#RSAC

RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

NOW MATTERS

SESSION ID: **TECH-R02**

CYBERSECURITY TIPS, TOOLS AND TECHNIQUES FOR ALL SECURITY PROFESSIONALS

Ron Woerner

IT Risk and Compliance Consultant
DirectDefense
@ronw123

DIRECTDEFENSE

Poll the Audience

- Session ID: TECH-R02

- Do you have a USB drive on you?
    - Yes
    - No

https://rsa1-live.eventbase.com/polls?event=rsa2018&polls=3821

Poll the Audience

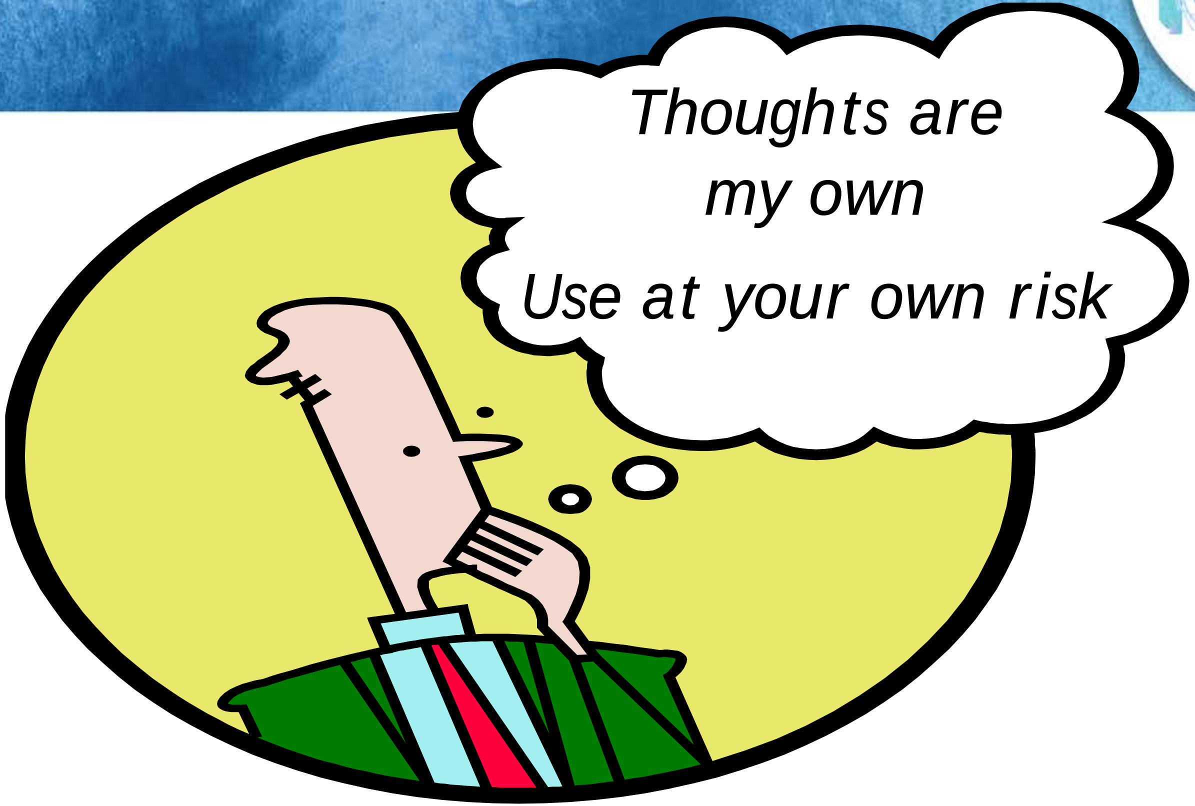
- Session ID: TECH-R02

- When were you last asked to fix someone's computer?
  - < 1 week
  - < 1 month
  - < 3 months

https://rsa1-live.eventbase.com/polls?event=rsa2018&polls=3822

Ron Woerner - BIO

- CyberSecurity Consultant / Trusted Advisor for DirectDefense
- Adjunct Professor, Bellevue University
- 25+ years experience in IT / Security
- CISSP, CISM, CEH, BS-A
- Blogger & writer
- Given tons'o presentations on security and Internet safety


Thoughts are my own
Use at your own risk

Content as of February 2018

If you only remember 1 slide…

STOP | THINK | CONNECT™

https://www.stopthinkconnect.org/

LOCK DOWN YOUR LOGIN

https://www.lockdownyourlogin.com/

if you SEE something | SAY something™

https://www.dhs.gov/see-something-say-something

What the $%$# are we doing here?

How to be really dangerous…

Cool technologies

Tools, applications, websites, references, other stuff that can help you do you job.

Cybersecurity tips to keep yourself, others, and hopefully your company out of trouble.

