

## حقائق الهاكر





New system technology – Mahmoud said

## المقدمة

السلام عليكم اهلا بكم في كتاب حقائق الهاكر هنا في الكتاب سوف نقوم بعمل جولة سريعة علي العالم الذي يمكن ان يكون غامض بالنسبة لبعض الناس ولكن الان بعد توجه الأنظار كلها الي الهاكر والي الاخبار التقنية الكثيرة التي أصبحت محطة نقاش بالنسبة للكل فعلي ان أقوم بتوضيح من هم الهاكر وكيف يقوموا بالاختراق والخطوات الأساسية لان هذا الجزء يعتقد البعض ان الهاكر هم خارقون او من كوكب اخر ولذلك سوف أقوم بتوضيح كل هذه الأمور.

## حقيقة الهاكر:

الهاكر ليس كما يعتقد الناس به او كما شبهته الأفلام التي انتشرت في هذه الأيام .

فهل هذه الصورة هي حقيقة الهاكر؟؟؟

الإجابة لا .. ونحن في هذا الكتاب سنناقش هذا السؤال من وجهة نظر علمية.

وسوف نناقش أيضا أكثر خمسة مكونات وأساليب رئيسية التي تتم بها عملية الاختراق .

انصح بشدة قراءة محتويات الفهرس لكي تأخذ فكرة عن النقاط الرئيسية التي سوف تكون محور النقاش.

وأخيرا اتمني لكم قراءة سعيدة ممتعة واستفادة كبيرة ....

## المحتويات

### الفصل الأول : الأسباب الرئيسية لتعليم الحماية

#### أهمية تعلم الحماية

#### المراحل الأساسية لتعلم الهاكر

### الفصل الثاني : المرحلة الاولى جمع المعلومات

#### الفرق بين البيانات التقنية والبيانات العامة .

#### الحصول علي بيانات المؤسسات .

#### الحصول علي بيانات المواقع .

#### الحصول علي بيانات الأشخاص .

#### طرق المكافحة.

### الفصل الثالث : المرحلة الثانية الفحص

#### فحص الشبكات .

#### فحص الأجهزة .

فحص السيرفرات .

طرق المكافحة .

## الفصل الرابع : المرحلة الثالثة طرق الاختراق

أنواع كلمات السر واختراقها .

استخدام Key logger .

الهندسة الاجتماعية .

طرق المكافحة .

## الفصل الخامس : المرحلة الرابعة تثبيت الاختراق

شرح مصطلح backdoor .

استخدام worms .

استخدام فيروس .

طرق المكافحة .

## الفصل السادس : المرحلة الخامسة إزالة اثر الاختراق

أهمية إزالة اثر الاختراق .

كيفية إزالة اثر الاختراق .

طرق المكافحة .

هندسة النجاح: تدعم برنامج التعليم الحر Virtual Academy  
التواصل عن طريق مدونة / محمد القبيصي:

<http://kobessi.blogspot.com>

التواصل عن طريق الصفحة الرسمية:

<https://www.facebook.com/Hndst.Elengah/>

التواصل عن طريق الهاتف:

+20 1276655624

### I.T. SKILLS

**المستوى الأول**

ويندوز 7  
أوفيس 2010  
الانترنت

**المستوى الثاني**

المكونات الداخلية  
اعداد ويندوز  
التجميع

**المستوى الثالث**

الصيانة و الأعطال  
مقدمة في الشبكات  
الدعم الفني



 [Kobessi.blogspot.com](http://Kobessi.blogspot.com)

 [Hndst.Elengah](https://www.facebook.com/Hndst.Elengah/)

 +201225278690



## الهدف

ان الهدف من الكتاب هو توضيح أهمية الهاكر وهو يتمثل في السعي وراء اكتشاف الثغرات وتعلم كيفية الحماية منها وان تكون قادر علي حماية نفسك والأنظمة التي تديرها من الاختراق علي ايدي مخالفتي القوانين.

فهذا الكتاب قد تعمدت فيه شرح أساليب الاختراق وليس الاختراق فعليا فيجب ان يكون لديك عقلية الهاكر وفي نفس الوقت كيف تقوم باستخدامها في حماية نفسك والآخرين وكذلك يمكنك ان تقوم بفرض هذه الحماية علي كبري الشركات بعد ان يصرحوا لك بتقرير مكتوب بانه بإمكانك اختبار الحماية وان تعطيتهم تقرير مفصل بالثغرات التي قد وجدتتها وكيفية حمايتها .

تحذير ....

ان استخدام بعض الأساليب هنا في هذا الكتاب قد يعرضك للمساءلة القانونية فلا تستخدمها إلا إذا طلب منك  
بتصريح مكتوب من مدير النظام أو الأشخاص المعنيين بالحماية وأن أي أداة مستخدمة هي شرعية لاختبار الاختراق  
وليس للاختراق العشوائي أو الانتقام .

ان الكاتب يخلي مسؤوليته من استخدام هذه الأدوات في أي شيء مخالف للقانون .





الكاتب

الاسم : محمود سعيد

البلد : الإسكندرية , مصر

العمل : محاضر في علوم الكمبيوتر

**Full stack developer**

**Logic design and algorithms**

Facebook للتواصل عبر

<https://www.facebook.com/mahmoud.said.NST>

للتواصل مع منظمة new system technology

التعليمية عن طريق رابط

<https://www.facebook.com/NSTechnologyO>





## الفصل الأول

## الأسباب الرئيسية لتعليم الحماية

### أهمية تعلم الهاكر

كثير من الناس يسألون عن سبب تعلم الحماية وقد انتشر هذا السؤال في تلك الأيام وأصبح محل قلق لكل من يستخدم التكنولوجيا في يومنا هذا فيجب علي ان أقوم بالإجابة عن هذا السؤال ؟

السبب الأول :

التوسع الكبير في مجال الانترنت حتي أصبح عنصرا فعالا في حياة الافراض والمجتمعات فعلي سبيل المثال يوجد الان قطاع كبير يسمى بالتجارة الالكترونية حيث من الممكن لمستخدمي الانترنت بيع او شراء أي سلعة او خدمة عن طريق الانترنت ويمكن أيضا عقد الصفقات التجارية بين الشركات الكبرى مما شكل خطر كبير علي البيانات الشخصية كالأسماء والعناوين وحسابات البنوك مما سهل سرقتها وإساءة استخدامها من جانب الهاكر .

