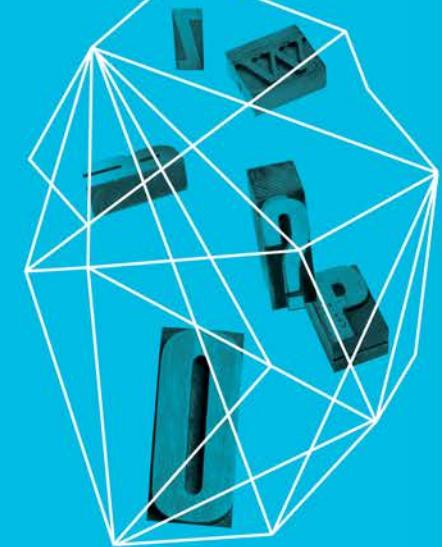


**RSA®CONFERENCE  
ASIA PACIFIC 2013**

# HACKING THE VIRTUALIZED WORLD

Jason Hart CISSP CISM  
Vice President Cloud Solutions  
SafeNet Inc

Security in  
knowledge



Session ID: CLD-T04

Session Classification: Intermediate

# 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!

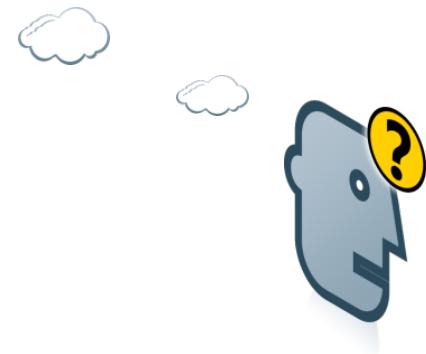
If you go to jail because of this material it's not my fault, although I would appreciate it if you dropped me a postcard. This presentation references tools and URLs - use them at your own risk and with permission

# Accepted Security Principles

- ▶ **Confidentiality**
- ▶ **Integrity**
- ▶ **Availability**
- ▶ **Accountability**
- ▶ **Auditability**



HOW DO I ACHIEVE THIS  
IN A VIRTUAL WORLD?



# Welcome to the next Generation

- ▶ 1<sup>st</sup> Age: Servers
  - ▶ Servers
  - ▶ FTP, Telnet, Mail, Web.
  - ▶ These were the things that consumed bytes from a bad guy
  - ▶ The hack left a foot print
- ▶ 2<sup>nd</sup> Age: Browsers:
  - ▶ Javascript, ActiveX, Java, Image Formats, DOMs
  - ▶ These are the things that are getting locked down
    - ▶ Slowly
    - ▶ Incompletely
- ▶ 3<sup>rd</sup> 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

# — Virtual Word – With Virtual Back Doors

## Welcome to the Future

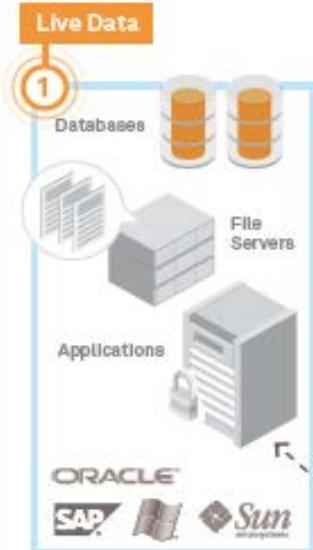
- Cloud Computing
- Virtual Environment
- With Virtual Security holes



During the past 15 years we “learnt” nothing

# Sensitive Data is Everywhere

WHERE IS YOUR DATA?



WHERE ARE YOUR KEYS?

Key Management and Root of Trust

**Warning**

- Pockets of Encryption
- Operational Inefficiencies
- Audit Deficiencies & Failures
- Sensitive Data Exposure

WHO AND WHAT IS ACCESSING YOUR DATA?