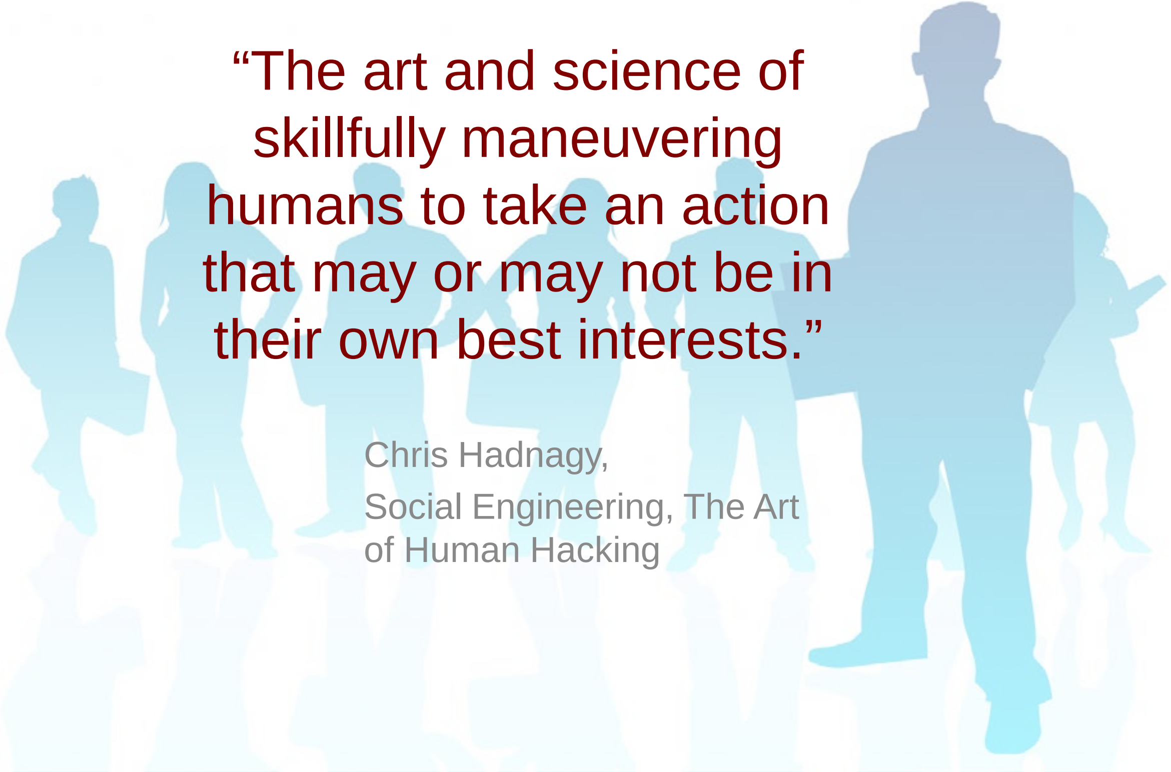
Security

Tools

Tips

Techniques

The Easiest Hack

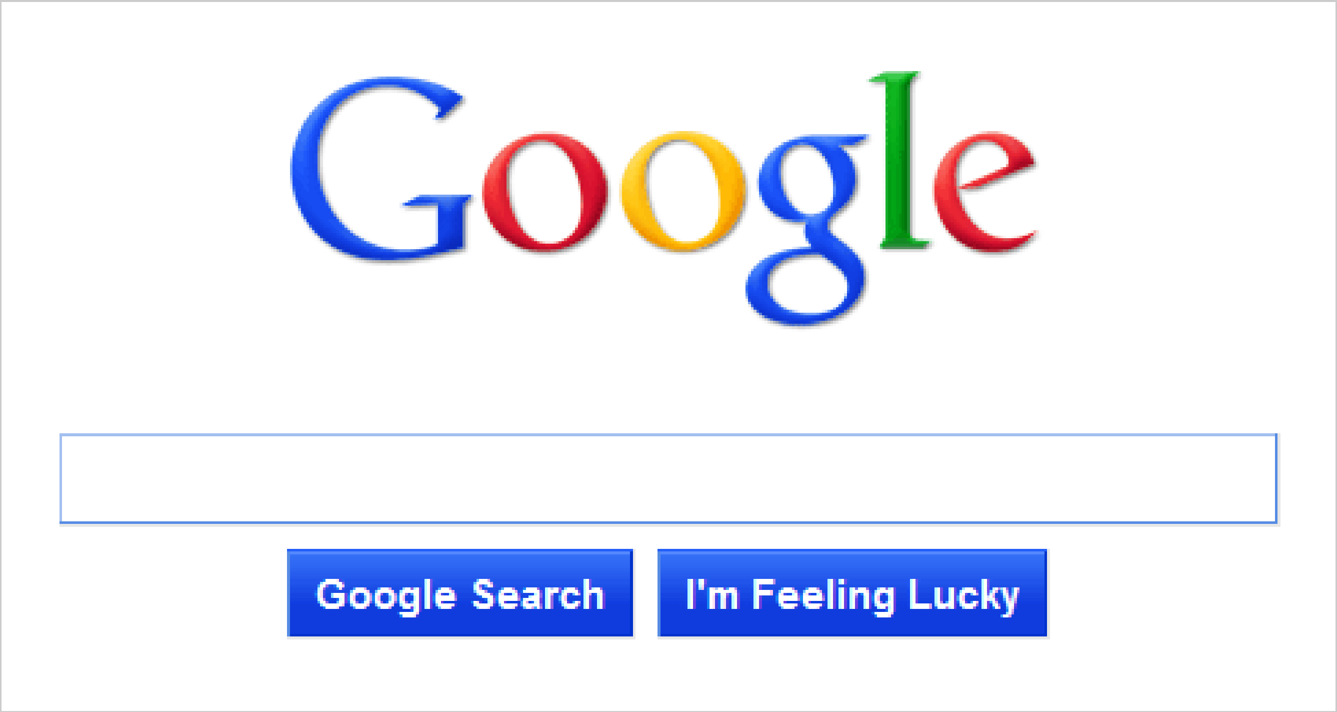


> “The art and science of skillfully maneuvering humans to take an action that may or may not be in their own best interests.”