السبب الثاني :

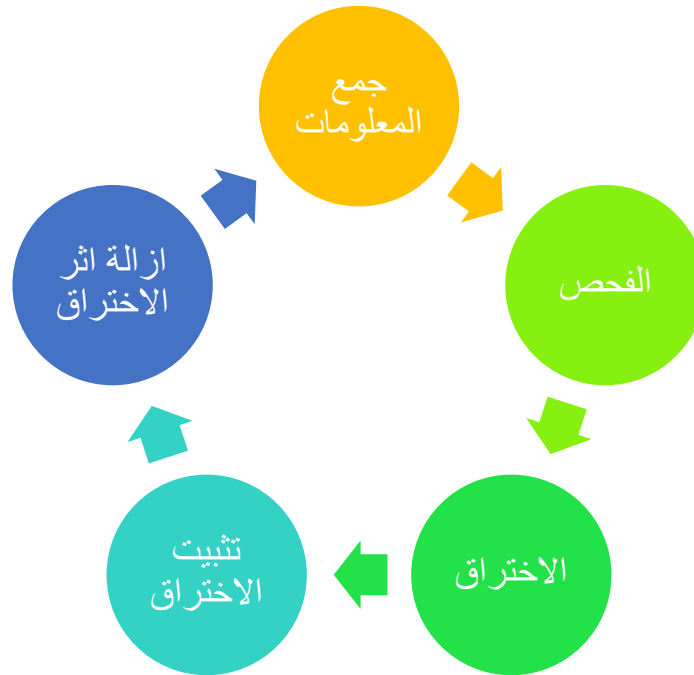
توافر برامج الاختراق وطريقة استخدامها وكلما زادت هذه البرامج كلما زادت اعداد الهاكر وهجماتها .

السبب الثالث :

ضعف الوعي لدي مستخدمي انترنت مما سهل الاحتيال عليهم بأساليب مختلفة مثل الهندسة الاجتماعية . وأخيرا لكل تلك الأسباب أصبح هناك الكثير من الثغرات التي وضعت عبئا علي مدير النظام ومهندسين الشبكات في حماية المعلومات مما جعل للهاكر الأخلاقي أهمية .

أهمية الهاكر الأخلاقي :

هو السعي وراء اكتشاف اجدد الثغرات وتعلم كيفية حماية الأنظمة من الاختراق .



## المراحل الأساسية في تعلم الهاكر

### 1- مرحلة جمع المعلومات

حيث يقوم المخترق بتجميع بيانات عن الهدف وتسمي **Foot Printing**



## 2 – مرحلة الفحص

يقوم المخترق بفحص النظام بدقة اعلى ومعرفة جميع برامج وأنظمة التشغيل المتاحة في الشبكة وتسمي

**Scan**

```

root@wks01:/home/vivek# nmap --top-ports 10 192.168.1.1

Starting Nmap 5.00 ( http://nmap.org ) at 2012-11-27 03:30 IST
Interesting ports on 192.168.1.1:
PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    open  ssh
23/tcp    closed telnet
25/tcp    closed smtp
80/tcp    open  http
110/tcp   closed pop3
139/tcp   closed netbios-ssn
443/tcp   closed https
445/tcp   closed microsoft-ds
3389/tcp  closed ms-term-serv
MAC Address: BC:AE:C5:C3:16:93 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.58 seconds

```

### 3 – مرحلة الاختراق

تختلف طريقة الاختراق باختلاف الهدف سواء كانت شبكة حواسيب أو هواتف ذكية .

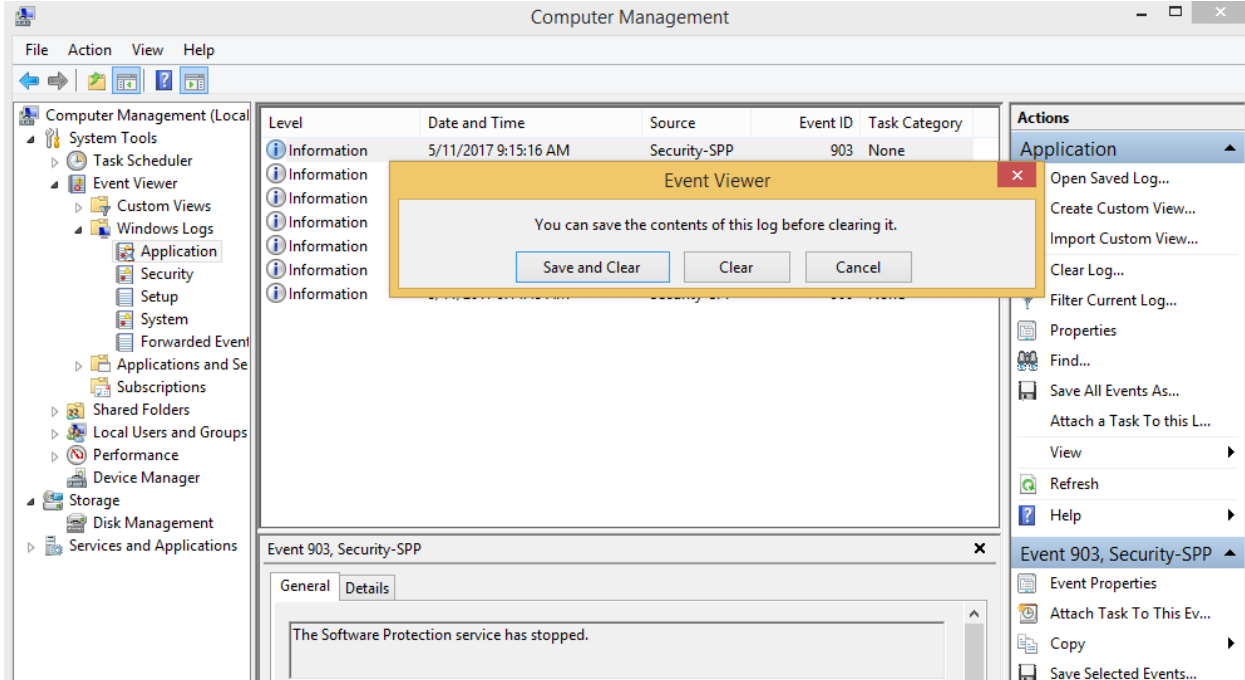
### 4 – مرحلة تثبيت الاختراق

هي مجموعة أساليب لإيجاد آلية لتسهيل الوصول للهدف فيما بعد .



## 5 – مرحلة حذف اثر الاختراق

يحذف المخترق جميع اثاره التي تدل علي الاختراق وهي من اهم الخطوات لان الاثار تكون بمثابة ادلة إدانة علي المخترق .





## الفصل الثاني



## جمع المعلومات

### الفرق بين البيانات التقنية و العامة

البيانات العامة	البيانات التقنية
ارقام هواتف وعناوين	<b>Ip</b> : الخاص بالأجهزة و المواقع
معلومات عن نشاط المؤسسة	<b>DNS</b>
أسماء العاملين وعناوين البريد الخاصة بهم	<b>E-mails</b> : الخاص بمسؤولين النظام

### 1 - الحصول علي بيانات الأشخاص

جمع المعلومات عن الأشخاص عن طريق البريد الالكتروني باستخدام أدوات مثل

**(confirm.to, didtheyreadit.com)**

**Example:**

Send | Save Draft | Attach ▼ | ! ↓ | Tools ▼ | Cancel

To: ellen@aol.com

Cc:

Bcc:

Subject: DidTheyReadIt

**Becomes...**

Send | Save Draft | Attach ▼ | ! ↓ | Tools ▼ | Cancel

To: ellen@aol.com.didtheyreadit.com

Cc:

Bcc:

Subject: DidTheyReadIt

\* If you are sending an e-mail to multiple recipients, you need to add ".DidTheyReadIt.com" to each address.

confirm.to أو تستخدم



The message is delivered to bill@abc.com correctly and if the recipient opens and reads your mail, you get the read receipt by email like this.