Internal Users +  
Administrators

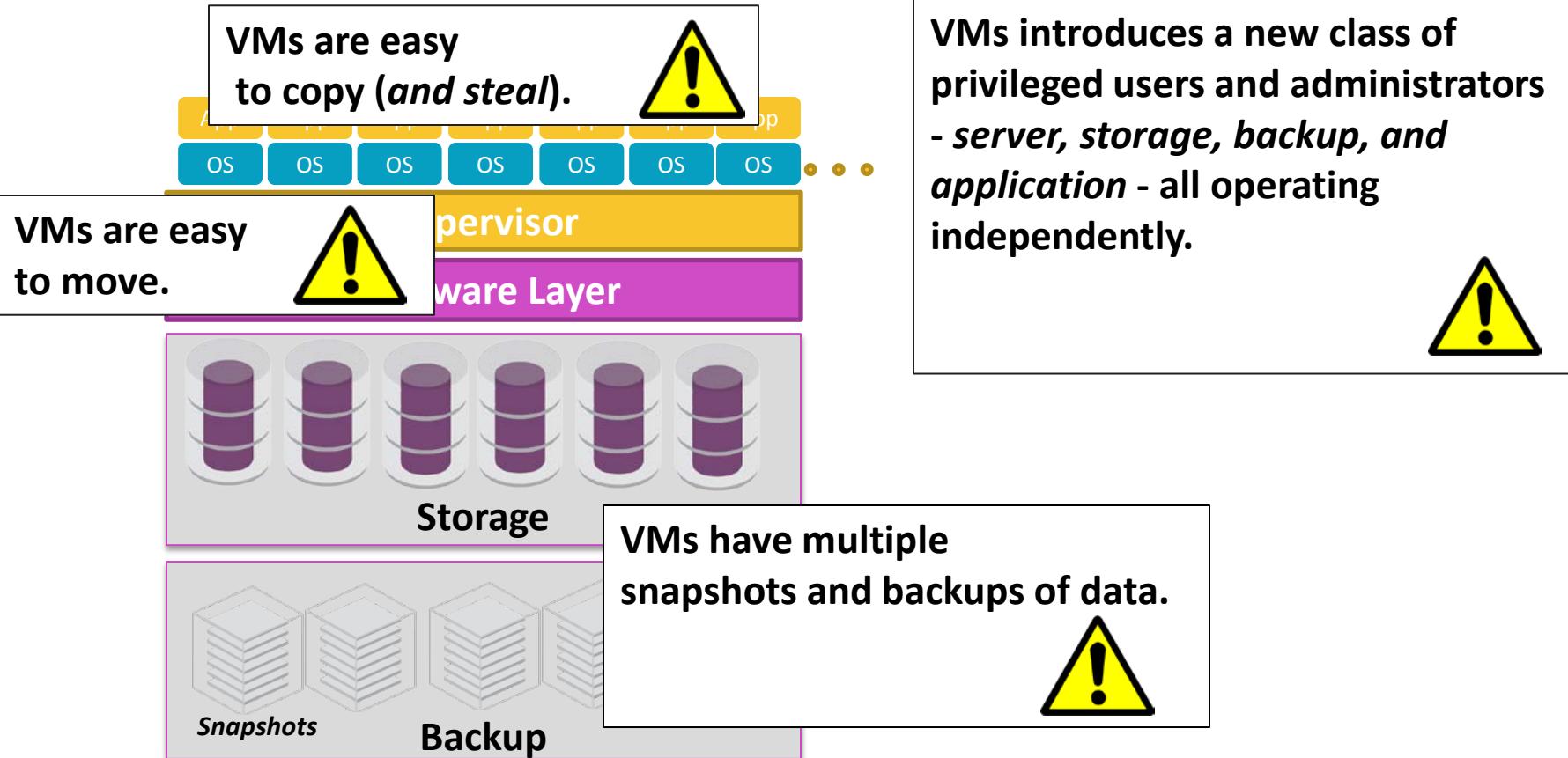


Cloud Providers  
Admins/Superusers



Customers +  
Partners

# — Security Gaps are Present



# — What do Auditors look for?

Type of Data?

- Classification

Who has access?

- Identity Management
- Key Management

How is data protected?

- Encryption
- Persistence
- Key Management
- Access SLA



Organizations  
have to prove  
ownership and  
control of their  
data

When was it accessed?

- Meta Data
- Encryption
- Key Management

Where is stored?

- Lifecycle
- Backups
- Snapshots

How was it disposed?

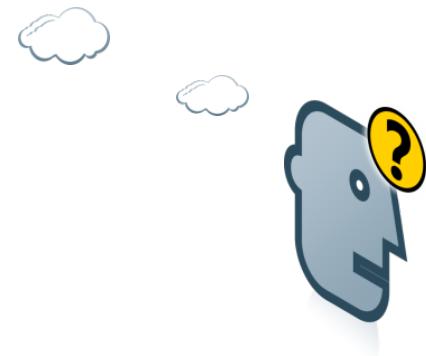
- Data shredding
- Key shredding

# — Back to Basics – PLEASE

- ▶ **Confidentiality**
- ▶ **Integrity**
- ▶ **Availability**
- ▶ **Accountability**
- ▶ **Auditability**