Chris Hadnagy,

Social Engineering, The Art of Human Hacking

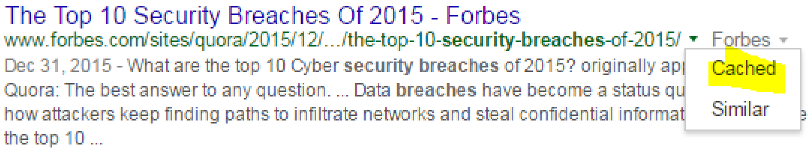
Google Hacking



http://www.google.com/intl/en/help/features_list.html

Time Travel

- Google Cache



The Top 10 Security Breaches Of 2015 - Forbes
www.forbes.com/sites/quora/2015/12/.../the-top-10-**security-breaches**-of-2015/ ▾ Forbes ▾
Dec 31, 2015 - What are the top 10 Cyber **security breaches** of 2015? originally app
Quora: The best answer to any question. ... Data **breaches** have become a status qu
how attackers keep finding paths to infiltrate networks and steal confidential informat e
the top 10 ...

- Archive.org – Wayback Machine

Lists of tools, tips, & tricks

- OlderGeeks
- SecTools
- HowToGeek.com, Geek School
- The Geek Stuff (mostly Linux)

Security Awareness

- DHS Stop-Think-Connect

STOP | THINK | CONNECT™

- NCSA Stay Safe Online

StaySafeOnline.org
Powered by National Cyber Security Alliance

- Director of National Intelligence: https://www.dni.gov/index.php/resources/protecting-personal-information

Virtual Environments

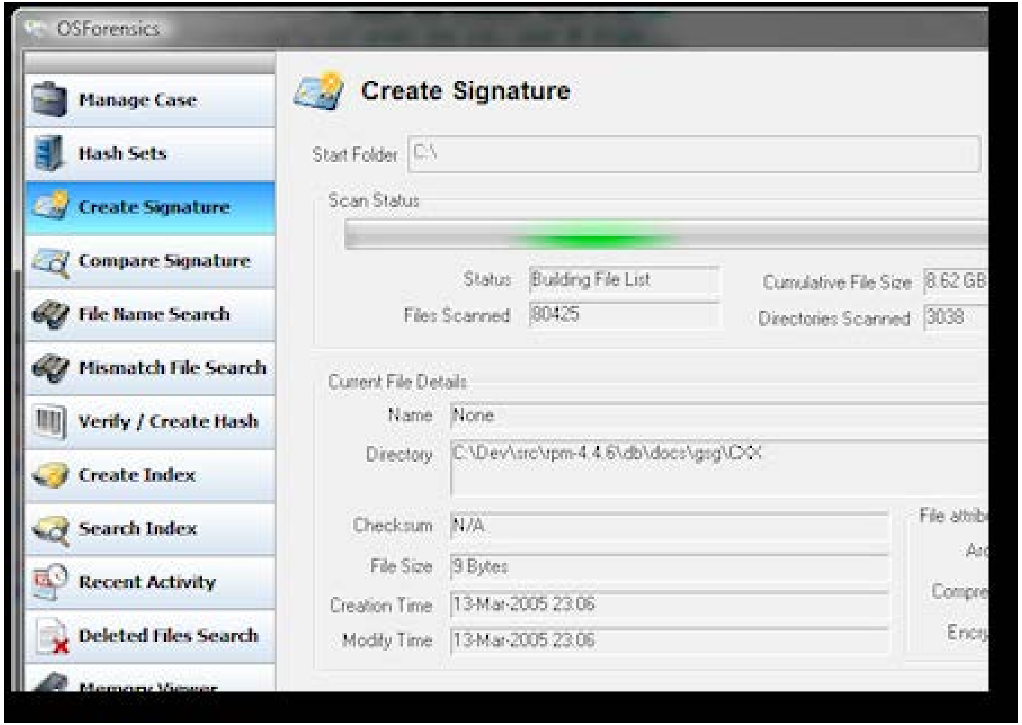
- VMWare Player / Workstation
- Oracle VM VirtualBox

Cookie & Ad Blockers

- Firefox NoScript
- Ghostery
- Editthiscookie
- EFF Privacy Badger
- Sandboxie
- EFF – Privacy Badger