### Confirm.TO Mail Read Receipt

Who Read:	lsbl@lsb.org
Subject:	Good Morning
Read When:	Mon, 20 Nov 2000 21:13:55 +0900
Read Where:	¼□□#58;MARKETING @ POSTEL (LAN-MAC: 00c026f0b049) ([203.240.252.124]) <a href="#">Position &amp; Map</a>
This Notice Sent To:	lsb@postel.co.kr
Sent When:	Mon, 20 Nov 2000 21:13:38 +0900
Notary ID:	974722418-780f9ac82bf614b8.083ad16409a9fdea

#### Mail Receipt Notification Service (Patent Pending) by Postel Services Co.

lsb@postel.co.kr' current usage and quota		
criteria	max # of recipients	max # of bytes
per message:	930	960 Mbytes
per hour:	930	9130 Mbytes
per month:	930	9130 Mbytes
current usage	157/930	2.2 Mbytes / 9130 Mbytes

وعندما يقوم المستهدف بفتح البريد ترسل الي الهاكر رسالة بها تاريخ ووقت فتح البريد والـ IP

الخاص بالمستهدف

2 = الحصول علي بيانات المواقع

يمكن الحصول عليها من خلال أدوات مثل

(netcraft, dnslookup , ID tools )

example: site contains .netcraft.com

## Results for google.com

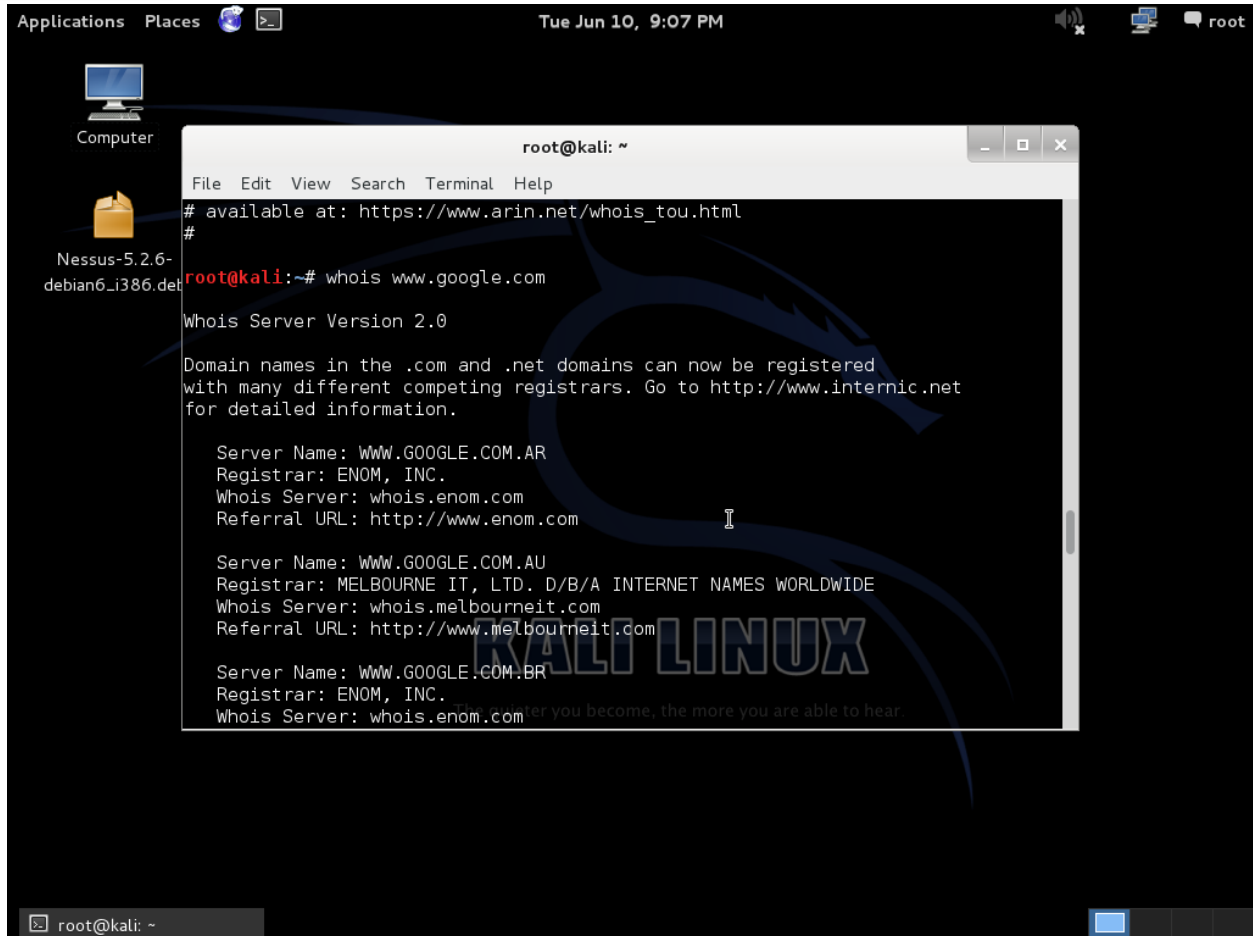
Found 433 sites

	Site	Site Report	First seen	Netblock	OS
1.	<a href="http://www.google.com">www.google.com</a>		november 1998	google inc.	linux
2.	<a href="http://google.com">google.com</a>		april 2000	google inc.	linux
3.	<a href="http://news.google.com">news.google.com</a>		april 2002	google inc.	linux
4.	<a href="http://maps.google.com">maps.google.com</a>		april 2005	google inc.	linux
5.	<a href="http://mail.google.com">mail.google.com</a>		june 2004	google inc.	linux
6.	<a href="http://translate.google.com">translate.google.com</a>		november 2001	google inc.	linux
7.	<a href="http://feedproxy.google.com">feedproxy.google.com</a>		september 2008	google inc.	linux
8.	<a href="http://www.google.com.au">www.google.com.au</a>		august 1999	google inc.	linux
9.	<a href="http://www.google.com.br">www.google.com.br</a>		march 2002	google inc.	linux
10.	<a href="http://drive.google.com">drive.google.com</a>		january 2012	google inc.	linux
11.	<a href="http://www.google.com.vn">www.google.com.vn</a>		october 2003	google inc.	linux
12.	<a href="http://www.google.com.mx">www.google.com.mx</a>		july 2002	google inc.	linux
13.	<a href="http://www.google.com.ar">www.google.com.ar</a>		august 1999	google inc.	linux
14.	<a href="http://www.google.com.tw">www.google.com.tw</a>		april 2003	google inc.	linux
15.	<a href="http://www.google.com.co">www.google.com.co</a>		july 2003	google inc.	linux
16.	<a href="http://scholar.google.com">scholar.google.com</a>		january 2005	google inc.	linux
17.	<a href="http://www.google.com.sg">www.google.com.sg</a>		december 2002	google inc.	linux
18.	<a href="http://www.google.com.ph">www.google.com.ph</a>		april 2004	google inc.	linux
19.	<a href="http://www.google.com.hk">www.google.com.hk</a>		march 2003	google inc.	linux