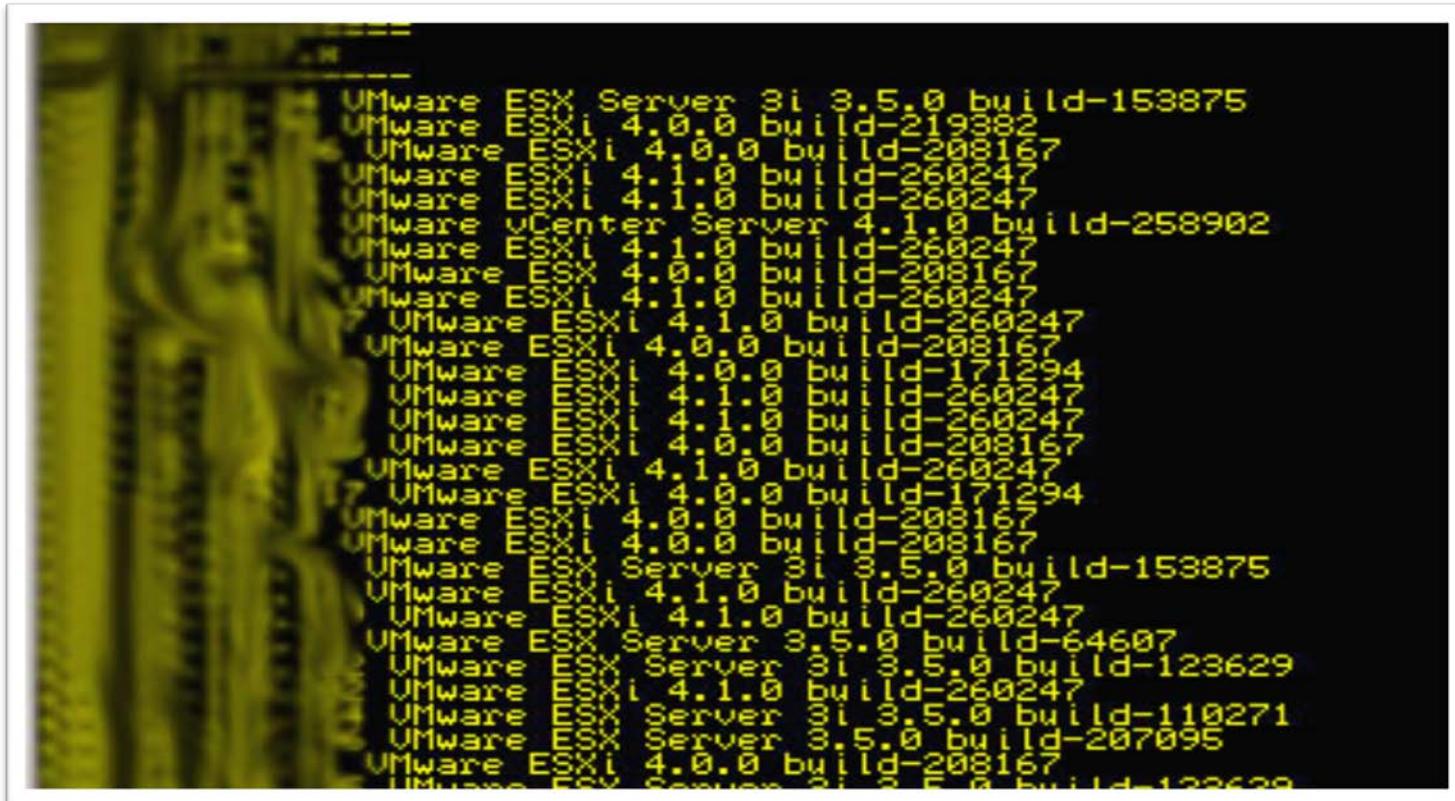


HOW DO I ACHIEVE THIS  
IN A VIRTUAL WORLD?



# Lets Start

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



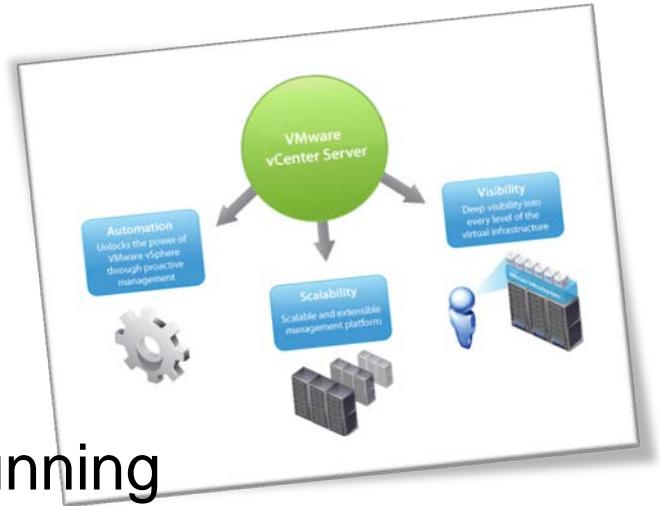
# **How do the hackers hack VMware vCenter in 60 seconds?**



# 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

# The Attack

vCenter Orchestrator attack vector 1.....

