```
acl CONNECT method CONNECT
```

و نضيف الأسطر التالية للسماح لشبكاتنا الوهمية بإستخدام الإنترنت

رمز:

```
acl 384_network src 192.168.11.0/255.255.255.0
acl 512_network src 192.168.22.0/255.255.255.0
acl 1024_network src 192.168.33.0/255.255.255.0
acl 2048_network src 192.168.44.0/255.255.255.0
acl 4096_network src 192.168.55.0/255.255.255.0
```

الآن نذهب إلى هذا السطر :

INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

نضيف تحته :
رمز:

```
http_access allow 384_network
http_access allow 512_network
http_access allow 1024_network
http_access allow 2048_network
http_access allow 4096_network
```

الآن لو حفظنا الملف و شغلنا الخدمة ستعمل و لكن ستسمح لك فقط بالإتصال بالمنافذ الخاصة بخدمة الإف تي بي و ال http و https فقط ، إذا أردت أن تتصل عبر البروكسي بأي بورت قم بإضافة الرمز # قبل أي سطر يحتوي هذه الجملة :

safe_ports

الآن إضغط CTRL + X ثم y ثم Enter لحفظ الملف

الآن قم بتحرير ملف الهوست بالأمر التالي :

رمز:

```
nano /etc/hosts
```

و قم بإضافة الآيبي الخاص بسيرفرك كهوست

الآن إحفظ الملف

أكتب الأمرين التاليين لبدء خدمة البروكسي بشكل صحيح :

رمز:

```
service network restart
service squid start
```

البروكسي الآن يعمل على البورت الذي قمت بتحديده و لكنه سيقبل الطلبات فقط من الشبكات المحددة أعلاه ، سترى كيف تدخل منها إن شاء الله في الرد التالي
و لكن قبل الذهاب للرد التالي سنكتب الأمر التالي كي تعمل خدمة البروكسي مع بدء تشغيل النظام :

رمز:

```
chkconfig --level 345 squid on
```

جاء الآن وقت تنصيب خدمة ال OpenVPN

3- تركيب خدمة openvpn

الآن سنقوم بتنزيل متطلبات خدمة ال OpenVPN

بالأمر التالي :

رمز:

```
yum -y install rpm-build lzo-devel pam-devel gcc
```

الآن علينا تحديث النظام كي نؤمنه من الثغرات

بالأمر التالي :

رمز:

```
yum -y update
```

بعد انتهاء الأمر السابق من العمل (سيحتاج بضعة ساعات غالباً) قم بإعادة تشغيل النظام :

رمز:

```
reboot
```

و بعد الإنتهاء سنقوم بإنشاء مجلد جديد لعملنا

قم بتنفيذ الأوامر التالية :

رمز:

```
mkdir /downloads/
```

الآن نقوم بتحميل الكود المصدري تمهيداً لتنصيبه :

رمز:

```
wget http://openvpn.net/release/openvpn-2.0.9.tar.gz
```

الآن نقوم بترجمته إلى لغة الآلة بما يتناسب مع النظام :

رمز:

```
rpmbuild -tb openvpn-2.0.9.tar.gz
```

سينتج لدينا ملف جديد هو openvpn-2.0.9-1.i386.rpm سنقوم بتنصيبه باستخدام أحد الأمرين التاليين (لا أذكر أيهما سيعمل و لكن إن عمل أحدهما فلا تجرب الآخر) :

رمز:

```
rpm -i openvpn-2.0.9-1.i386.rpm
```

أو الأمر التالي :

رمز:

```
rpm --install /usr/src/redhat/RPMS/i386/openvpn-2.0.9-1.i386.rpm --nosignature
```

بعد التنصيب علينا اعداد الخدمة

سننشئ ملفات إعدادات الخدمة ، فنقوم بالذهاب لمجلد الخدمة الرئيسي

رمز:

```
cd /etc/openvpn
```

الآن ننشى مجلدات درجات التشفير المختلفة :

رمز:

```
mkdir /etc/openvpn/384
mkdir /etc/openvpn/512
mkdir /etc/openvpn/1024
mkdir /etc/openvpn/2048
mkdir /etc/openvpn/4096
```