Forensics

- OSForensics
  - Licensed – free for home use
- WinHex



Create Signature

Start Folder: C:\

Scan Status

Status: Building File List

Files Scanned: 80425

Cumulative File Size: 8.62 GB

Directories Scanned: 3038

Current File Details

Name: None

Directory: C:\Dev\src\rpm-4.4.6\db\docs\gsg\CXX

Checksum: N/A

File Size: 9 Bytes

Creation Time: 13-Mar-2005 23:06

Modify Time: 13-Mar-2005 23:06

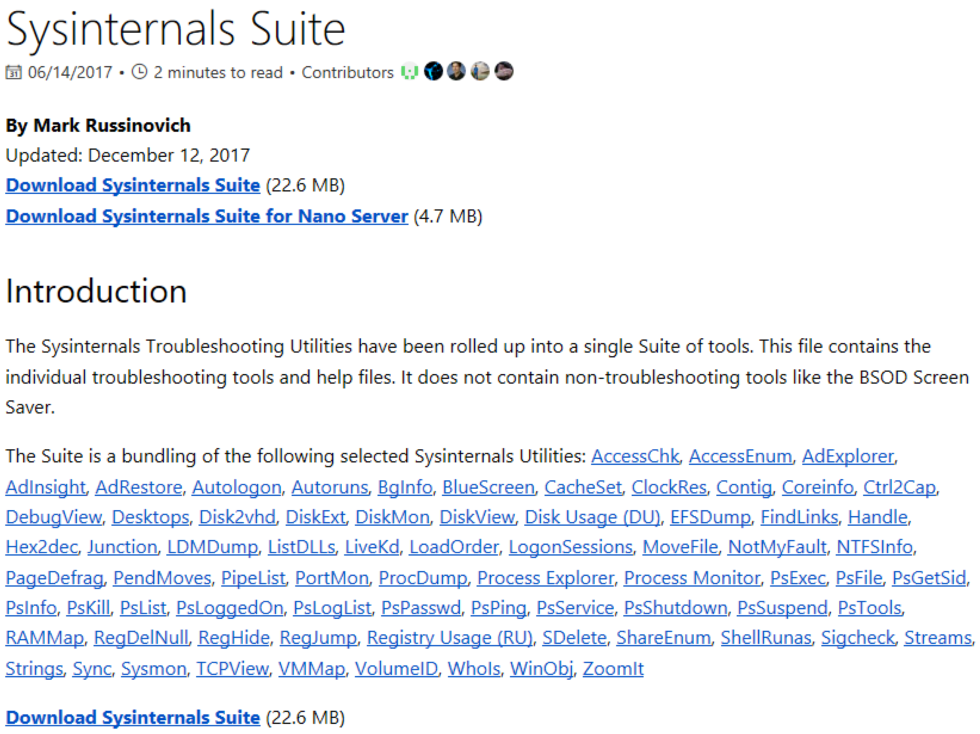
Windows Administration

SysInternals Suite

- Autoruns
- Process Explorer
- Process Monitor

Video:

Mark Russinovich, Malware Hunting



Sysinternals Suite

06/14/2017 • 2 minutes to read • Contributors

By Mark Russinovich

Updated: December 12, 2017

Download Sysinternals Suite (22.6 MB)

Download Sysinternals Suite for Nano Server (4.7 MB)

Introduction

The Sysinternals Troubleshooting Utilities have been rolled up into a single Suite of tools. This file contains the individual troubleshooting tools and help files. It does not contain non-troubleshooting tools like the BSOD Screen Saver.

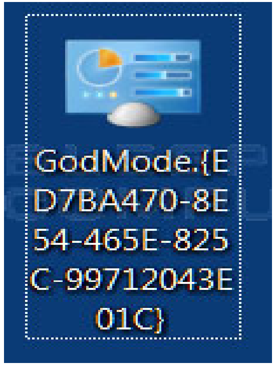
The Suite is a bundling of the following selected Sysinternals Utilities: AccessChk, AccessEnum, AdExplorer, AdInsight, AdRestore, Autologon, Autoruns, BgInfo, BlueScreen, CacheSet, ClockRes, Contig, Coreinfo, Ctrl2Cap, DebugView, Desktops, Disk2vhd, DiskExt, DiskMon, DiskView, Disk Usage (DU), EFSDump, FindLinks, Handle, Hex2dec, Junction, LDMDump, ListDLLs, LiveKd, LoadOrder, LogonSessions, MoveFile, NotMyFault, NTFSInfo, PageDefrag, PendMoves, PipeList, PortMon, ProcDump, Process Explorer, Process Monitor, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsList, PsLoggedOn, PsLogList, PsPasswd, PsPing, PsService, PsShutdown, PsSuspend, PsTools, RAMMap, RegDelNull, RegHide, RegJump, Registry Usage (RU), SDelete, ShareEnum, ShellRunas, Sigcheck, Streams, Strings, Sync, Sysmon, TCPView, VMMap, VolumeID, WhoIs, WinObj, ZoomIt

Download Sysinternals Suite (22.6 MB)

Windows Administration

GodMode

- Create a new folder and edit it so that it is named the following and then press enter.
  - GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}
- When done, you should have an icon on your desktop

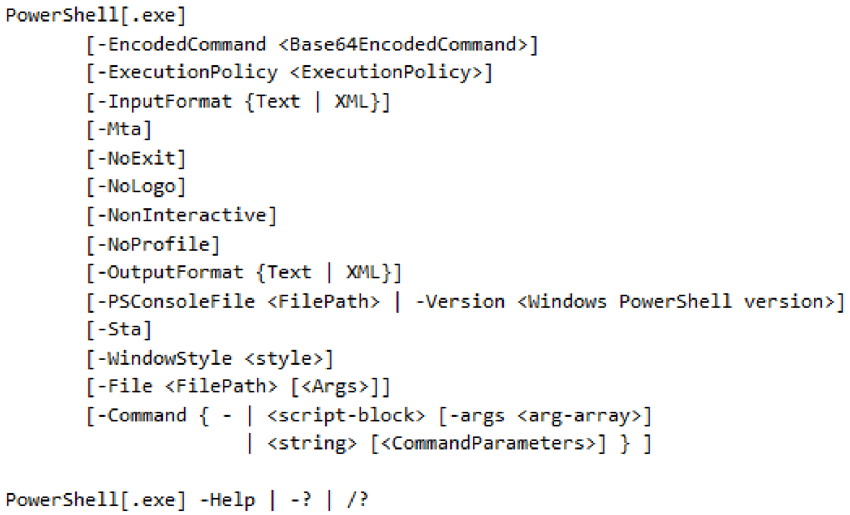


GodMode.{E
D7BA470-8E
54-465E-825
C-99712043E
01C}

Windows Administration

PowerShell

- Using Windows PowerShell
- PowerShell.exe Command-Line Help



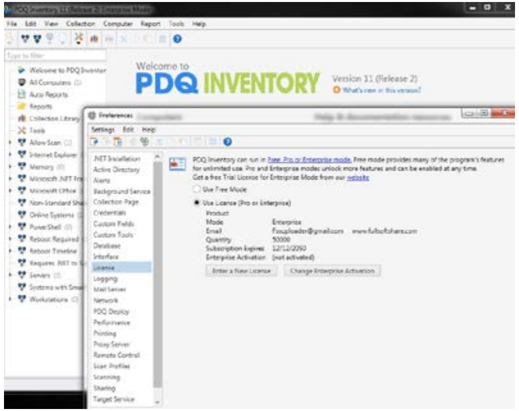
```
PowerShell[.exe]
       [-EncodedCommand <Base64EncodedCommand>]
       [-ExecutionPolicy <ExecutionPolicy>]
       [-InputFormat {Text | XML}]
       [-Mta]
       [-NoExit]
       [-NoLogo]
       [-NonInteractive]
       [-NoProfile]
       [-OutputFormat {Text | XML}]
       [-PSConsoleFile <FilePath> | -Version <Windows PowerShell version>]
       [-Sta]
       [-WindowStyle <style>]
       [-File <FilePath> [<Args>]]
       [-Command { - | <script-block> [-args <arg-array>]
                     | <string> [<CommandParameters>] } ]

PowerShell[.exe] -Help | -? | /?
```

