Hacking the Virtual World

Jason Hart CISSP CISM

SafeNet, Inc.

Session ID: HTA-302

Session Classification: Advanced

RSA CONFERENCE EUROPE 2012

About Me

Legal Disclaimer

ALWAYS GET PERMISSION IN WRITING.

- Performing “scans” against networked systems without permission is illegal. Password cracking too
- You are responsible for your own actions!
- If you go to jail because of this material it’s not my fault, although I would appreciate it if you dropped me a postcard.
- This presentation references tools and URLs - use them at your own risk and with permission

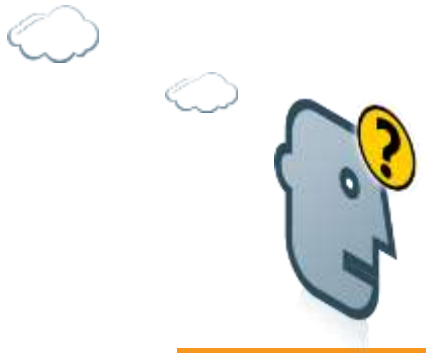
SafeNet

© SafeNet Confidential and Proprietary

Accepted Security Principles

- Confidentiality
- Integrity
- Availability
- Accountability
- Auditability

HOW DO I ACHIEVE THIS IN A VIRTUAL WORLD?



SafeNet

© SafeNet Confidential and Proprietary

Welcome to the next Generation

- 1st Age: Servers
  - Servers
  - FTP, Telnet, Mail, Web.
  - These were the things that consumed bytes from a bad guy
  - The hack left a foot print
- 2nd Age: Browsers:
  - Javascript, ActiveX, Java, Image Formats, DOMs
  - These are the things that are getting locked down
    - Slowly
    - Incompletely
- 3rd Age: Virtual Hacking: - **Simplest and getting easier**
  - Gaining someone's password is the skeleton key to their life and your business
  - Accessing data from the virtual world can be simple

SafeNet

© SafeNet Confidential and Proprietary

Virtual Word – With Virtual Back Doors

Welcome to the Future

- Cloud Computing
- Virtual Environment
- With Virtual Security holes

During the past 15 years with learnt nothing

© SafeNet Confidential and Proprietary

Lets Start

vCenter servers directly connected to the web.....WOW

© SafeNet Confidential and Proprietary

How do the hackers hack VMware vCenter in 60 seconds?

SafeNet

© SafeNet Confidential and Proprietary

The Target

Vmware vCenter Version 4.1 update 1 .....

- Services running:
  - Update Manager
  - vCenter Orchestrator
  - Chargeback

- Each Service has a web server running

Web Attack 101 .....History repeating

© SafeNet Confidential and Proprietary

The Attack

vCenter Orchestrator attack vector 1.....

Installed by default within vCenter is an very interesting file:

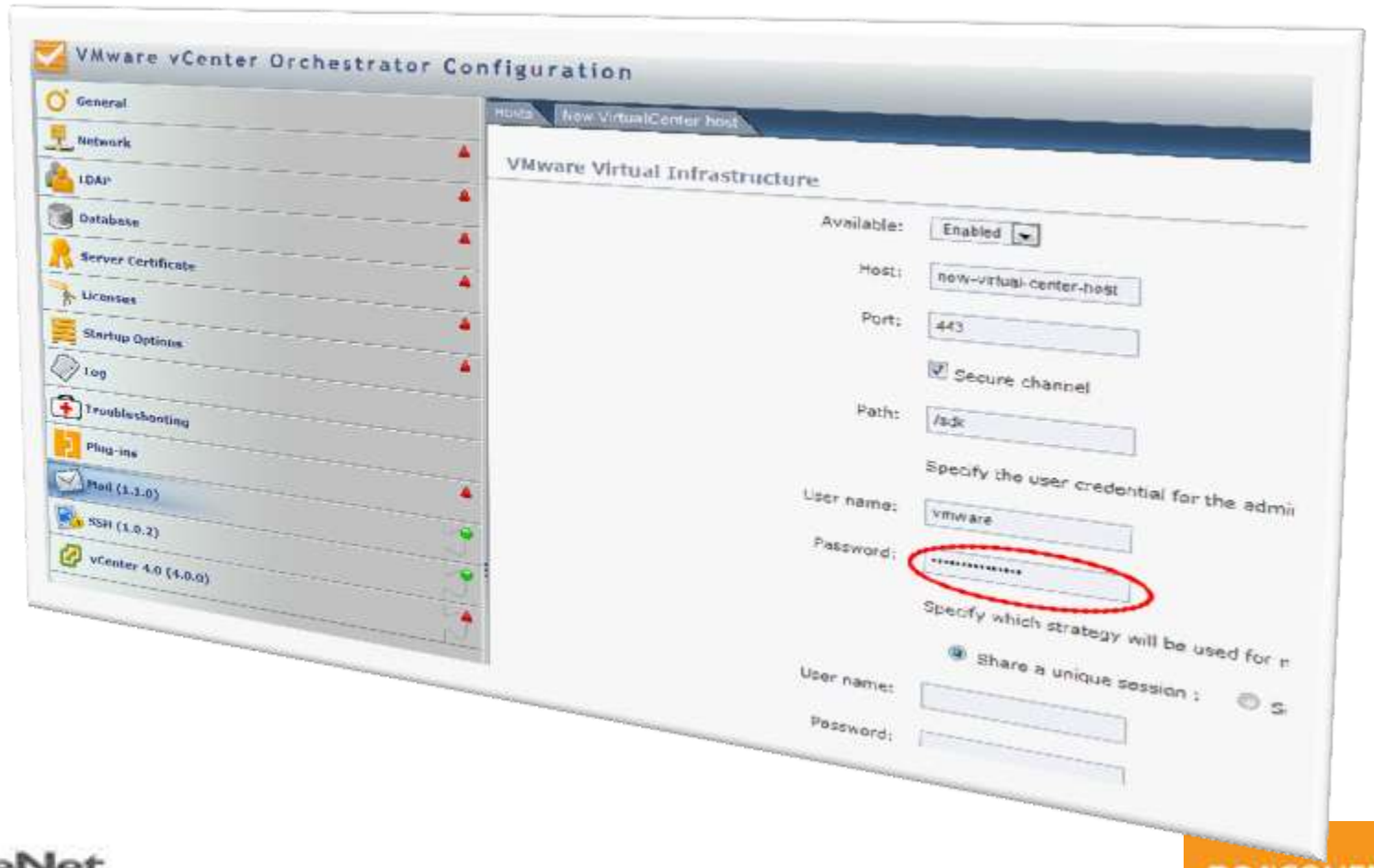
C:\Programfiles\VMware\Infrastructure\Orchestrator\configuration\jetty\etc\passwd.properties