### 3 - الحصول علي بيانات الشركات

عن طريق موقع الشركة باستخدام أداة **whois** او عن طريق مواقع التواصل

او محرك البحث جوجل ولكن بشكل مختلف تسمى **Google Dorks**:



```
root@kali: ~  
File Edit View Search Terminal Help  
# available at: https://www.arin.net/whois_tou.html  
#  
root@kali:~# whois www.google.com  
  
Whois Server Version 2.0  
  
Domain names in the .com and .net domains can now be registered  
with many different competing registrars. Go to http://www.internic.net  
for detailed information.  
  
Server Name: WWW.GOOGLE.COM.AR  
Registrar: ENOM, INC.  
Whois Server: whois.enom.com  
Referral URL: http://www.enom.com  
  
Server Name: WWW.GOOGLE.COM.AU  
Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE  
Whois Server: whois.melbourneit.com  
Referral URL: http://www.melbourneit.com  
  
Server Name: WWW.GOOGLE.COM.BR  
Registrar: ENOM, INC.  
Whois Server: whois.enom.com
```

او تستخدم **GOOGLE DORKS**

## Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Any Category ▼

Search

Search

Date	Title	Category
2017-05-10	"Section" inurl:"xorg.conf" ext:conf -wiki	Files Containing Juicy Info
2017-05-10	inurl:"member.php?action=login"	Pages Containing Login Portals
2017-05-10	inurl:"multimon.cgi" intitle:"UPS"	Various Online Devices
2017-05-10	inurl:"this.LCDispatcher?nav="	Various Online Devices
2017-05-10	"Stealer by W33DY" ext:txt	Files Containing Passwords

### طرق المكافحة

1 – إخفاء الهوية باستخدام بروكسي (وذلك باستخدام أي بي آخر عن طريق احد شركات مزودي خدمة VPN)

2 – عدم عرض البيانات الشخصية المهمة علي مواقع التواصل الاجتماعي ووضع الكثير من الحماية مثل كلمات مرور قوية وربط المواقع بأرقام الهواتف كمرحلة ثانية من الحماية .

3 – اتخاذ خطوات

**Private registration** لإخفاء البيانات المهمة لدي المواقع مثل اسم

مدير المواقع والبريد الذي تم تسجيل الموقع به .



New system technology – Mahmoud said

## الفصل الثالث

## مرحلة الفحص

مازلنا نتحدث عن تجميع البيانات ومرحلة الفحص هي المرحلة الثانية من تجميع البيانات التي قد بدأناها في الفصل السابق .

لكن في هذه المرحلة سوف نبدأ بجمع المعلومات بشكل أدق .



تحذير

هذه المرحلة تعتبر مرحلة خطيرة لأنك تقوم بفحص الأجهزة والشبكات وتتعرف علي معلومات

ليست من حقك فيجب ان تقوم باستخدام محاكات الأنظمة مثل : **VMware**

### Virtual machine

مرحلة الفحص تتضمن ثلاث عناصر رئيسية .

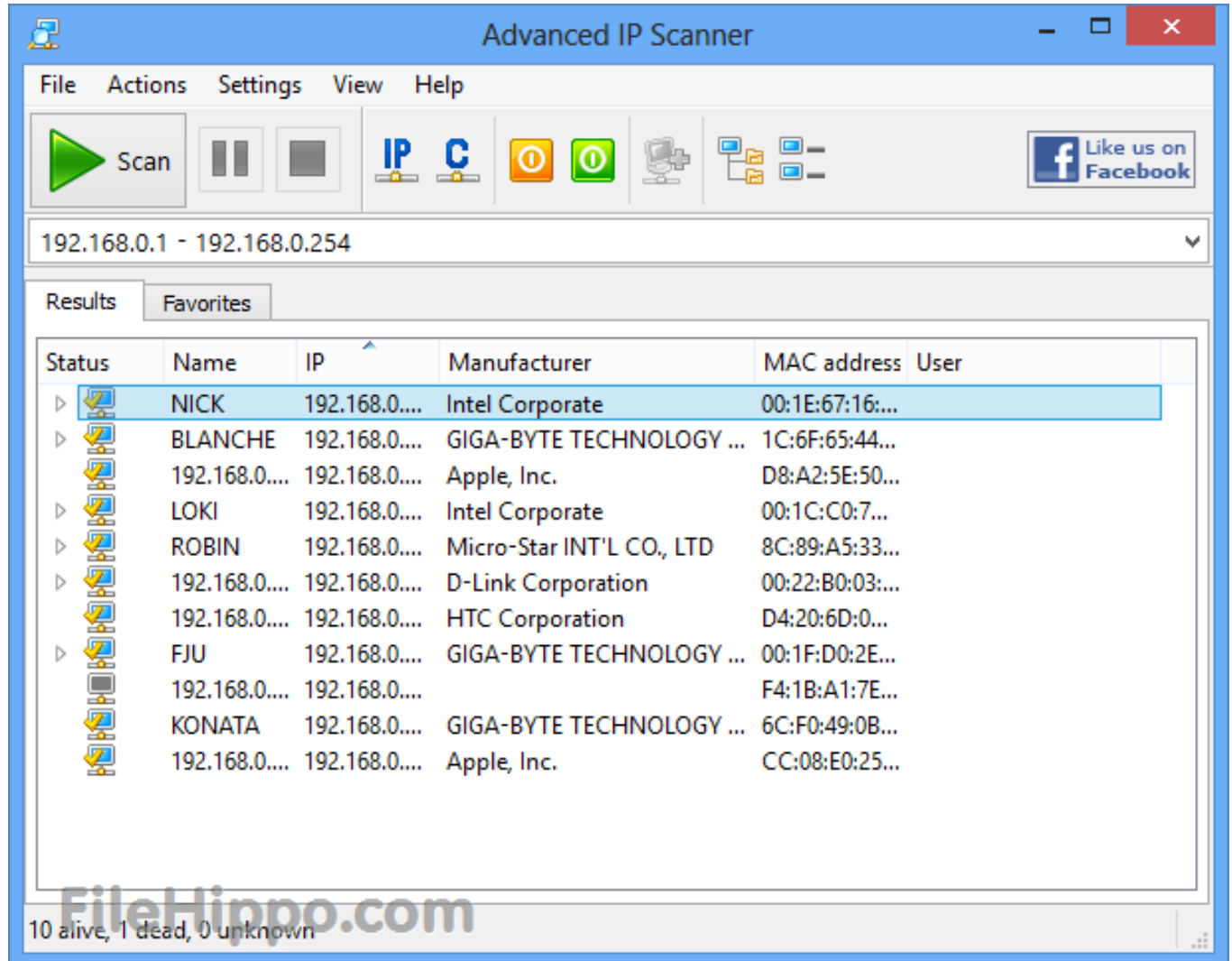
#### 1 – فحص الشبكات

المقصود من فحص الشبكة هو معرفة عدد الأجهزة التي توجد في الشبكة وأرقام التعريف الخاصة بها بواسطة بعض