Installed by default within vCenter is an very interesting file:

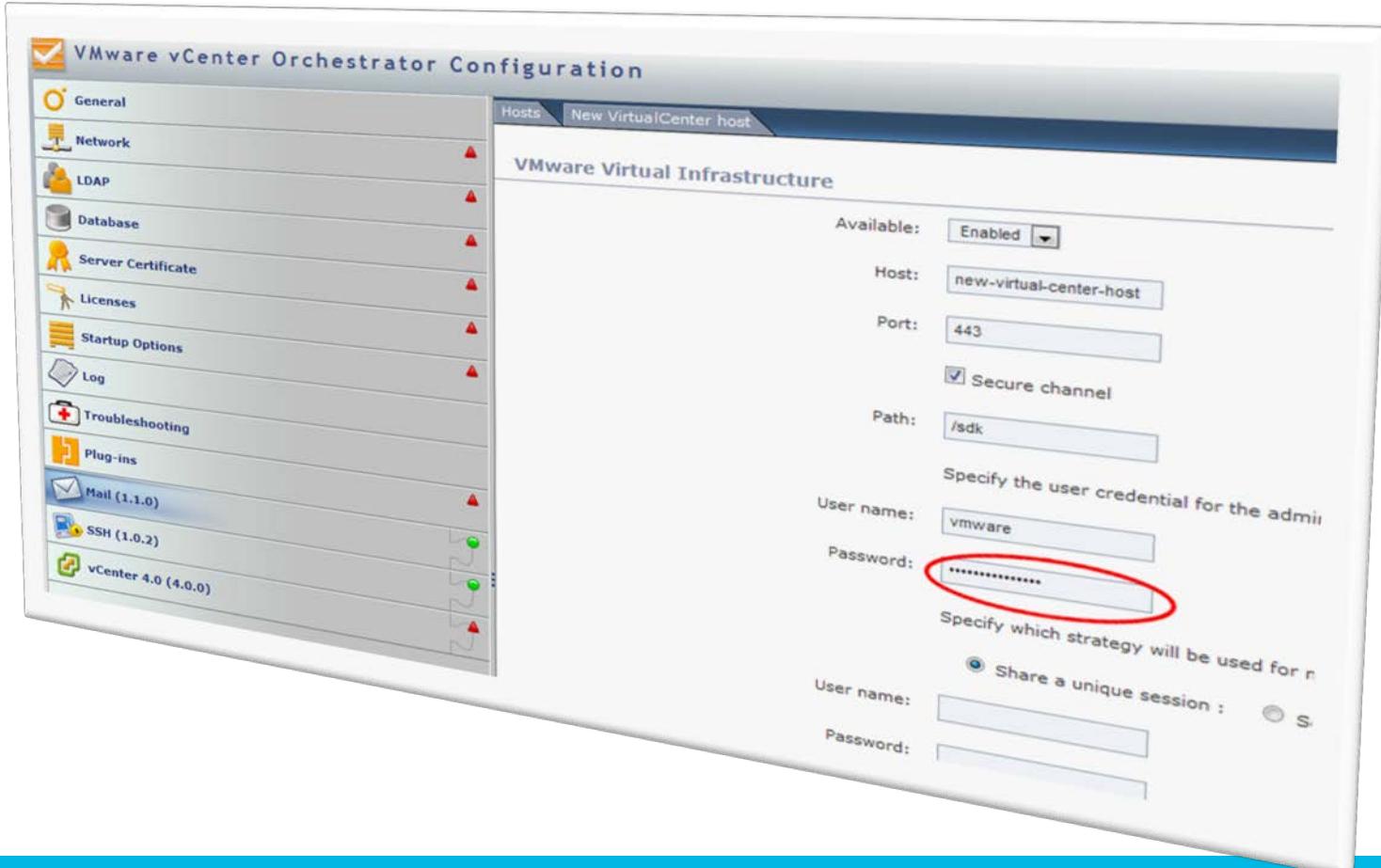
**C:\Programfiles\VMware\Infrastructure\Orchestrator\configuration\jetty\etc\passwd.properties**



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

# We are in

After bruteforcing the MD5.....



# Point & Click



Any one can do .....