This file contains md5 passwords and can easily be bruteforced using rainbow tables

© SafeNet Confidential and Proprietary

We are in

After bruteforcing the MD5.....



© SafeNet Confidential and Proprietary

Point & Click

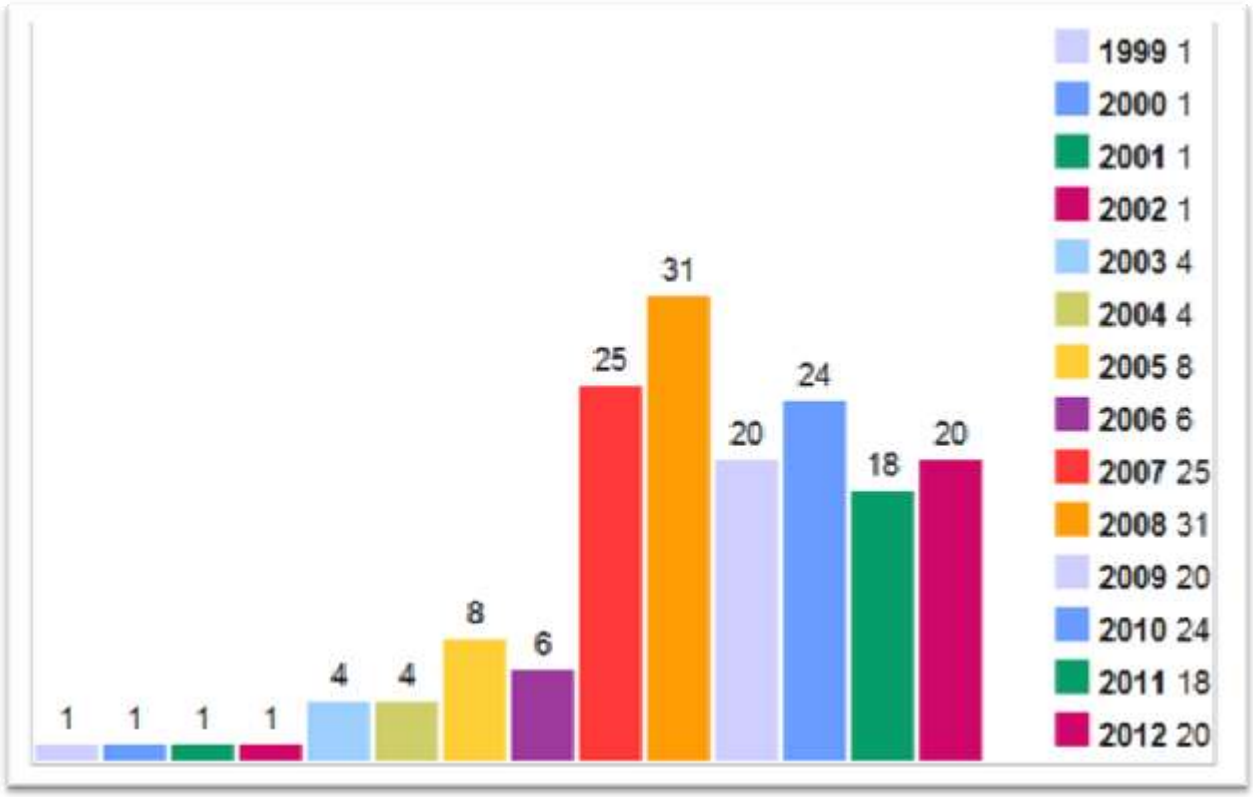
Any one can do .....

This module will log into the Web API of VMWare and try to enumerate all the login sessions

© SafeNet Confidential and Proprietary

Look

More and More Vulnerabilities. .by Year . . . .