الآن ننشئ ملفي إندكس و سيريال الضروريين كما سنرى لاحقاً :

رمز:

```
nano index.txt
```

نضع في الملف اعلاه مسافة واحدة (نعم ! فقط كبسة space bar) ثم نحفظه و ننشئ الملف التالي :

رمز:

```
nano serial
```

نكتب فيه بالضبط :

رمز:

```
01
```

يعني نضغط : 0 ثم 1 ثم إنتر ثم نحفظ الملف

الآن ننسخها إلى المجلدات بالأوامر التالية :

رمز:

```
cp index.txt /etc/openvpn/384/index.txt
cp index.txt /etc/openvpn/512/index.txt
cp index.txt /etc/openvpn/1024/index.txt
cp index.txt /etc/openvpn/2048/index.txt
cp index.txt /etc/openvpn/4096/index.txt
cp serial /etc/openvpn/384/serial
cp serial /etc/openvpn/512/serial
cp serial /etc/openvpn/1024/serial
cp serial /etc/openvpn/2048/serial
cp serial /etc/openvpn/4096/serial
```

الآن نذهب للمجلد الخاص بسكربتات النظام :

رمز:

```
cd /usr/share/doc/openvpn-2.0.9/easy-rsa
```

هناك ملف اسمه vars سننشئ منه خمس نسخ ، لكل درجة تشفير نسخة تناسبها :

رمز:

```
nano vars
```

الآن سنقوم بإنشاء نسخة لدرجة التشفير الأقل 384 ، علينا أن نقوم بتعديل السطر :

رمز:

```
export D=`pwd`
```

إلى :

رمز:

```
export D='/downloads/openvpn-2.0.9/easy-rsa'
```

و نقوم بتعديل :

رمز:

```
export KEY_CONFIG=$D/openssl.cnf
```

لتصبح :

رمز:

```
export KEY_CONFIG=/usr/share/doc/openvpn-2.0.9/easy-rsa/openssl.cnf
```

و نقوم بتعديل :

رمز:

```
export KEY_DIR=$D/key
```

لتصبح :

رمز:

```
export KEY_DIR=/etc/openvpn/384
```

و نقوم بتعديل :

رمز:

```
export KEY_SIZE=1024
```

لتصبح :

رمز:

```
export KEY_SIZE=384
```

الآن الملف الأول جاهز ، نقوم بحفظ نسخة منه عن طريق ضغط CTRL + O
فيطلب منا اختيار اسم الملف فنجعله vars384

و نكرر العملية بالنسبة لباقي درجات التشفير تماماً كما في الشرح أعلاه مع استبدال الرقم 384 في كل موضع بالدرجة البديلة (512 عندما نريد إنشاء vars512 و 1024 عندما نريد إنشاء vars1024 و 2048 عندما نريد إنشاء vars2048 و 4096 عندما نريد إنشاء vars4096

الآن سنقوم بإنشاء الشهادات للسيرفر و الزبائن

نبدأ بدرجة 384 فنكتب الأمر التالي :

رمز:

```
. vars384
```

الآن تم تحميل مجلدات الدرجة 384 في الذاكرة
نطلب إنشاء مفتاح أساسي :

رمز:

```
./build-dh
```

سيستغرق وقتاً بسيطاً جداً عند هذه الدرجة (عند الدرجة 4096 احتاج هذا الأمر مني ذات مرة 12 ساعة !!!!)

الآن ننشئ شهادة عامة مبنية على المفتاح الأساسي

رمز:

```
./build-ca
```

سيطالبك بتعبئة بعض البيانات للشهادة ، أنت حر في تعبئتها أو تركها كما هي ، ما عدا السطر الذي يطالبك فيه ب : Common Name فستضطر أن تدخل أي شئ مثل OVPN أو proxy أو أي شئ يخطر ببالك ، فإن طالبك بهذا السطر فدع ما بعده كما هو إلا أن يسألك ب Y/n فتكتب y ثم Enter

الآن سننشئ شهادة السيرفر

رمز:

```
./build-key-server 384-server
```

كما تعاملت في التعامل مع الشهادة العامة تعامل مع انشاء شهادة و مفتاح السيرفر ، الآن سننشئ مفتاح و شهادة للزبون الأول و لنفترض إسمه client01