System Inventory & Automation

PDQ Inventory & Deploy

https://www.pdq.com/



PDQ Inventory can run in Free, Pro or Enterprise mode. Free mode provides many of the program's features for unlimited use. Pro and Enterprise modes unlock more features and can be enabled at any time. Get a free Trial License for Enterprise Mode from our website

○ Use Free Mode

● Use License (Pro or Enterprise)

Product	
Mode	Enterprise
Email	Fxxuploader@gmail.com www.fullofshare.com
Quantity	50000
Subscription Expires	12/12/2050
Enterprise Activation	(not activated)

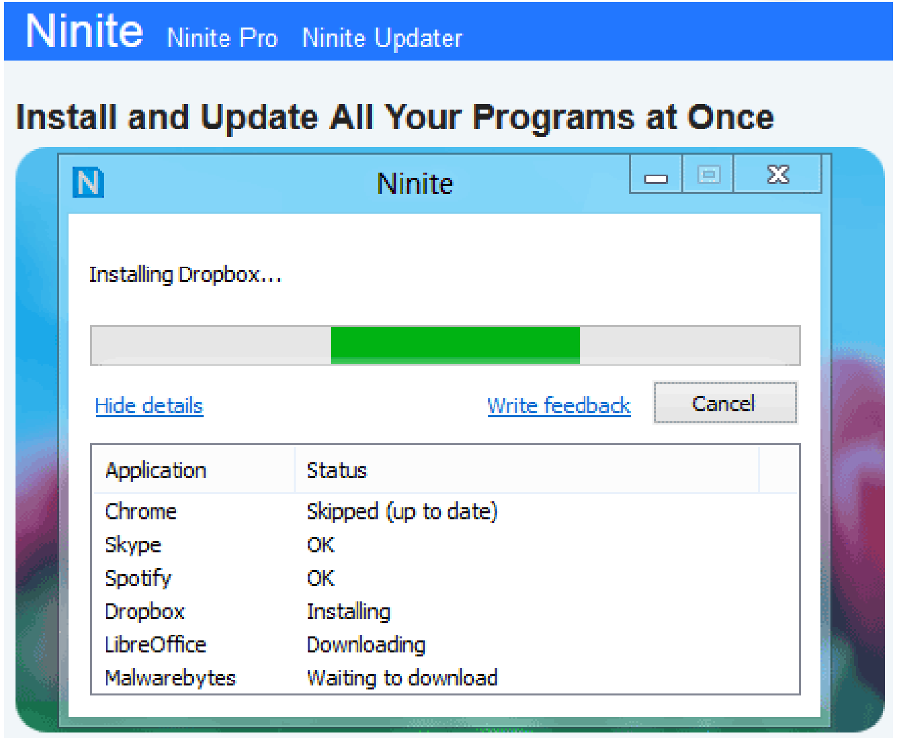
Ansible

https://www.ansible.com/

ANSIBLE

Patching & Updating

Ninite (https://ninite.com/)



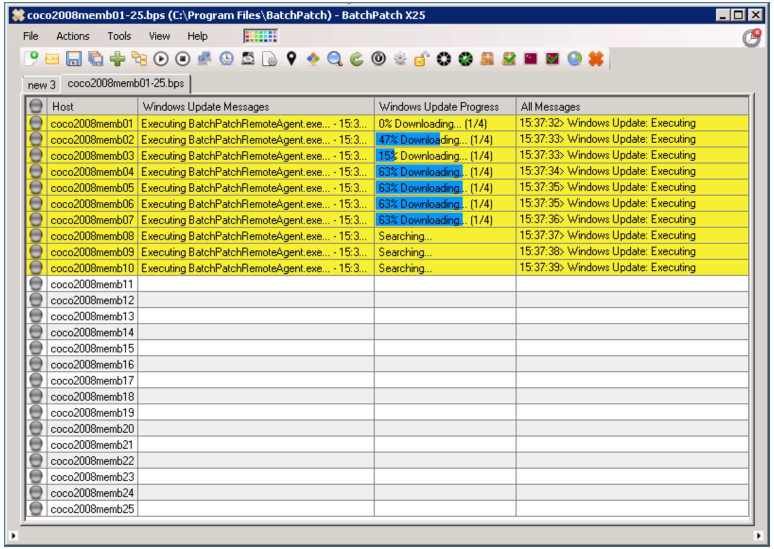
Install and Update All Your Programs at Once

Installing Dropbox...