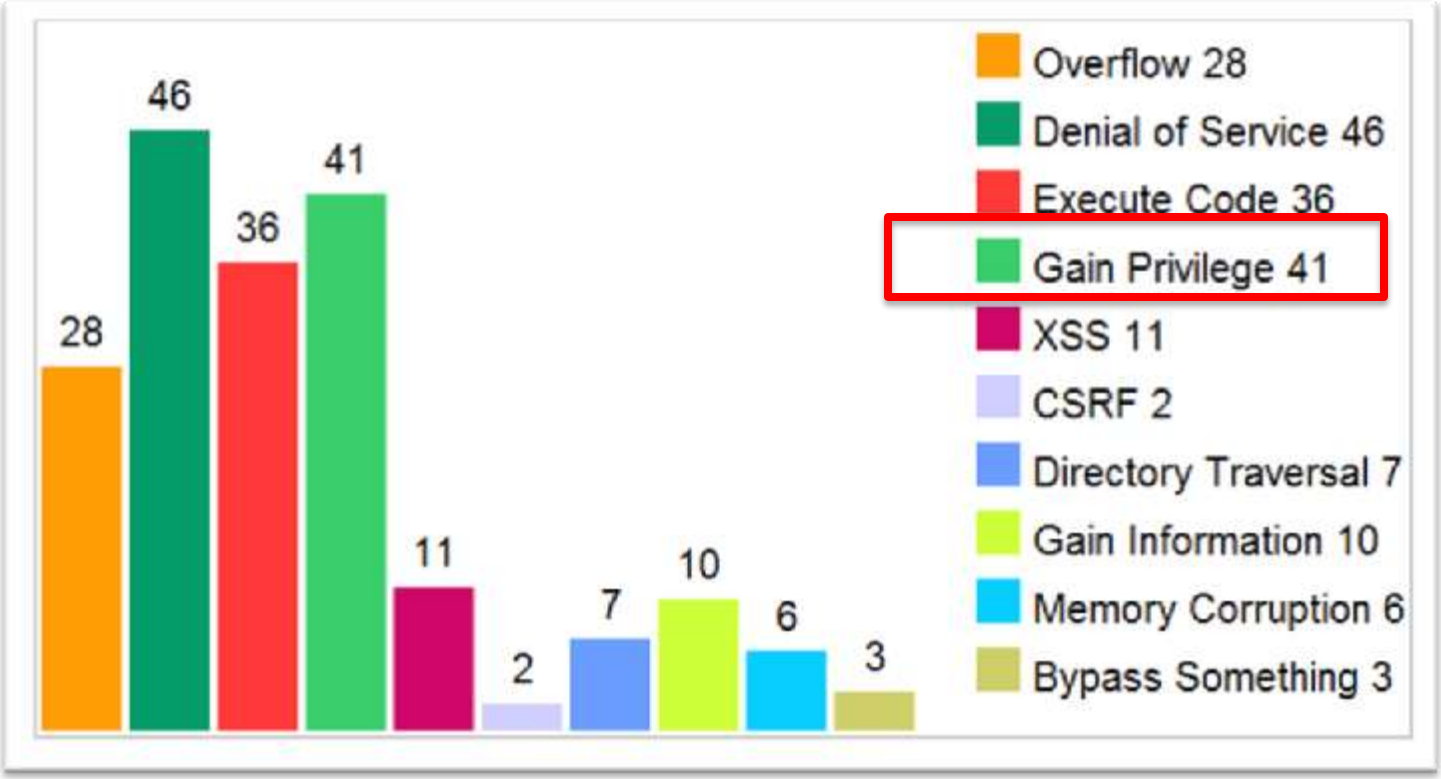


Source: http://www.cvedetails.com/vendor/252/Vmware.html

© SafeNet Confidential and Proprietary

Total

Current Vulnerabilities todate by .... Type



Source: http://www.cvedetails.com/vendor/252/Vmware.html

© SafeNet Confidential and Proprietary

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : Cve Number Descending Cve Number Ascending CVSS Score Descending Number Of Exploits Descending