A screenshot of the msfconsole interface. The top window shows the command '\$ msfconsole'. Below it, a larger window shows the following msfconsole session:

```
$ msfconsole

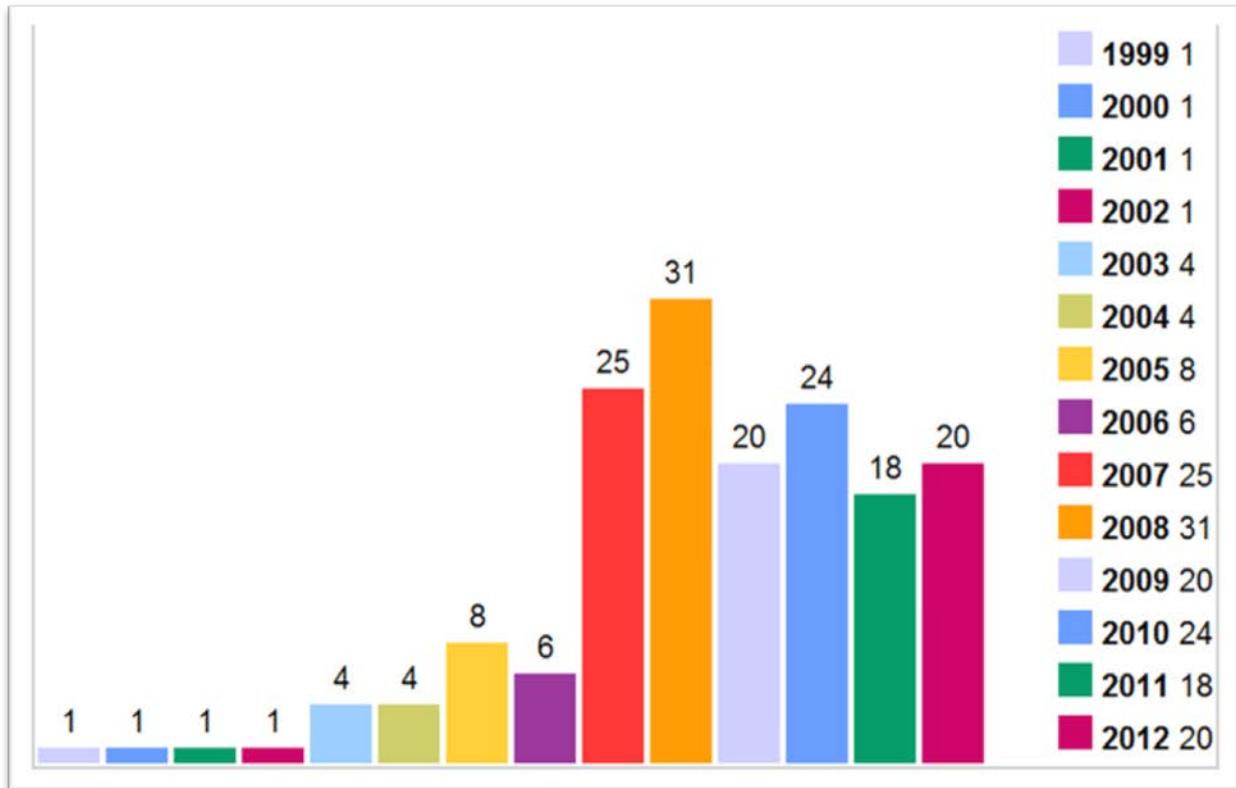
msf > use auxiliary/scanner/vmware/vmware_enum_sessions
msf auxiliary(vmware_enum_sessions) > set RHOSTS [TARGET HOST RANGE]
msf auxiliary(vmware_enum_sessions) > run
```