البرامج مسماها العلمي **ping swapper**

مثل: **Nmap , advanced ip scanner**





## 2 – فحص الأجهزة

وهي المرحلة التي نتعرف فيها علي بعض المعلومات الخطيرة عن الأجهزة التي توجد في الشبكة مثل :

(معرفة أنظمة التشغيل الخاصة بالأجهزة , معرفة المنافذ المفتوحة داخل الأجهزة )

ويمكننا الاعتماد علي هذه الأدوات في الفحص

**nmap {1**

**Wireshark {2**

طريقة تنفيذ الأداة :

يوجد أكثر من مرحلة في الاتصال بين الأجهزة وسوف نقوم باستعراض أهم مرحلتين

المرحلة الأولى : عندما يقوم المخترق بفحص جهاز الضحية بأحد الأدوات

ينشأ اتصال بين الجهازين وهو ما يسمى الاتصال الثلاثي وخطواته كالآتي :-

1 - يقوم جهاز الهاكر بإرسال دفعة من بيانات إلى الجهاز المستهدف تسمى : **syn**

2 - يقوم جهاز المستهدف باستقبال هذه الدفعة من البيانات وإرسال تأكيد يسمى : **Ack/syn**

3 - يقوم جهاز الهاكر بإرسال دفعة من البيانات تسمى : **Syn/ack**

وهذا مثال توضيحي أكثر

فهذه العملية تشبه بمكالمة هاتف :-

الطرف الأول : الو **Syn**

الطرف الثاني : الو مين **ack**

الطرف الأول : يبدا الحديث

المرحلة الثانية : تتمثل في هذه الخطوات :-

1 - الجهاز الأول يرسل حزمة بيانات تسمى : **Syn**

2 – الجهاز الثاني يرسل حزمة بيانات تسمى : **Ack**

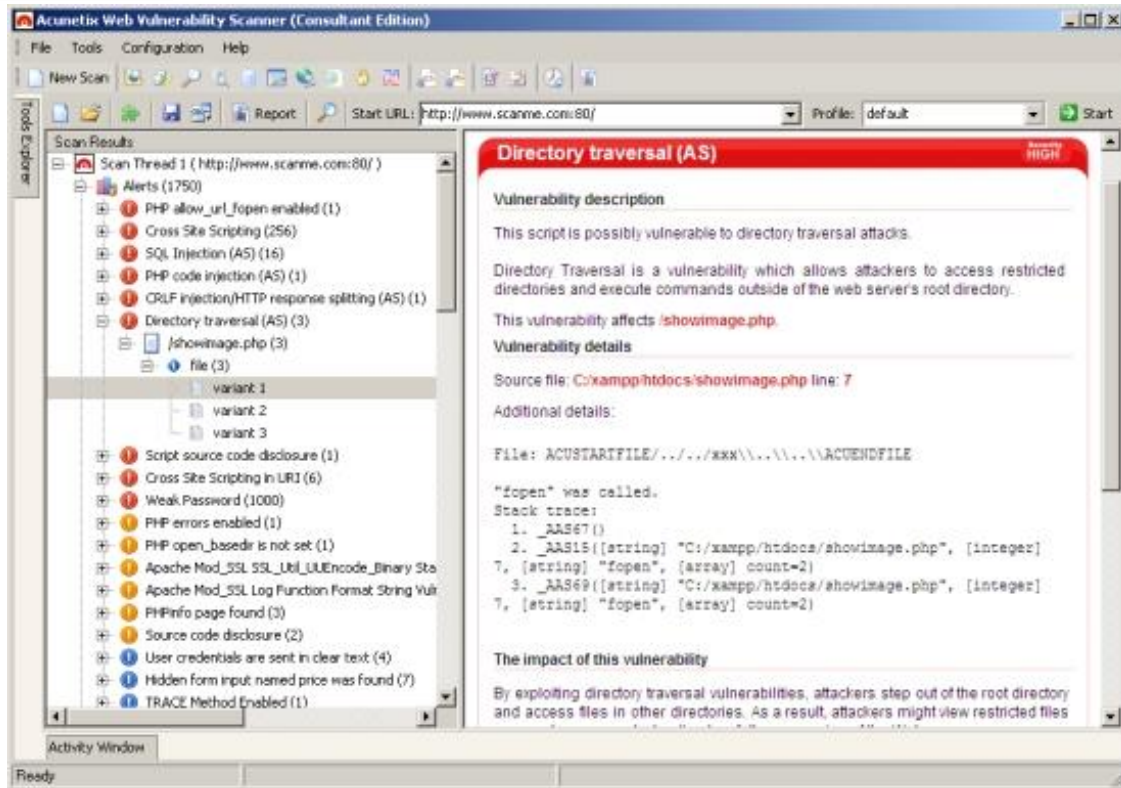
3 – الجهاز الأول يرسل حزمة بيانات تسمى : **Fin**

أي إنهاء العملية وتسمى هذه العملية (half scan)

3 – فحص السيرفرات

وهو يتمثل في فحص المواقع الديناميكية التي تقوم علي قواعد بيانات والتفاعل مع المستخدمين بحيث يوجد جانب للسيرفر يقوم فيه عمليات معالجة البيانات و طالما ما يكون في هذه الجزئية ثغرات والجزء الثاني الذي يظهر عند العميل ويتمثل في نصوص و صور هياكل ويمكن ان يكون به ثغرة حيث يقوم الهاكر بحقن هذه الصفحات ببعض الاكواد الخبيثة التي تقوم بفتح منافذ داخل الجهاز الخاص بك او تحميل بعض الفيروسات ويمكن ان تقوم بكشف هذه الثغرات من خلال أدوات التي تقوم بالكشف عن الثغرات ومن ثم عمل تقرير عوضا عن ان تقوم باكتشافها يدويا فمثل هذه الأدوات

(owasp , nikto , Acunetix )



## طرق المكافحة

طرق المكافحة هنا هجومية أكثر من أن تكون دفاعية فيجب أن تقوم باكتشاف ثغراتك قبل غيرك .