Application	Status
Chrome	Skipped (up to date)
Skype	OK
Spotify	OK
Dropbox	Installing
LibreOffice	Downloading
Malwarebytes	Waiting to download

Patching & Updating

BatchPatch
(https://batchpatch.com/)



coco2008memb01-25.bps (C:\Program Files\BatchPatch) - BatchPatch X25

Host	Windows Update Messages	Windows Update Progress	All Messages
coco2008memb01	Executing BatchPatchRemoteAgent.exe... - 15:3...	0% Downloading... (1/4)	15:37:32> Windows Update: Executing
coco2008memb02	Executing BatchPatchRemoteAgent.exe... - 15:3...	47% Downloading... (1/4)	15:37:33> Windows Update: Executing
coco2008memb03	Executing BatchPatchRemoteAgent.exe... - 15:3...	15% Downloading... (1/4)	15:37:33> Windows Update: Executing
coco2008memb04	Executing BatchPatchRemoteAgent.exe... - 15:3...	63% Downloading... (1/4)	15:37:34> Windows Update: Executing
coco2008memb05	Executing BatchPatchRemoteAgent.exe... - 15:3...	63% Downloading... (1/4)	15:37:35> Windows Update: Executing
coco2008memb06	Executing BatchPatchRemoteAgent.exe... - 15:3...	63% Downloading... (1/4)	15:37:35> Windows Update: Executing
coco2008memb07	Executing BatchPatchRemoteAgent.exe... - 15:3...	63% Downloading... (1/4)	15:37:36> Windows Update: Executing
coco2008memb08	Executing BatchPatchRemoteAgent.exe... - 15:3...	Searching...	15:37:37> Windows Update: Executing
coco2008memb09	Executing BatchPatchRemoteAgent.exe... - 15:3...	Searching...	15:37:38> Windows Update: Executing
coco2008memb10	Executing BatchPatchRemoteAgent.exe... - 15:3...	Searching...	15:37:39> Windows Update: Executing
coco2008memb11			
coco2008memb12			
coco2008memb13			
coco2008memb14			
coco2008memb15			
coco2008memb16			
coco2008memb17			
coco2008memb18			
coco2008memb19			
coco2008memb20			
coco2008memb21			
coco2008memb22			
coco2008memb23			
coco2008memb24			
coco2008memb25			

Chocolatey

(https://chocolatey.org/)

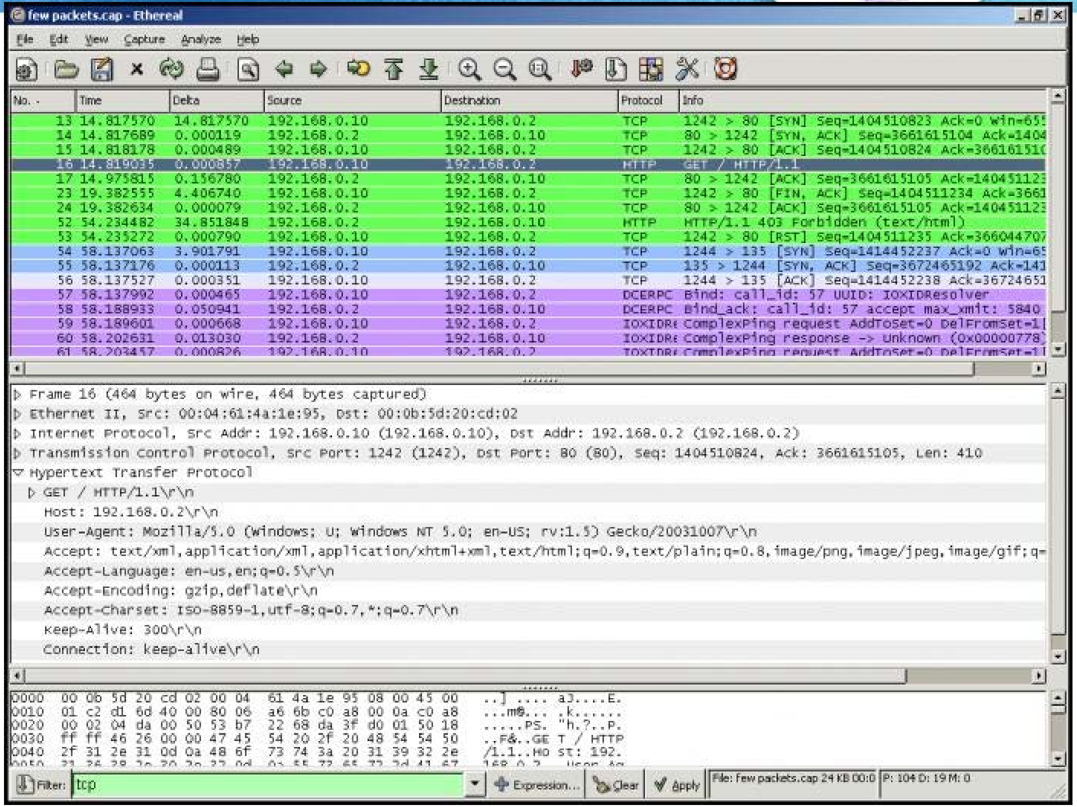
Chocolatey
Software Management Automated