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

# —Look



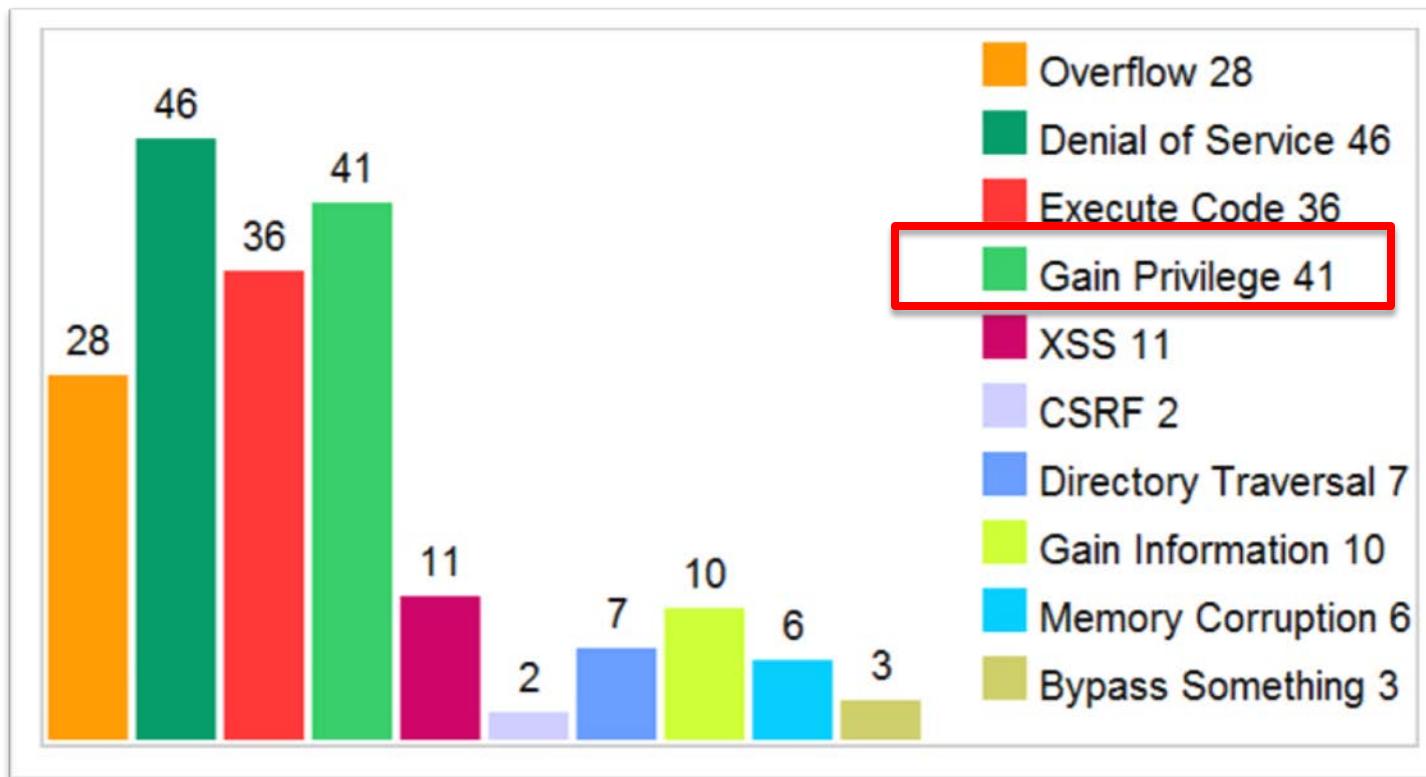
More and More Vulnerabilities..by Year....



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

# Total

Current Vulnerabilities todate by .... Type



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

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	CVSS Score
---	--------	--------	---------------	-----------------------	--------------	-------------	-------	---------------------	--------	------------	----------------	------------

20 [CVE-2009-1147](#)

+Priv

2009-04-06 2010-08-21

**7.2**

None

Local

Low

Not required

CVSS

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

CVSS

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 2.0.7; 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 flag, which allows local authenticated guest 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

CVSS

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 Datastore Manager role to gain privileges via unknown vectors.

23 [CVE-2008-4279](#) [264](#)

+Priv

2008-10-06 2009-09-08

**6.8**

Admin

Local

Low

Single system

CVSS

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.x before 2.0.5 build 109488; ACE 2.0.x before 2.0.7 build 108880; and ESX 2.5.4 through 3.5 allows authenticated guest OS users to gain additional guest OS privileges by triggering the 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

CVSS

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, VMware Workstation 6.5.x before 6.5.3 build 185404, 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 before 2.0.2 build 203138 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

CVSS

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-Type" header.

26 [CVE-2008-1363](#) [264](#)

+Priv

2008-03-19 2011-06-24

**7.2**

Admin

Local

Low

Not required

CVSS

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 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 to gain elevated privileges.

27 [CVE-2008-1362](#) [264](#)

DoS +Priv

2008-03-19 2008-09-05

**7.2**

Admin

Local

Low

Not required

CVSS

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 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 "insecure" feature, which is similar to the 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 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 mode is enabled, allows local users to gain privileges via an unspecified exploit.

# — Attacking the Virtual World



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:c3:22	172.16.42.114	uk816002	01:00:21:6a:9b:c3:22

# Live Attack

Against the Virtual World . . . ARP Attack



# — Virtual World

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





Google

Search 7 results (0.23 seconds)

Everything [PDF] .... W-9 https://dl.dropbox.com/s/.../CTMUN\_W9\_Request\_For\_TaxID.pdf?...  
File Format: PDF/Adobe Acrobat - Quick View  
Request for **Taxpayer** ... Fiequester's **name** and **address** (optional) ... The number shown on this form is my correct **taxpayer** identification number (or I am waiting ...)

Images [PDF] PG933-17 Page 1 of 16 05/2010 Mailing Address: PO Box 9394 ...  
https://dl.dropbox.com/.../Burke%20-...  
File Format: PDF/Adobe Acrobat  
Aug 24, 2011 – titled in the **name** of the deceased participant as well as your **name** – for ..... Mailing **Address** of Financial Institution (Street or PO Box). **Name** of ...