- 1 - محاولة عمل فحص على الشبكة والأجهزة وقفل المنافذ الغير مستعملة .
- 2 - تفعيل بما يسمى **Firewall** وتحديثه باستمرار .
- 3 - قم باكتشاف الثغرات واستخدام أكثر من أداة حتي تتأكد ان النظام خالي من الثغرات من قبل تقرير الأدوات .



New system technology – Mahmoud said

## الفصل الرابع

## الاختراق

تختلف طرق الاختراق باختلاف الهدف منه وباختلاف نوع المستهدف فيمكن ان يكون المستهدف موقع او جهاز في شبكة او شبكات قواعد بيانات وسيرفرات كما وضحنا سابقا .

يجب تطبيق الفحص وجمع المعلومات لكي تكون مؤهلاً لاختراق أي نوع من هذه الأنواع .

### أولا أنواع كلمات السر واختراقها

اخترق كلمات السر أكثر أنواع الاختراقات شيوعاً وذلك لسهولة هذا ناتج عن ضعف ثقافة المستخدم

فيمكن ان يقوم المستخدم باستعمال كلمة سر يسهل استنتاجها او توقعها مثل : اسم احد أولاده او تواريخ ميلاد او ارقام الهواتف .

والكثير من المستخدمين يستعمل كلمة مرور واحدة لكل حساباته فيكون أكثر عرضه للاختراق كليا .

### أنواع كلمات السر

- 1 – كلمة سر بها حروف
- 2 – كلمة سر بها حروف و ارقام
- 3 – كلمة سر بها حروف وأرقام ورموز

## طرق الحصول علي كلمة السر

1 – طريقة الكراك

2 – طريقة Sniffer

3 – طريقة Key logger

4 – طريقة الهندسة الاجتماعية

سوف نستخدم ثلاثة من هذه الطرق لتوضيح كيفية اختراق كلمة السر

طريقة الكراك :

تعتمد هذه الطريقة علي استخدام بعض البرمجيات علي الانترنت او داخل النظام حيث تقوم بعمل اتصال بالحساب الذي تريد اختراقه وذلك بإدخال كلمات مرور بشكل متكرر حتي تقوم بإيجاد كلمة المرور الصحيحة ومن اشهر هذه الأدوات هي ” hydra “



## ثانيا استخدام Key logger

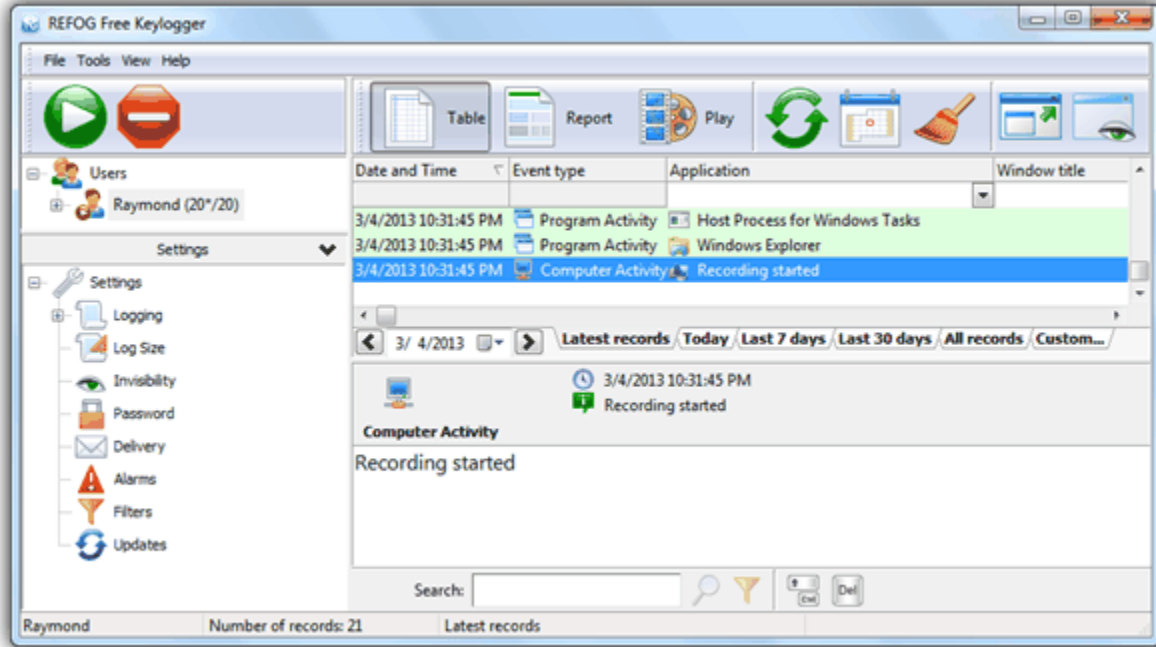
هو برنامج يستخدم للحصول علي أي بيانات فور كتابتها في الهاتف او علي الأجهزة ثم يقوم بنقل هذه المعلومات الي الهاكر عن طريق بريد الكتروني .

ملحوظة :

كان الاستخدام الأساسي للـ **Key logger** لفرض الرقابة علي الصغار في المنزل او مدير الأنظمة في الشركة علي الموظفين لمنع دخول الفيروسات .

فيمكن ان يقوم المستخدم بفتح برنامج قد أعطاه اليه شخص ولا يعرف الاضرار التي تقع عليه من خلال هذا البرنامج ثم يقوم المستخدم بالدخول علي حساباته فمن هذه اللحظة يبدأ الهاكر بأخذ كلمات المرور .





### ثالثا الهندسة الاجتماعية

مفهوم الهندسة الاجتماعية :

التأثير علي الأشخاص ببعض المعلومات التي تعرفها عنه ومن ثم بناء جدار الثقة الي ان تقوم بخداعه واختراقه .

تعتمد الهندسة الاجتماعية علي ضعف الوعي لدي المستخدمين فهذا ما يجعلهم عرضة لاستقبال برامج من أي جهة تعرض عليهم استخدامها بمقابل مادي.

او انه يثق في هذه الجهة كالبنوك والشركات التي يتعامل معها ولا يلتفت الي الأسماء والرموز الغريبة التي تكون مرفقة بجانب اسم المرسل فاذا استخدم البرنامج او قام بفتح رابط فانه يعمل علي سرقة كلمات السر الخاصة به .