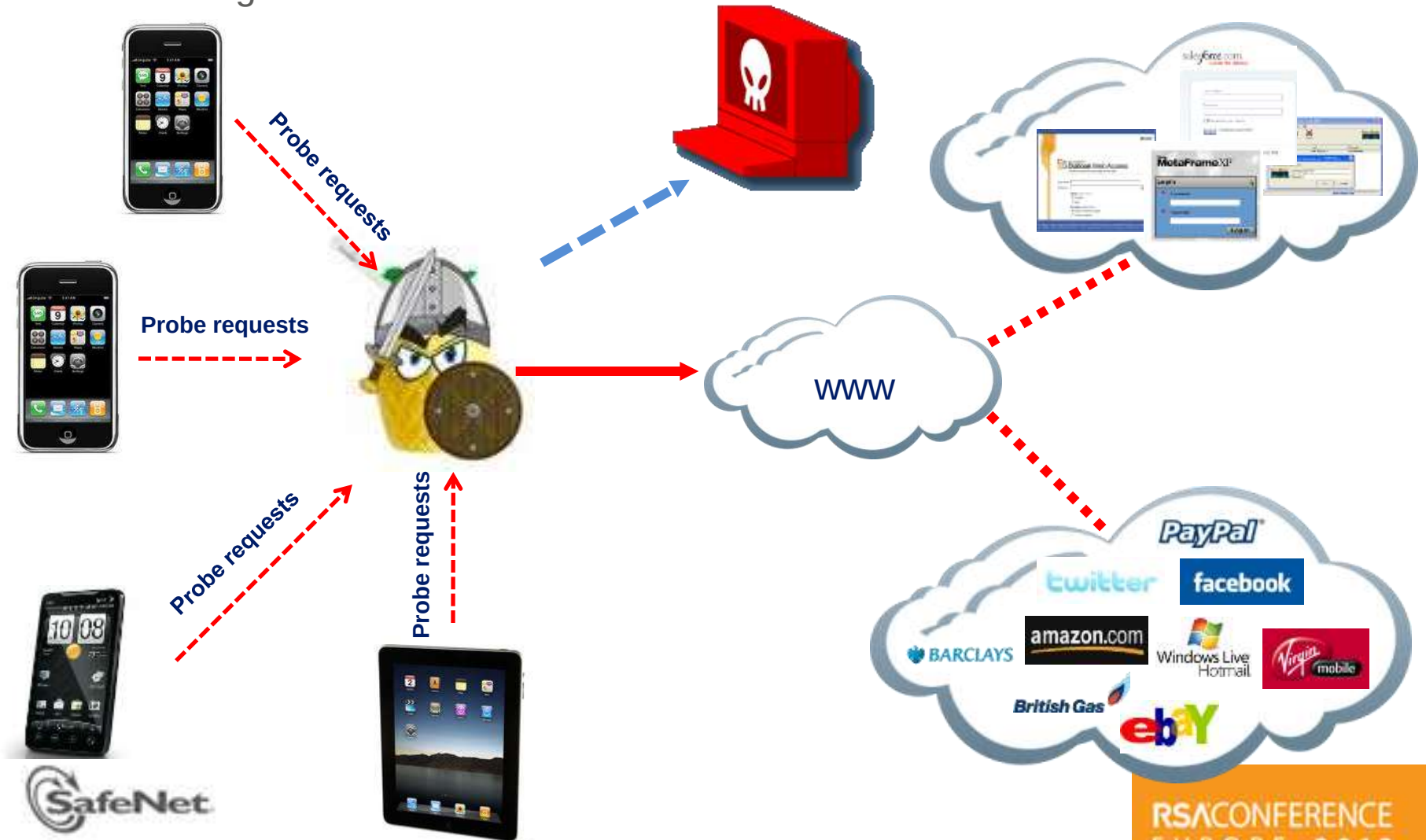
#	CVE ID	CWE ID	# of Exploits	Vulnerability Type (s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	C
20	CVE-2009-1147			+Priv	2009-04-06	2010-08-21	7.2	None	Local	Low	Not required	C
Unspecified vulnerability in vmci.sys in the Virtual Machine Communication Interface (VMCI) in VMware Workstation 6.5.1 and earlier, VMware Player 2.5.1 and earlier VMware Server 2.0.x before 2.0.1 build 156745 allows local users to gain privileges via unknown vectors.												
21	CVE-2008-4915	264		+Priv	2008-11-10	2010-08-21	6.9	Admin	Local	Medium	Not required	C
The CPU hardware emulation in VMware Workstation 6.0.5 and earlier and 5.5.8 and earlier; Player 2.0.x through 2.0.5 and 1.0.x through 1.0.8; ACE 2.0.x through 2. 1.0.7; Server 1.0.x through 1.0.7; ESX 2.5.4 through 3.5; and ESXi 3.5, when running 32-bit and 64-bit guest operating systems, does not properly handle the Trap fl OS users to gain privileges on the guest OS.												
22	CVE-2008-4281	22		+Priv Dir. Trav.	2008-11-10	2010-08-21	9.3	None	Remote	Medium	Not required	C
Directory traversal vulnerability in VMWare ESXi 3.5 before ESXe350-200810401-O-UG and ESX 3.5 before ESX350-200810201-UG allows administrators with the Dat gain privileges via unknown vectors.												
23	CVE-2008-4279	264		+Priv	2008-10-06	2009-09-08	6.8	Admin	Local	Low	Single system	C
The CPU hardware emulation for 64-bit guest operating systems in VMware Workstation 6.0.x before 6.0.5 build 109488 and 5.x before 5.5.8 build 108000; Player 2.0 before 1.0.8; Server 1.x before 1.0.7 build 108231; and ESX 2.5.4 through 3.5 allows authenticated guest OS users to gain additional guest OS privileges by triggering CPU to perform an indirect jump to a non-canonical address.												
24	CVE-2008-3698	264		+Priv	2008-09-03	2009-01-29	7.2	None	Local	Low	Not required	C
Unspecified vulnerability in the OpenProcess function in VMware Workstation 5.5.x before 5.5.8 build 108000, VMware Workstation 6.0.x before 6.0.5 build 109488, VM 108000, VMware Player 2.x before 2.0.5 build 109488, VMware ACE 1.x before 1.0.7 build 108880, VMware ACE 2.x before 2.0.5 build 109488, and VMware Server be allows local host OS users to gain privileges on the host OS via unknown vectors.												
25	CVE-2008-2097	119		Overflow +Priv	2008-06-05	2011-06-20	9.0	Admin	Remote	Low	Single system	C
Buffer overflow in the openwsman management service in VMware ESXi 3.5 and ESX 3.5 allows remote authenticated users to gain privileges via an "invalid Content-												
26	CVE-2008-1363	264		+Priv	2008-03-19	2011-06-24	7.2	Admin	Local	Low	Not required	C
VMware Workstation 6.0.x before 6.0.3 and 5.5.x before 5.5.6, VMware Player 2.0.x before 2.0.3 and 1.0.x before 1.0.6, VMware ACE 2.0.x before 2.0.1 and 1.0.x be before 1.0.5 on Windows allow local users to gain privileges via an unspecified manipulation of a config.ini file located in an Application Data folder, which can be used												
27	CVE-2008-1362	264		DoS +Priv	2008-03-19	2008-09-05	7.2	Admin	Local	Low	Not required	C
VMware Workstation 6.0.x before 6.0.3 and 5.5.x before 5.5.6, VMware Player 2.0.x before 2.0.3 and 1.0.x before 1.0.6, VMware ACE 2.0.x before 2.0.1 and 1.0.x be before 1.0.5 on Windows allow local users to gain privileges or cause a denial of service by impersonating the authd process through an unspecified use of an "insecu vulnerability than CVE-2008-1361.												