رمز:

```
./build-key client01
```

سنتعامل معه كما تعاملنا مع الشهادات أعلاه ، بعد ذلك سنجد هناك الكثير من الملفات في المجلد :

رمز:

```
/etc/openvpn/384
```

كلها ملفات تشغيلية للخدمة ما يهم الزبون الحصول عليه هو :

رمز:

```
client01.crt
client01.key
ca.crt
```

ملاحظة 1 : تسريب أي ملف آخر قد يسبب تهديداً أمنياً ! عليك بالحفاظ على الملفات الآخرى لأنها مهمة جداً و تعتبر أساس فك تشفير الحزم الخاصة بالخدمة !
ملاحظة 2 : الخدمة لم تعمل بعد !
ملاحظة 3 : الزبون أعلاه يعمل فقط مع الدرجة 384 ، و لو أردنا أن يعمل مع خدمة أخرى أو درجة أخرى فعلينا إنشاء مفتاح آخر له بعد تحميل مجلدات الدرجة المطلوبة إلى الذاكرة أولاً !
الآن نبدأ بصنع ملفات الدرجة 512 فنقوم بتحميل مجلدات الدرجة 512 إلى الذاكرة بأن نكتب

رمز:

```
. vars512
```

و نكمل كما هو مشروح أعلاه

و نكرر العملية حتى ننشئ ملفات جميع الخدمات

بقيت الخطوة الأخيرة على السيرفر

الآن نقوم بتشغيل الخدمة

علينا أن ننشئ ملف إعدادات لهذا

فنكتب الأمر التالي :

رمز:

```
cd /etc/openvpn
```

ثم

رمز:

```
nano 384-server.conf
```

ثم نلصق السطور التالية داخل الملف و نحفظه

رمز:

```
port 33384
proto tcp-server
dev tun
ca /etc/openvpn/384/ca.crt
cert /etc/openvpn/384/384-server.crt
key /etc/openvpn/384/384-server.key
dh /etc/openvpn/384/dh384.pem
server 192.168.11.0 255.255.255.0
duplicate-cn
keepalive 10 120
cipher BF-CBC
comp-lzo
persist-tun
verb 0
```

حيث :

port: رقم منفذ الخدمة الخاص بدرجة 384 ، تستطيع تعيينه كما تريد و لا تنسى أن تفتح المنفذ المعين هنا في الجدار الناري للنكس و إلا لن تعمل الخدمة !
cert : مسار شهادة السيرفر (الذي قمنا بإنشاءه في وقت سابق)
key : مسار مفتاح السيرفر
dh : مسار المفتاح الأساسي
ca : الشهادة التي قمنا بإنشاءها
server : مجموعة الآيبيهات التي سيتم تعيينها لمن يتصل بالخدمة
duplicate-cn : وجود هذا السطر يسمح بالإتصال من أكثر من زبون بنفس الشهادة فإن أردت فأبقه موجوداً
verb 0 : هذا لمنع تسجيل من أي أيبي يتصل الزبائن ، في حالة حدوث مشاكل في الخدمة و اردت ان يعرض رسائل الخطأ قم باستبدال الصفر بثلاثة أو برقم 4 ثم اعد تشغيل الخدمة

نقوم الآن بإنشاء ملف جديد بنفس الطريقة لباقي درجات التشفير ، مع استبدال ما يلزم

و هنا مثال لخدمة ال 512 كما يجب أن تكون بناء على الإعدادات أعلاه

رمز:

```
port 33512
proto tcp-server
dev tun
ca /etc/openvpn/512/ca.crt
cert /etc/openvpn/512/512-server.crt
key /etc/openvpn/512/512-server.key
dh /etc/openvpn/512/dh512.pem
server 192.168.22.0 255.255.255.0
duplicate-cn
keepalive 10 120
cipher BF-CBC
comp-lzo
persist-tun
verb 0
```

الآن نعين الخدمة لتبدأ مع كل تشغيل للنظام بشكل آلي
رمز:

```
chkconfig --level 345 openvpn on
```