## طرق المكافحة

1 – استخدام كلمات مرور قوية ويكون بها حروف ورموز وأرقام غير متعلقين بشخص المستخدم , مثال :

**P-6651@\$var**

2 – التحقق من البرامج التي يقوم باستخدامها واستخدام مكافح الفيروسات قبل فتح البرنامج

3 – عدم تحميل او فتح ملفات عن طريق البريد او أي موقع تواصل بدون التحقق منها

عن طريق موقع **Virus total**

4 – عدم الضغط علي أي إعلانات تقوم بفتح نوافذ كثيرة داخل المتصفح ووضع أداة

**Block ads**



## الفصل الخامس

## تثبيت الاختراق

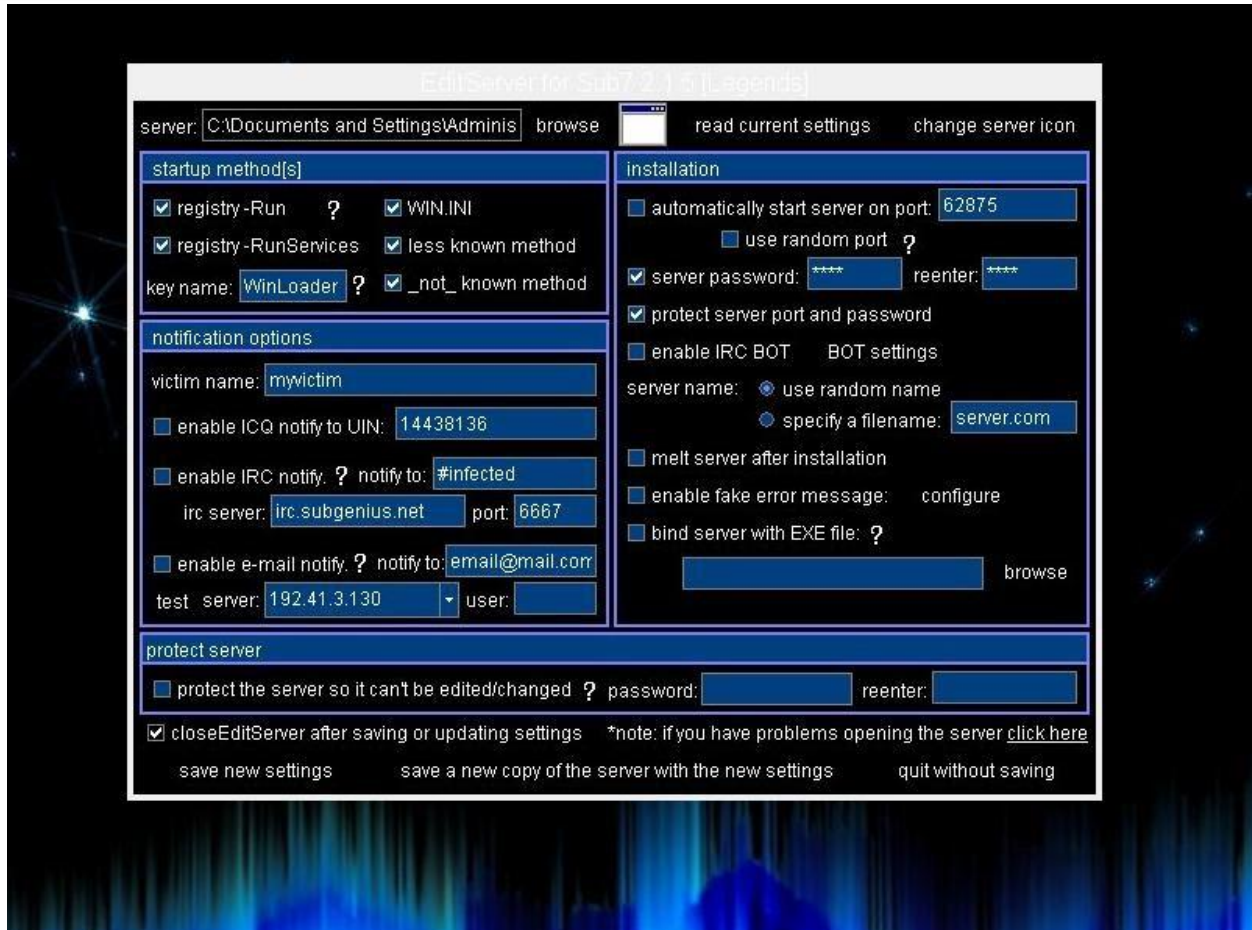
عادة ما يبحث المخترق عن طريقة تسمح له بفتح منفذ علي جهاز المستهدف لكي يقوم بالدخول مرة اخري بعد الاختراق حتي لا يقوم بعمل عملية الاختراق دائما وهذا ما يسمى بتثبيت الاختراق .

## شرح مصطلح Backdoor

هو عبارة عن برامج صغيرة ترسل للمستهدف علي هيئة صور او ملفات او مختبئة داخل برامج اخري

تقوم بفتح منافذ جهاز المستهدف ومن اشهر البرامج القديمة **Subseven**

وهذا البرنامج يتيح للهacker ان يتحكم في جهاز المستهدف عن طريق سيرفر يقوم بعمل اتصال بين جهاز المستهدف وجهاز الهاكر .

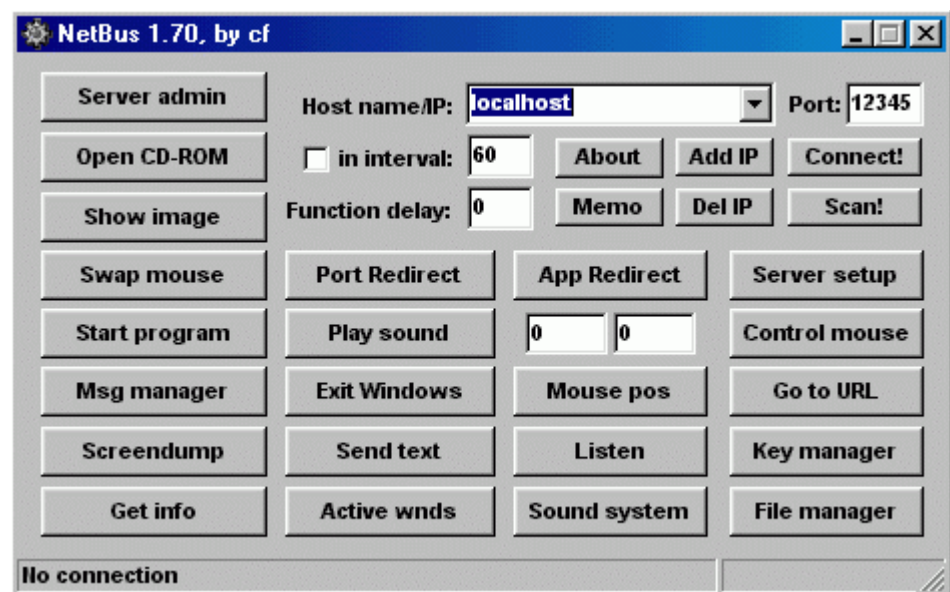


## مخاطر الأبواب الخلفية (backdoors)

- 1 – يمكن للهاكر نقل ملفات من جهاز المستهدف
- 2 – نقل أي فيروسات أخرى إلى الجهاز
- 3 – معرفة جميع كلمات المرور المخزنة
- 4 – تشغيل الكاميرا والتحكم الكامل بجهاز المستهدف

برامج مستعملة اخري مثل :

(beast , netbus )



## استخدام الفيروس (virus)

هو برنامج يقوم الهاكر بإرساله للضحية ويقوم بتشغيل نفسه أوتوماتيكيا وينسخ نفسه داخل ملفات النظام ويقوم بأعمال تدميرية .