Network Evaluation

WIRESHARK

Introduction video

- TcpDump


few packets.cap - Ethereal
File Edit View Capture Analyze Help

```
No. .  Time       Delta      Source         Destination    Protocol Info
    13 14.817570  14.817570  192.168.0.10   192.168.0.2    TCP      1242 > 80 [SYN] Seq=1404510823 Ack=0 Win=65
    14 14.817689  0.000119   192.168.0.2    192.168.0.10   TCP      80 > 1242 [SYN, ACK] Seq=3661615104 Ack=1404
    15 14.818178  0.000489   192.168.0.10   192.168.0.2    TCP      1242 > 80 [ACK] Seq=1404510824 Ack=36616151(
    16 14.819035  0.000857   192.168.0.10   192.168.0.2    HTTP     GET / HTTP/1.1
    17 14.975815  0.156780   192.168.0.2    192.168.0.10   TCP      80 > 1242 [ACK] Seq=3661615105 Ack=14045112:
    23 19.382555  4.406740   192.168.0.10   192.168.0.2    TCP      1242 > 80 [FIN, ACK] Seq=1404511234 Ack=3661
    24 19.382634  0.000079   192.168.0.2    192.168.0.10   TCP      80 > 1242 [ACK] Seq=3661615105 Ack=14045112:
    52 54.234482  34.851848  192.168.0.2    192.168.0.10   HTTP     HTTP/1.1 403 Forbidden (text/html)
    53 54.235272  0.000790   192.168.0.10   192.168.0.2    TCP      1242 > 80 [RST] Seq=1404511235 Ack=366044707
    54 58.137063  3.901791   192.168.0.10   192.168.0.2    TCP      1244 > 135 [SYN] Seq=1414452237 Ack=0 Win=65
    55 58.137176  0.000113   192.168.0.2    192.168.0.10   TCP      135 > 1244 [SYN, ACK] Seq=3672465192 Ack=141
    56 58.137527  0.000351   192.168.0.10   192.168.0.2    TCP      1244 > 135 [ACK] Seq=1414452238 Ack=36724651
    57 58.137992  0.000465   192.168.0.10   192.168.0.2    DCERPC   Bind: call_id: 57 UUID: IOXIDResolver
    58 58.188933  0.050941   192.168.0.2    192.168.0.10   DCERPC   Bind_ack: call_id: 57 accept max_xmit: 5840
    59 58.189601  0.000668   192.168.0.10   192.168.0.2    IOXIDRε  ComplexPing request AddToSet=0 DelFromSet=1[
    60 58.202631  0.013030   192.168.0.2    192.168.0.10   IOXIDRε  ComplexPing response -> Unknown (0x00000778)
    61 58.203457  0.000826   192.168.0.10   192.168.0.2    IOXIDRε  ComplexPing request AddToSet=0 DelFromSet=1[
```

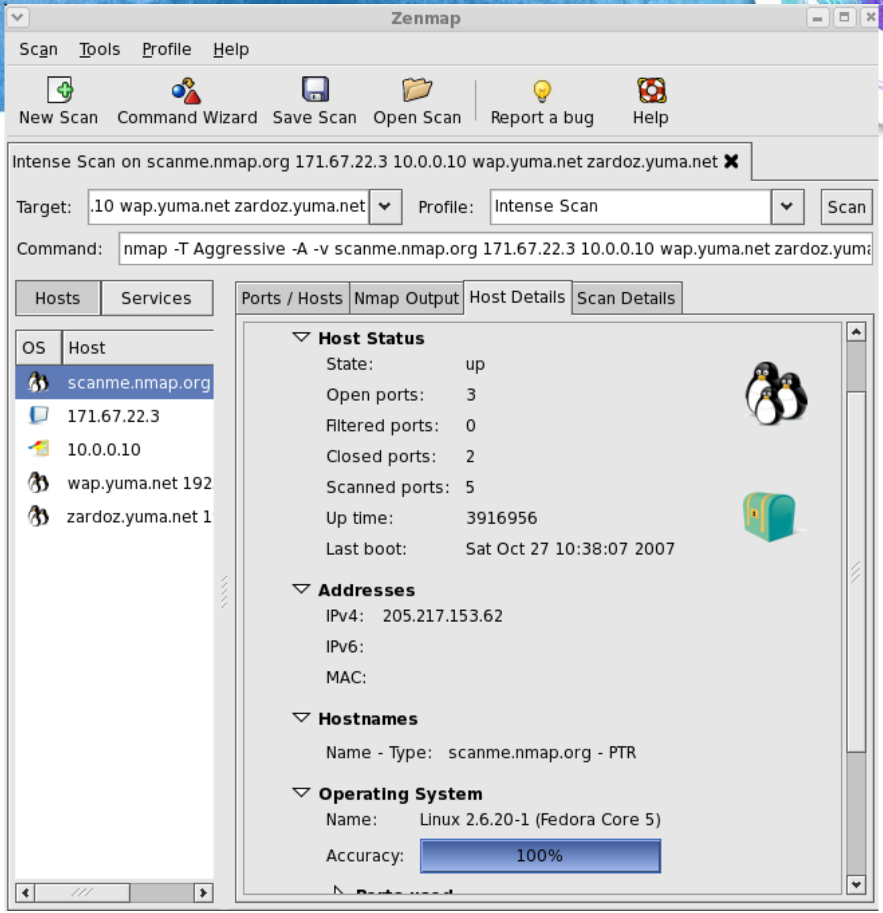
```
▷ Frame 16 (464 bytes on wire, 464 bytes captured)
▷ Ethernet II, Src: 00:04:61:4a:1e:95, Dst: 00:0b:5d:20:cd:02
▷ Internet Protocol, Src Addr: 192.168.0.10 (192.168.0.10), Dst Addr: 192.168.0.2 (192.168.0.2)
▷ Transmission Control Protocol, Src Port: 1242 (1242), Dst Port: 80 (80), Seq: 1404510824, Ack: 3661615105, Len: 410
▽ Hypertext Transfer Protocol
  ▷ GET / HTTP/1.1\r\n
    Host: 192.168.0.2\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.5) Gecko/20031007\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
```

```
0000  00 06 5d 20 cd 02 00 04  61 4a 1e 95 08 00 45 00   ..] .... aJ....E.
0010  01 c2 d1 6d 40 00 80 06  a6 6b c0 a8 00 0a c0 a8   ...m@... .k......
0020  00 02 04 da 00 50 53 b7  22 68 da 3f d0 01 50 18   .....PS. "h.?..P.
0030  ff ff 46 26 00 00 47 45  54 20 2f 20 48 54 54 50   ..F&..GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 31 39 32 2e   /1.1..Ho st: 192.
```

Filter: tcp

Network Evaluation

[Nmap / ZenMap]



