

إخفاء الآثر

Remove Logs

معنى إخفاء الآثر ؟

إخفاء الآثر في الخطوة الأخيرة من خطوات الاختراق الأخلي، بعد الدخول الناجح على النظام او الجهاز وامتلاك صلاحيات مدير يعدل المخترق على إخفاء آثاره من النظام حتى لا يتم كشف الاختراق والتحركات في النظام.

خطوات يتبعها المخترق إخفاء الآثر:

- مسح السجلات - Clear Logs
- التحكم بالسجلات - Manipulating Logs
- 禁用审核 - Disable Auditing
- إخفاء الأدوات

طريقه المسح اليدوي للسجلات :

- الذهاب إلى مجلد النظام `/var/log`
- فتح نافذة بحث على رسائل السجلات `/var/log/messages`
- نفخ جميع السجلات

الآن نأتي على الخطوة last step وهي إنشاء Backup لـ logs . وهذا يمكّننا فعله من خلال

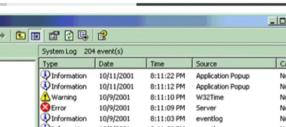
إخفاء الآثار Remove Logs

طريقة المسح اليدوي للسجلات :

Start > Control Panel > System and Security > Administrative Tools > Event Viewer

أنقر بثانية على Event Viewer

تحف جميع السجلات



Start > Control Panel > System and Security > Administrative Tools > Event Viewer

حذف حمزة السحلات

حذف الآخرين - Registry 
حذف الآخرين استخداماً مؤخراً (Recently Deleted) حذف الكوكيز والكاش وتنظيف (MRU) Used

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer

Recent Docs حذف المفتاح الموجود في ملف

(Default) حذف جميع القيم والملفات مادعا ملف

For more information about the study, please contact Dr. Michael J. Hwang at (319) 356-4330 or via email at mhwang@uiowa.edu.

MRU-Blaster

Scan your computer for MRU lists, and other lists that might store sensitive information.

Settings

About/FAQ

Exit

- Internet Explorer (typed URLs)
- Windows Run - Desktop MRU
- Google Toolbar History
- Microsoft Internet Explorer (typed URLs)
- Microsoft Internet Explorer (recent sites)
- Microsoft Internet Explorer (visited sites)
- Microsoft Recent MRU
- Windows Recent Items
- WordPerfect MRU
- Windows OpenWithMRU Items
- Corel Painter MRU Items
- Install Locations MRU
- Custom Notifications Past Items
- Windows OpenWithMRU

<https://www.brightfort.com/>

إخفاء الآثار

Remove Logs



MRU-Blaster أداة

يساعد برنامج **MRU-Blaster** على حذف وتقطيع آخر القوائم المستخدمة المحفوظة في الحاسوب.

وايضا ينطفل الملفات المؤقتة من متصلب الانترنت والكونفر

إخفاء الآثار

تعطيل فحص النظام



تعطيل فحص النظام

تعطيل فحص الملفات النظام هو أحد الطرق لإخفاء آثر

الاختراع بعد اتمتالاً صلاحيات المدير.

بعد الانتهاء من عملية الاختراق والدخول بـ**لفظ المخترع**

يتعين خاصية (**فحص الملفات مرة أخرى**) باستخدام

auditpol.exe

in linux remove history:

- > history -c
- > history -w
- > rm .bash_history

In windows:

إخفاء الآثار

Remove Logs

Clearing Logs

في نظام ويندوز غالباً المخترعون يستخدمون برنامج **clearlogs.exe**

<http://www.ntsecurity.nu/toolbox/>

BlackBerry

التشفير

Encryption



GAK (Government Access to Keys)

Cryptographic key



الشركات البرمجية توفر نسخ من كلـ **keys** او على الأقل مجموعة منـ **Keys** كافية للحكومة في حالة مصر الحرارية.

تحتل الحكومة حاليةـ **Keys** والاحتفاظ بها من المسرقة والتسريب.

Hash tool :

↳ in Linux : md5sum

↳ in Windows: winmd5sum

Thank you for downloading
Ubuntu Desktop

Your download should start automatically, if it doesn't, download now.

= Verify your download

Run this command in your terminal in the directory the file was downloaded to verify the SHA256 checksum:

```
echo "9eab93501640700097055f21277a7a1f62f8d6a699375fa4394e83679" | sha384 -c 256 --check
```

You should get the following output:

```
ubuntu-19-10-desktop-and4.1:~%
```

التشفير

Encryption



DISK Encryption



السرية وخصوصية: البيانات حيث يتم حفظ البيانات في قرص وتحويلها إلى أ��اد غير مقروءة مشفرة بـ **AES** بـ **برامج**.

* التشفير: يعدل القرص المشفر مثل طريقة عمل النصوص المشفرة لحماية البيانات حتى لو ان قفل التشفير داخل الأقراص يتم حرق البيانات في القرص

الحماية: باستخدام التشفير داخل الأقراص يتم حرق البيانات في القرص وحفظهم من التسريب والضياع.

Tools: Bitlocker, fileVault

>Zip --password 123 File.zip files

>Fcrackzip -b -c 'l' -l 1-3 -v File.zip

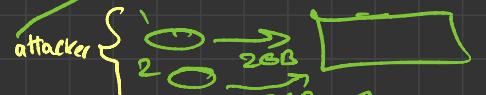
↑
brute force
attack

what
letter
number
to use

long
of the
word

Bandwidth

Server 5 GB



الجهاز الواحد لا يمكنه عمل هجوم او ارسال طلبات كافية في الشبكة لذلك تم عمل خدمة جديدة وهي DDoS ليتمكن المخترق من استخدام أجهزة كثيرة لنفخ في الشبكة

عند بدء عمل DDoS تظهر بعض الصعوبات والمشاكل في الشبكات مثل الرووت والسوينتش نظر للمتغيرات التيحدث داخل الشبكة بسبب الهجوم وارتفاع الطلبات

ICMP ECHO packets لذلك استخدم المخترق Botnets لاستمراره عمل حجب الخدمة في شبكة مع

بساطة جميع no bandwidth تستخدمنا للاستخدام المشروع والقانوني

Bandwidth Attack



1

2

3

4

Application-Level Flood Attacks



Application-Level Flood

يسbib المخادع بالخدعة الشبيهة معينة مثل البريد الإلكتروني، شبكة التواصل وغيرها

مخدع

يسكتد المخدع الثقة في المطلب المقدمة (الرسائل كرو) لمنع المسألة القانونية

لابق

ويشتت خدمة نظام معن لتجوية ملائ مع مستخدم من دخول تطبيق او موقع وظيف

خطأ في كلمة المرور او البريد الإلكتروني

يسخدم المخدع البرمجيات العينة في استعلامات

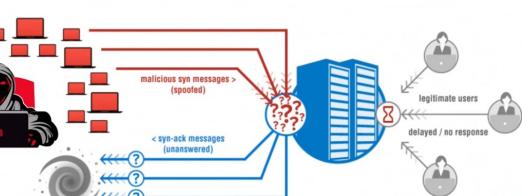
DB

SYN Flooding Attack



SQL Query

صحيح هناك ثغرة اصحاب خطأ مع



تخفيض خطر DoS & DDoS



Load Balancing



Throttling



وضع راوتر لدخول الخادم باستخدام منطق Throttle لحماية من حجم الازدحام في الشبكة

يساعد منع تعطل خادم DoS بالتحكم ومواجهة

يساعد في مواجهة ازدحام هجوم DDoS ويسعى بالاستخدام القانوني للنتائج افضل