### اعراض إصابة الفيروس

- 1 – عطل في مكونات الجهاز
- 2 – البطء الشديد للجهاز
- 3 – يصدر صفيرا وتتحول الشاشة الى زرقاء

### سلوكيات الفيروس

- 1 – يقوم بمسح او اتلاف الملفات التنفيذية
- 2 – تدمير بعض ملفات النظام
- 3 – يقوم بنسخ نفسه داخل الملفات

## استخدام الديدان (worms)

تشبه الي حد كبير للفيروس في اثره المدمرة وخصائصه ولكنها ينتقل من وحدة تخزين الي اخري بدون أي تدخل اما الفيروس فيجب ان تقوم بنقل الملف المصاب حتي ينتقل .

### طرق المكافحة

- 1 – التحقق من الروابط التي يقوم المستخدم بالتحميل منها فيجب ان يكون الموقع موثوق به
- 2 – التحقق من البرامج المستخدمة يوميا عن طريق فحصها بمكافح الفيروسات
- 3 – يعمل تحديث للأنظمة
- 4 – تحميل الألعاب من أماكن موثوق بها وعدم نسخها من أماكن اخري





## الفصل السادس

## ازالة اثار الاختراق

الخطوة الأهم والأخيرة التي قد تعرفها عن حقائق الهاكر .

### أهمية إزالة اثر الاختراق

انهم يلجؤون الي إزالة اثار الاختراق ويهتمون بهذه المرحلة بشكل كبير حتي لا يتم الكشف عن هويتهم  
ملحوظة :

يلجأ بعض الهاكر بتدمير محتويات الأجهزة مثل :

**(hard disk , flash memory)**

لكي لا يكون هناك ادلة تدينهم .

### كيفية إزالة اثر الاختراق

هذه المرحلة تنقسم الي قسمين :-

1 – إزالة السيرفرات التي استخدمها في جهاز المستهدف ومسح الملفات المخزنة **Logs**

من عند المستهدف ويقوم بحذف الاتصال نهائيا .

2 – يقوم الهاكر بحذف السجلات او يقوم بحذف النظام الذي يعمل عليه اذا كان **Virtual machin**

## طرق المكافحة

1 – استخدام احدث برامج الحماية والتي من الصعب حذف السجلات منها

2 – استخدام برامج **Recovery logs**

3 – الاستعانة بخبير محلل جنائي رقمي اذا كانت شركة او منظمة كبيرة



New system technology – Mahmoud said

الخاتمة

ملخص :

تعلمنا من هذا الكتاب :-

خمسة طرق رئيسية لأي هجوم ناجح وكيفية صد هذه الهجمات من العالم الخارجي.

أولا يجب ان تقوم بجمع معلومات حتي تعرف اذا كان هذا الهدف تريد حقا اختبار اختراقه ام لا "تحديد الهدف " الحقيقة الاولى .

ثانيا بعد ان تقوم بتحديد الهدف فيجب ان تقوم بدراسته بشكل ادق مما تعرف ما هي نقاط الضعف الخاصة به "تحديد نقاط الضعف " الحقيقة الثانية .

ثالثا بدء عملية الاختراق ولكنها الأطول لأنك تأخذ وقت كبير في كسر تشفير كلمات مرور او محاولة اختراق ثغرة او تشفير رابط معين او بناء صفحة ويب لاصطياد المستهدف عن طريق الهندسة الاجتماعية فمنها الواقعي بحيث تقوم بنفسك ببناء جدار الثقة او الوهمية بانتحال شخصية اخري "التحايل واقوي الأدوات لفك التشفير " الحقيقة الثالثة .

رابعا تثبيت الاختراق فكيف يقوم الهاكر باستغلال الأجهزة التي قام باختراقها من قبل في هجمات اخري ليس باختراقها مرة اخري لأنها تكون عملية مجهدة , بل بعمل أبواب خلفية داخل الأنظمة حتي يستطيعوا التحكم بالأجهزة متي يشاؤون فهي تفيد جدا في هجمات حجب الخدمة حيث يستغل الأجهزة المسيطر عليها حتي يقوم

بإرسال حزم بيانات الي بعض المواقع والخدمات واسقاطها "أبواب خلفية واستخفاف بعقلية المستهدف " الحقيقة الرابعة .

خامسا إزالة اثر الاختراق حتي لا يتعرض الي هجوم او مساءلة قانونية فاذا كشفت هويته اصبح عرضة للسجن " الخوف يولد معرفة كبيرة بإزالة اثار الجريمة " الحقيقة الخامسة .

الترتيب في الفكر والتكنيك هو من اهم الصفات التي يتمتع بهم الهاكر الحقيقي

وما قد تحدثنا عنه هو مجرد شيء قليل من العلم الذي يوجد بداخل هذا العالم التقني المريب

ولكن لا تقلق عزيزي القارئ فانت اذا كنت تريد ان تتعمق في هذا العلم فيعتبر هذا الكتاب

اول خطوة من الالف خطوة حين تكون قد فرغت من القراءة فيمكنك البحث خلال الانترنت

ومعرفة الكثير والكثير من الأساليب المتبعة في عالم الهاكر ولا تقلق سوف أكون معك في

إصدارات اخري لهذا الكتاب وأساليب احدث وتجارب وقصص ممتعة ومفيدة .

يتوارد الي ذهنك الان ماذا بعد لا تقلق ستراني اجيب علي هذا السؤال في الجزء الأسفل

من الكتاب .

ماذا بعد :

1 – ان تتعمق في أساليب جديدة

2 – تذهب الان الي الانترنت وتبحث عن افضل المواقع التي تتحدث عن هذه الثغرات

3 – قم بتعلم أنظمة التشغيل مفتوحة المصدر مثل : لينوكس

4 – قم بالدخول الي المسار التعليمي الاكاديمي لتحصل علي اول شهادة هي :

**CEH , CHFI ...**

5 – انضم الي جروبات تتحدث عن الكثير من البرامج الجديدة ولكن احذر وان تستخدم

جهازك الأصلي وانت تجرب هذه البرامج

6 – وهو اهم شيء هو تعلم البرمجة وانتظروا منا أيضا كتب عن تعلم لغات البرمجة

قريبا ...

انتظروا اعمال اخري :

لينوكس بالعربي

**OOP in C++**

**CEH for ALL in Arabic**

مقدمة في علم الخوارزميات

**JavaScript** تطبيقات حياتية علي