Maps

Videos

News

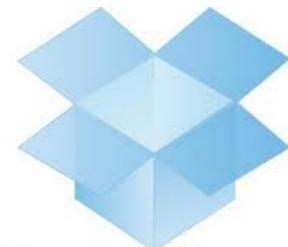
Shopping

More

Looking for sensitive data leaks in Dropbox cloud storage



site:dropbox.com/gallery



Dropbox

Google

site:dropbox.com/gallery

Search

About 164,000 results (0.33 seconds)

Web

[www.dropbox.com/gallery/](http://www.dropbox.com/gallery/)

Images

[Sommerblut 2011 - Dropbox - Photos - Simplify your life](https://www.dropbox.com/gallery/16453785/1/Sommerblut_2011_COPYRIGHT-HINWEISE)

[https://www.dropbox.com/gallery/16453785/1/Sommerblut\\_2011\\_COPYRIGHT-HINWEISE](https://www.dropbox.com/gallery/16453785/1/Sommerblut_2011_COPYRIGHT-HINWEISE) 1 image. Last modified 5/18/2011.

18 images. Last modified 5/23/2011. ALFONS\_Fotos\_wg 12 images

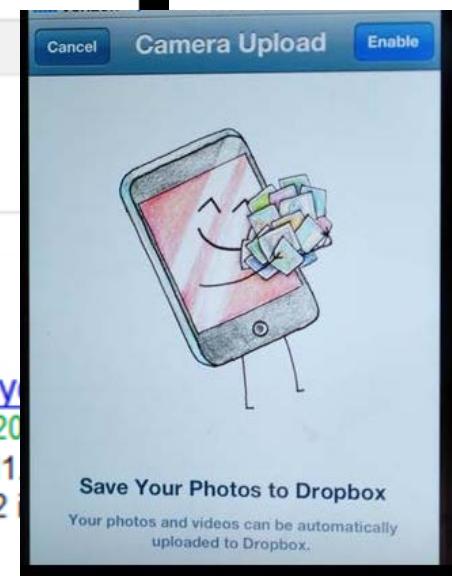
Maps

Videos

News

Shopping

More



[GracerHopper112011 - Dropbox - Photos - Simplify your life](https://www.dropbox.com/gallery/9183906/.../GracerHopper112011...)

<https://www.dropbox.com/gallery/9183906/.../GracerHopper112011...>

Dropbox is a free service that lets you bring your photos, docs, and videos together in one place and share them easily. Never email yourself a file again!



site:live.com "skydrive" ext:dmp



SkyDrive®

Google site:live.com "skydrive" ext:dmp

Search About 2,700 results (0.41 seconds)

Database dump files on Microsoft SkyDrive

Everywhere https://cid-8847e773b11eec31.skydrive.live.com/embedicon.aspx/.../060510-38688-01.dmp...

Images

Maps

Videos

News

Windows Live SkyDrive  
https://skydrive.live.com/embedicon.aspx/.../060510-38688-01.dmp  
Open 060510-38688-01.dmp 060510-38688-01.dmp.

Shopping

Windows Live SkyDrive  
https://skydrive.live.com/embedicon.aspx/122509-26520-01.dmp?cid...  
Open 122509-26520-01.dmp 122509-26520-01.dmp.

Web https://skydrive.live.com/embedicon.aspx/Minidump/...

Images https://skydrive.live.com/embedicon.aspx/Minidump/...

Maps https://skydrive.live.com/embedicon.aspx/Minidump/...

Videos https://skydrive.live.com/embedicon.aspx/Minidump/...

News https://skydrive.live.com/embedicon.aspx/Minidump/...

Shopping https://skydrive.live.com/embedicon.aspx/Minidump/...

More https://skydrive.live.com/embedicon.aspx/Minidump/...



Google

Search 4 results (0.13 seconds)

Everything [nepsi-sw22](#)  
<https://docs.google.com/View?docid=0AbKTT...1...1...>  
boot-end-marker ! enable secret 5 \$1\$BHsg\$izpAqHDUbLzEWCqfP/leT/. **enable**  
**password 7** 0455254C5F765C ! no aaa new-model. system mtu routing 1500 ...

Images [ncepsti-sw21-01-04-10](#)  
<https://docs.google.com/View?docid=0AbKTT...1...1...>  
enable secret 5 \$1\$P6du\$.NRbLzz5WiKER5mgw.t7r. **enable password 7**  
000A3D4C540C1B ! no aaa new-model. system mtu routing 1500. ip subnet-zero ...

Maps [ncepsti-rt06-01-04-10](#)  
<https://docs.google.com/View?docid=0AbKTT...1...1...>  
logging buffered 51200 warnings. enable secret 5 \$1\$..7N\$Ru28/DDfSHrAgq5bhUFzh  
**enable password 7** 151C2546547D25 ! no aaa new-model ! resource ...