VMware Workstation 6.5.x before 6.5.3 build 185404, VMware Player 2.5.x before 2.5.3 build 185404, VMware ACE 2.5.x before 2.5.3 build 185404, VMware Server 1 2.x before 2.0.2 build 203138, VMware Fusion 2.x before 2.0.6 build 196839, VMware ESXi 3.5 and 4.0, and VMware ESX 2.5.5, 3.0.3, 3.5, and 4.0, when Virtual-8086

```
43823 50:ea:d6:91:bc:93 172.16.42.103 isiks-iPhone 01:50:ea:d6:91:bc:93
43799 c8:bc:c8:ea:59:13 172.16.42.215 GhostMAC 01:c8:bc:c8:ea:59:13
43735 a8:6a:6f:ca:c8:c0 172.16.42.163 BLACKBERRY-E7B4 01:a8:6a:6f:ca:c8:c0
43663 28:6a:ba:1a:6d:fc 172.16.42.224 Mr-Macs-ipad 01:28:6a:ba:1a:6d:fc
43647 d0:23:db:41:de:8a 172.16.42.100 Martins-iPhone 01:d0:23:db:41:de:8a
43642 00:16:e3:8f:75:a1 172.16.42.177 swlpt 01:00:16:e3:8f:75:a1
43634 00:1d:fe:dc:e1:85 172.16.42.117 * *
43634 0c:60:76:65:d5:a8 172.16.42.112 FLDLP114B 01:0c:60:76:65:d5:a8
43661 14:8f:c6:c4:ba:06 172.16.42.107 Scotts-Phone 01:14:8f:c6:c4:ba:06
43626 f0:cb:a1:5e:ed:93 172.16.42.127 * 01:f0:cb:a1:5e:ed:93
43619 90:21:55:b7:a0:b0 172.16.42.170 Android_352212047584847 *
43602 78:a3:e4:e9:ac:f0 172.16.42.138 * 01:78:a3:e4:e9:ac:f0
43602 18:20:32:a8:e4:c7 172.16.42.219 iPad 01:18:20:32:a8:e4:c7
43562 24:ab:81:4d:56:5f 172.16.42.237 * 01:24:ab:81:4d:56:5f
43585 d0:23:db:2f:74:79 172.16.42.111 Jasonhs-iPhone 01:d0:23:db:2f:74:79
43444 38:e7:d8:78:f3:c1 172.16.42.225 android_20014688ba37b875 *
43407 a0:88:b4:c5:d3:fc 172.16.42.162 20141-lap 01:a0:88:b4:c5:d3:fc
43371 40:6a:ab:fd:54:59 172.16.42.227 BLACKBERRY-393E 01:40:6a:ab:fd:54:59
43697 00:26:ff:74:88:9e 172.16.42.232 BLACKBERRY-305B 01:00:26:ff:74:88:9e
43360 00:1e:65:18:e1:98 172.16.42.166 uk812211 01:00:1e:65:18:e1:98
43346 0c:74:c2:d5:05:c2 172.16.42.178 * 01:0c:74:c2:d5:05:c2
43342 90:84:0d:ae:36:ef 172.16.42.115 Nicole 01:90:84:0d:ae:36:ef
43319 00:21:6a:7f:a1:fc 172.16.42.190 UK813411 01:00:21:6a:7f:a1:fc
43673 cc:08:e0:be:d7:99 172.16.42.147 Burzuj 01:cc:08:e0:be:d7:99
43283 00:21:6a:83:ba:e0 172.16.42.128 UK813682 01:00:21:6a:83:ba:e0
43452 30:7c:30:5e:28:09 172.16.42.181 BLACKBERRY-C9B6 01:30:7c:30:5e:28:09
43652 00:23:14:2d:17:a0 172.16.42.202 uk783613 01:00:23:14:2d:17:a0
43550 4c:ed:de:60:33:c6 172.16.42.106 Jason-TOSH 01:4c:ed:de:60:33:c6
43697 18:3d:a2:1c:a9:68 172.16.42.156 uk827790 01:18:3d:a2:1c:a9:68
43270 00:1e:65:42:6b:8e 172.16.42.124 uk814617 01:00:1e:65:42:6b:8e
43665 a0:88:b4:06:e7:68 172.16.42.150 UK833187 01:a0:88:b4:06:e7:68
43264 00:21:6a:9b:c3:72 172.16.42.114 uk816008 01:00:21:6a:9b:c3:72
```