كي نعرف أنها عملت أو لا فسنقوم بفحص آيبيهات السيرفر ، فنكتب الأمر :
رمز:

```
ifconfig
```

سيعرض لنا الآيبيهات الخاصة بالسيرفر ، طبعاً لن يكون منها أي آيبي داخلي لأن الخدمة لم تعمل بعد ، نقوم الآن بتشغيل الخدمة :
رمز:

```
service openvpn start
```

بعد أن تعمل نعيد تجربة الأمر ، نجد أن الواجهات الجديدة و الآيبيهات تعمل بنجاح ! مبارك

تم بحمد الله شرح تجهيز السيرفر

بقي فقط تجهيز الزبون

برمجة الزبون :

لقد تحدثت فيما سبق عن تجهيز السيرفر ، و الآن و قد أصبح جاهزاً لم أتكلم عن كيف يمكن لنا أن نستفيد منه ؟

الآن نريد تجهيز ملفات الإتصال بالسيرفر

أولاً علينا تنصيب البرنامج الذي سيقوم بالإتصال

و هذا هو رابطه :

http://openvpn.se/files/install_pack....3-install.exe

الآن نريد أن نتصل بإستخدام رخصة client01 التي أنشأناها أعلاه

نقوم بنسخ الملفات الثلاثة

ca.crt
client01.crt
client01.key

إلى مجلد

c:\program files\openvpn\config

الذي سينشأه البرنامج بعد أن ننصبه أعلاه

طبعاً لن ننسخه وحده

بل سننشئ ملف إعدادات للزبائن ، فنقوم بإنشاء ملف نصي بإسم client.ovpn-384 ثم نحرره بالمفكرة و نضيف إليه السطور التالية :

رمز:

```
client
dev tun
proto tcp-client
remote 11.22.33.44 33384
resolv-retry infinite
nobind
persist-tun
ca ca.crt
cert client01.crt
key client01.key
cipher BF-CBC
comp-lzo
verb 3
hand-window 300
```

حيث :

remote : نعبئ هنا الآيبي الحقيقي للسيرفر و منفذ درجة التشفير
ca : كما بأعلى
cert : اسم ملف شهادة الزبون
key :اسم ملف مفتاح الزبون
verb : كمية عرض المعلومات أثناء الإتصال كي تعرف مكان الخلل في حال وجوده

المهم يجب علينا أن ننسخ هذا الملف في المجلد المذكور أعلاه

الآن إضغط بزر الماوس الأيمن على أيقونة البرنامج في ركن الأيقونات أسفل الشاشة

ستجد عدة خيارات ، و منها :

Connect

بعدما تضغط

Connect

ستظهر شاشة ، إنتظر لدقيقة ...

يفترض خلال دقيقة أن تختفي الشاشة من تلقاء نفسها و تتحول الأيقونة اسفل الشاشة الى اللون الأخضر ..

الآن قم بتعبئة البيانات التالية كبروكسي خاص بك (بافتراض انك تستخدم ملفات إتصال الدرجة 384 بت المعدة وفق الأمثلة أعلاه - قم بتعديلها بما يتناسب مع وضعك) :

الآي بي :192.168.11.1
البورت :33128

الآن يتم كل تصفحك عبر السيرفر الذي تربطك به قناة مشفرة ..

افتح أي موقع آيبيهات و إن شاء الله ترى أن آيبي السيرفر هو الظاهر على الشاشة

ملاحظات :

1- إحدى الحيل هي أن تقوم بإضافة آيبي إضافي للسيرفر نفسه و تجعل إتصالك عليه بينما التصفح يخرج من الآيبي الآخر ، ذلك أكثر أماناً و الله أعلم
2- يرجى تنظيف مجلد var/log/ بشكل منتظم للإحتياط في حالة تم اختراق السيرفر لا سمح الله
3- يستحسن تغيير البورت الخاص بخدمة ssh و اختيار بسورد قوية .
4- يرجى إستعمال هذا الشرح على نطاق ضيق و عدم تعميمه للعامة بل للخواص فقط .

تم بحمد الله

كتبه الفقير إلى عفو ربه
خادم المجاهدين
الجبهة الإعلامية الإسلامية العالمية
أمير سرية الأمن التقني