Videos

News

Shopping

More

Tempe, AZ

Change location

Cisco config files  
with passwords in  
Google Docs files

# Data Loss In The News

Yale Alumni 43,000 SSNs Exposed in Excel Spreadsheet

The screenshot shows a news article from CNET News. The header features the CNET logo and the word "News". Below the header is a navigation bar with links for Home, Reviews, News, Download, CNET TV, and How To. The main title of the article is "Yale oversight exposes 43,000 Social Security numbers". A subtitle below the main title reads "Purdue University also reports exposure of more than 7,000 Social Security numbers after unknown person accesses server." The author of the article is Elinor Mills, and it was published on August 23, 2011, at 5:35 PM PDT. There is a link to follow the author on Twitter (@elinormills). A summary of the article states: "Names and Social Security numbers of 43,000 Yale University students, faculty, staff, and alumni were accessible via the Google search engine for about 10 months, according to the school newspaper." The background of the page has a torn paper effect.

# Cloud Security

N O P R O M I S E S.....

## **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



THE  
DATA  
PROTECTION  
COMPANY



# CodeSearch Diggity

## CLOUD SECRET KEYS

The screenshot shows the CodeSearch Diggity application interface. The menu bar includes File, Options, Help, GoogleDiggity, CodeSearchDiggity (which is selected), BingDiggity, LinkFromDomainDiggity, DLPDiggity, FlashDiggity, and MalwareDiggity. Below the menu is a toolbar with Advanced (selected) and Simple tabs, a SCAN button, and a Cancel button. On the left, a 'Query Appender' panel lists various security queries like SQL Injection, Cross-site Scripting (XS), and Hard-coded Passwords. A red box highlights a section of this panel. The main area is a table titled 'Scan Results' with columns: Category, Subcategory, Search String, Page Title, and URL. One row in the table is highlighted with a yellow background and has a red box around it. This row contains the search string 'ec2[^\\d]["]{20}["]', the page title 'Cloud Keys Stored in Plain Text', and the URL 'http://www.google.com/codesearch/p?hl=en#Kcy'. The URL column also shows truncated URLs. At the bottom, there are tabs for Output and Selected Result, with the Selected Result tab active. The output pane shows a snippet of Java code: 

```
Jec2 ec2 = new J<b>ec2("AK[REDACTED]ZEHQ"</b>, "[REDACTED]n+RCIkuoEeAD6");
```

 A red arrow points from the highlighted table row to the output pane, indicating that the sensitive data found in the scan results was copied or displayed here.

Category	Subcategory	Search String	Page Title	URL
Cloud Keys Stored in Plain Text		ec2[^\\d]["]{20}["]	Cloud Keys Stored in Plain Text	http://www.google.com/codesearch/p?hl=en#Kcy
		ec2[^\\d]["]{20}["]		http://www.google.com/codesearch/p?hl=en#Kcy
		ec2[^\\d]["]{20}["]	trunk/src/chron	http://w[REDACTED]n#CQI
		ec2[^\\d]["]{20}["]	trunk/src/chron	http://w[REDACTED]n#CQI
		ec2[^\\d]["]{20}["]	chrome/content	http://www.google.com/codesearch/p?hl=en#ulAI
		ec2[^\\d]["]{20}["]	chrome/content	http://www.google.com/codesearch/p?hl=en#ulAI
		ec2[^\\d]["]{20}["]	trunk/src/eifaw:	http://www.google.com/codesearch/p?hl=en#aM(
		ec2[^\\d]["]{20}["]	trunk/EC2Samp	http://www.google.com/codesearch/p?hl=en#nfD
		A-Z0-9){20}["]	lookups.py	http://www.google.com/codesearch/p?hl=en#474



## Hyperlink

The screenshot illustrates a search result for "password ext:xls site:.com". The search results page on the left shows various links, including one for a file named "spring [XLS]". The main focus is an Excel spreadsheet titled "Copy\_of\_user.xls" which contains a list of user credentials. A red box highlights the search query in the Google bar, and a red callout bubble points to the spreadsheet with the text: "Username and passwords for bank accounts, email, and everything else".

	A	B	C	D
1		Username	Password	Pin/Notes
2	MUD	st[REDACTED]@gmail.com	mud[REDACTED]	
3	Cox	mi[REDACTED]@cox.net	cox[REDACTED]	
4	OPPD	op[REDACTED]	opp[REDACTED]	
5	USAA	ms[REDACTED]	ms[REDACTED]	
6	FAFSA		12q[REDACTED]	6[REDACTED]
7	Metro	mg[REDACTED]	UIC[REDACTED]	
8	US Bank	usb[REDACTED]	usb[REDACTED]	990[REDACTED]
9	Black Hills gas	blac[REDACTED]	blac[REDACTED]	
10	phone	mich[REDACTED]	sprin[REDACTED]	
11				
12				





The Battle  
For the Virtual  
World Has  
Begun

# Thank You

**Jason Hart CISSP CISM  
VP Cloud Solutions**

**[Jason.Hart@Safenet-inc.com](mailto:Jason.Hart@Safenet-inc.com)**



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