Live Attack

Against a the Cloud . . . . ARP Attack



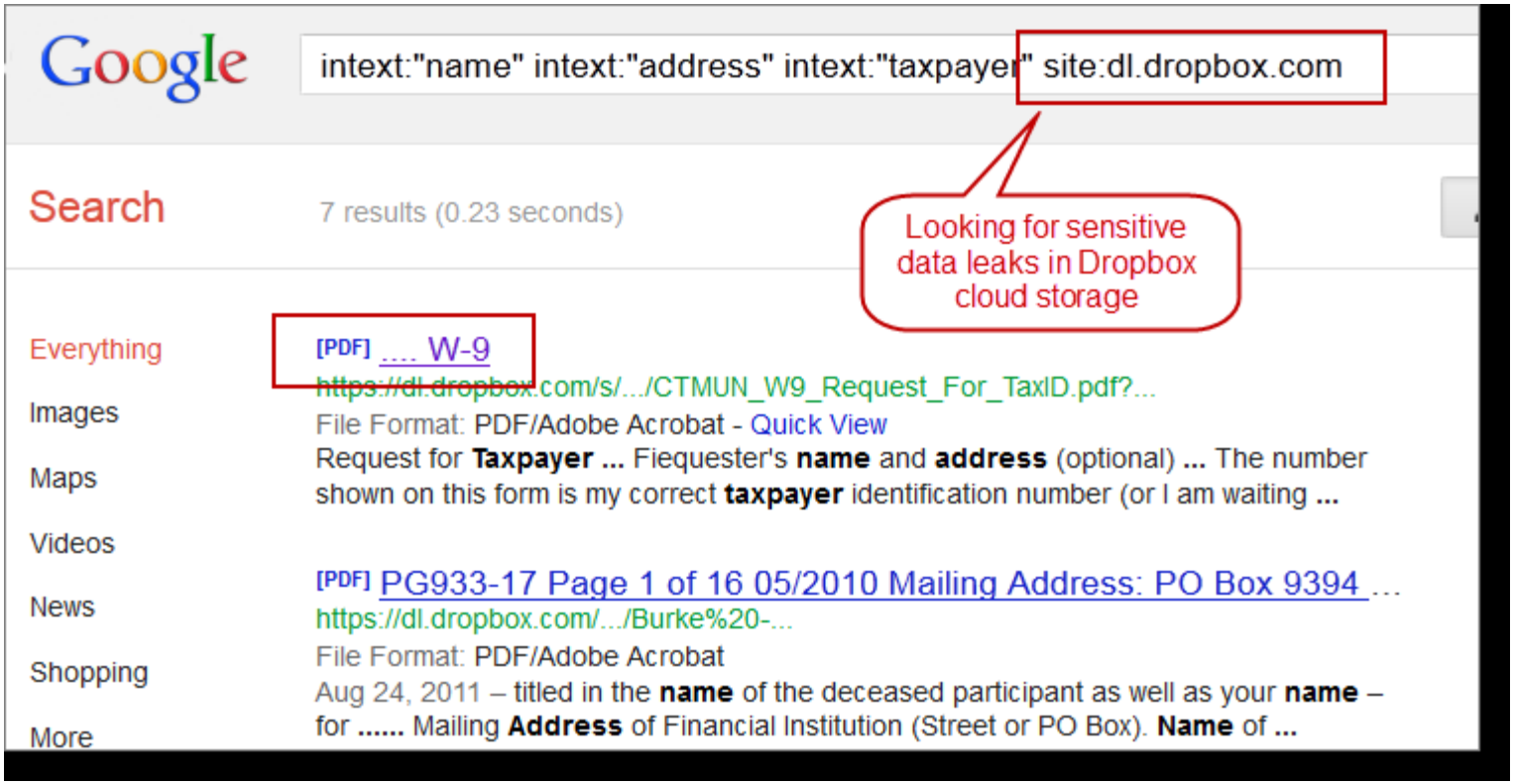
© SafeNet Confidential and Proprietary

Virtual World

With Virtual access by any one ……. With only a click

SafeNet

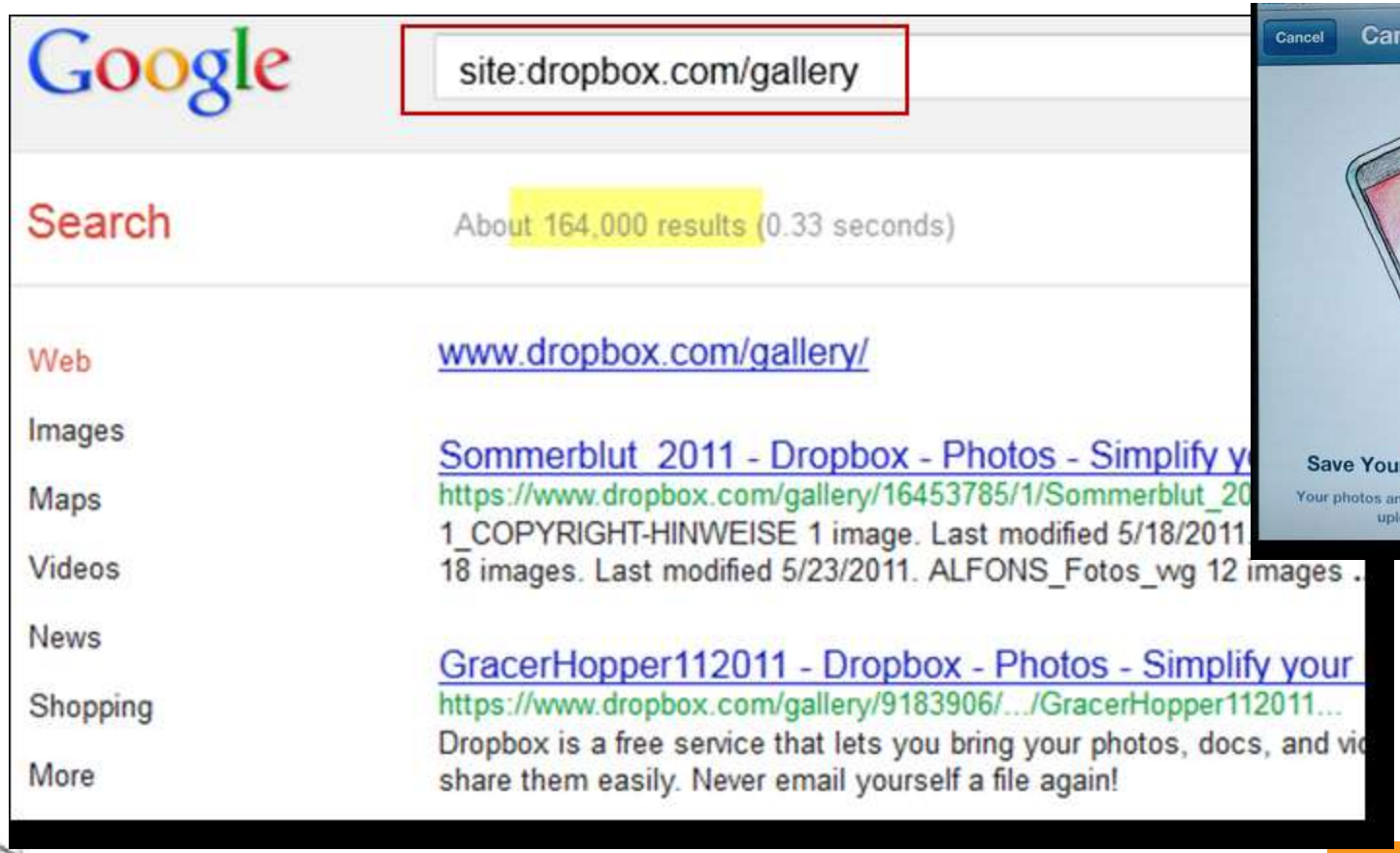
© SafeNet Confidential and Proprietary



© SafeNet Confidential and Proprietary

site:dropbox.com/gallery

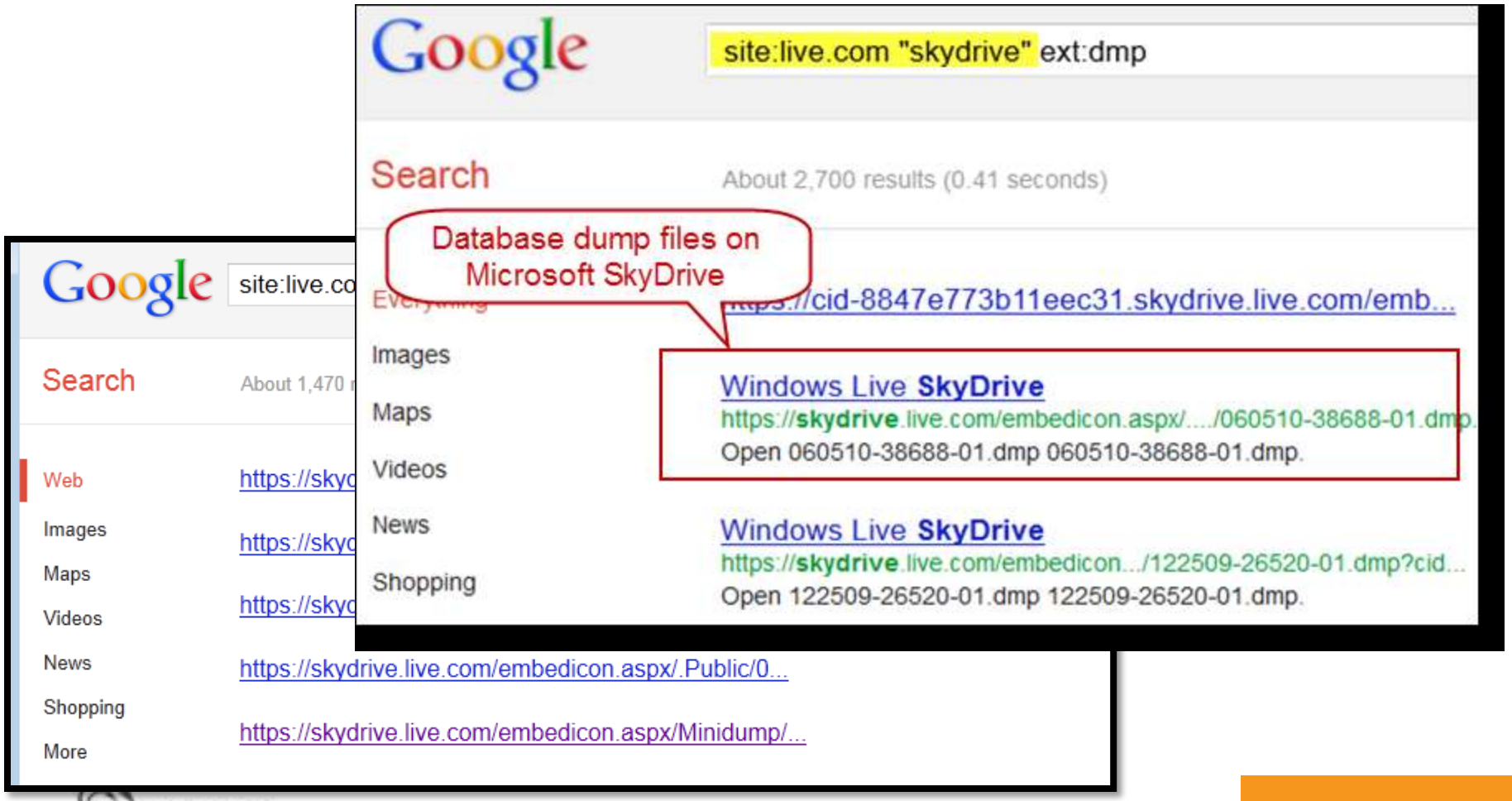
Dropbox



SafeNet

© SafeNet Confidential and Proprietary

site:live.com "skydrive" ext:dmp



© SafeNet Confidential and Proprietary

Google docs

SafeNet

© SafeNet Confidential and Proprietary

Data Loss In The News

Yale Alumni 43,000 SSNs Exposed in Excel Spreadsheet

© SafeNet Confidential and Proprietary

Cloud Security

NO PROMISES.....

Amazon AWS Customer Agreement

- http://aws.amazon.com/agreement/#10

10. Disclaimers.

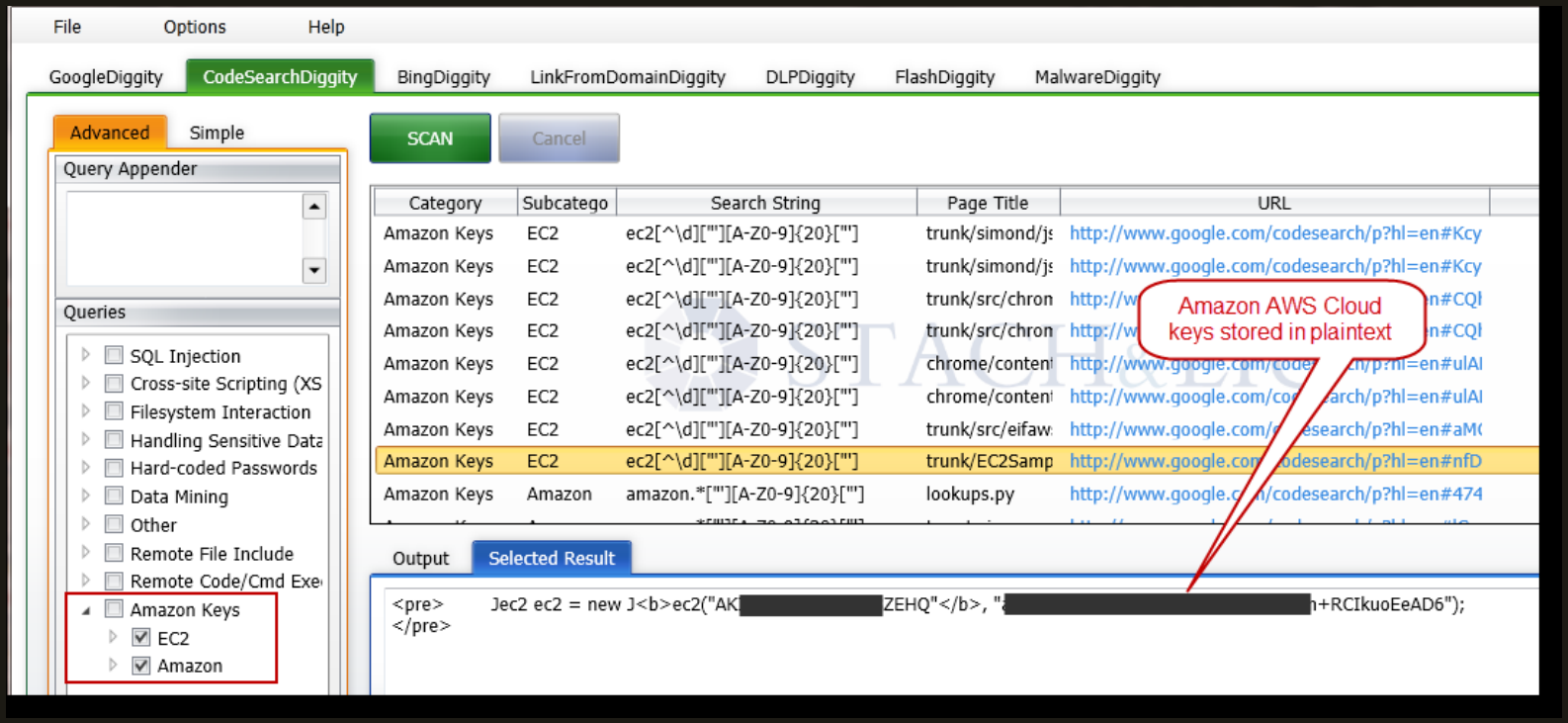
THE SERVICE OFFERINGS ARE PROVIDED "AS IS." WE AND OUR AFFILIATES AND LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICE OFFERINGS OR THE THIRD PARTY CONTENT, INCLUDING ANY WARRANTY THAT THE SERVICE OFFERINGS OR THIRD PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING YOUR CONTENT OR THE THIRD PARTY CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, WE AND OUR AFFILIATES AND LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE.

In summary no guarantee of confidentiality integrity or availability (CIA) of your data in anyway

© SafeNet Confidential and Proprietary

CodeSearch Diggity

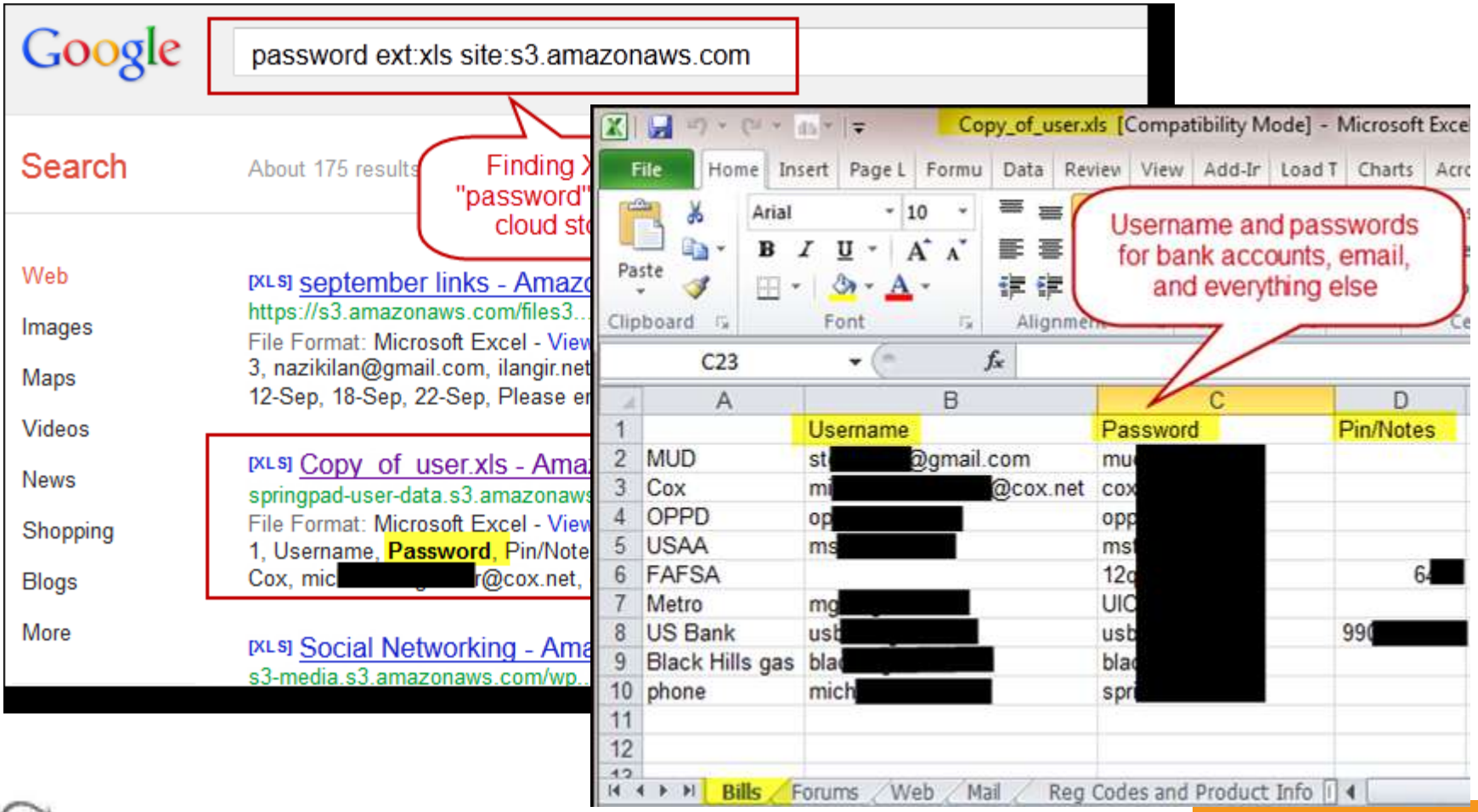
AMAZON CLOUD SECRET KEYS



Hyperlink

amazon web services™

S3 Simple Storage Service



SafeNet

© SafeNet Confidential and Proprietary

RSA CONFERENCE EUROPE 2012


facebook
digg
friendster
reddit
Meetup
StumbleUpon
Discover new
del.icio.us
social bookmarking
flickr
myspace
a place for friends
YouTube
twitter
LIVEJOURNAL


The Battle
For the Virtual
World Has
Begun

Thank you

Jason Hart CISSP CISM
VP Cloud Solutions

Jason.Hart@Safenet-inc.com

Visit us today at Stand ###

SafeNet delivers comprehensive data protection solutions for persistent protection of high value information.

© SafeNet Confidential and Proprietary