Intense Scan on scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net

Target: .10 wap.yuma.net zardoz.yuma.net

Profile: Intense Scan

Command: nmap -T Aggressive -A -v scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma

scanme.nmap.org
171.67.22.3
10.0.0.10
wap.yuma.net 192
zardoz.yuma.net 1

Host Status

State: up
Open ports: 3
Filtered ports: 0
Closed ports: 2
Scanned ports: 5
Up time: 3916956
Last boot: Sat Oct 27 10:38:07 2007

Addresses

IPv4: 205.217.153.62
IPv6:
MAC:

Hostnames

Name - Type: scanme.nmap.org - PTR

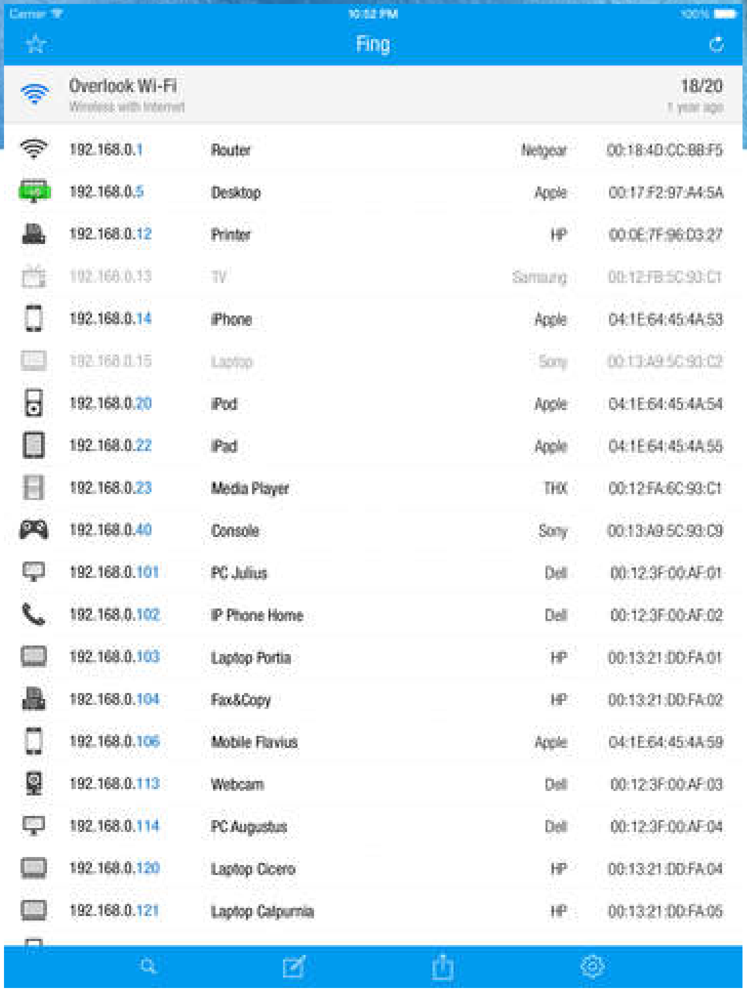
Operating System

Name: Linux 2.6.20-1 (Fedora Core 5)
Accuracy: 100%

Network Evaluation

Fing

(iOS & Android)



Carrier 10:52 PM 100%

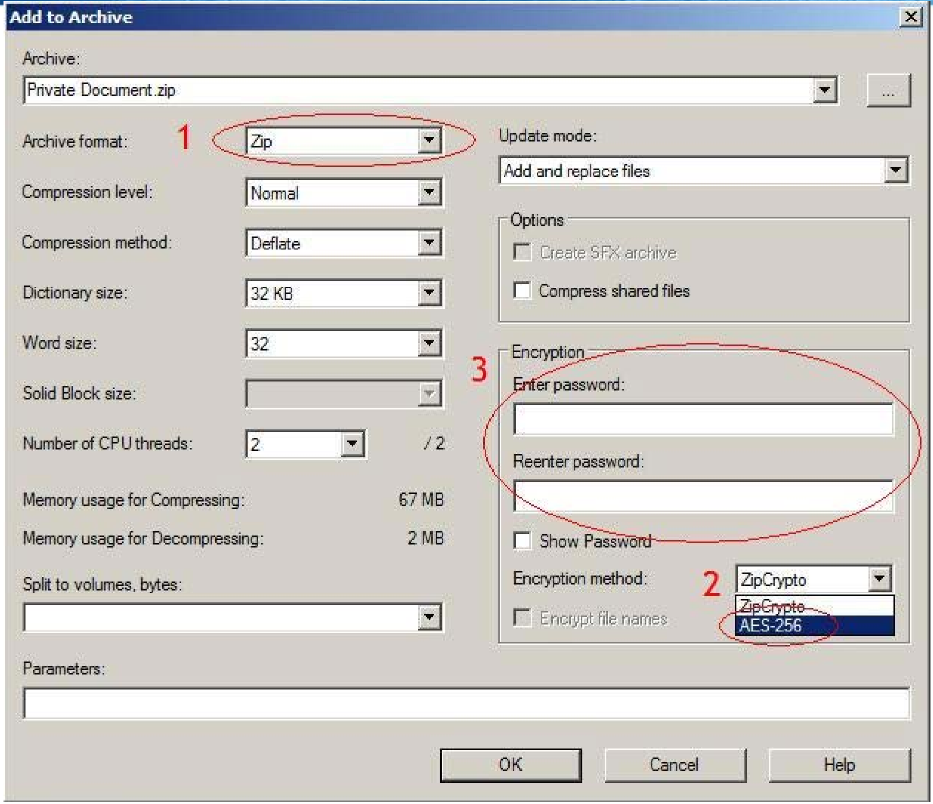
Fing

Overlook Wi-Fi 18/20
Wireless with Internet 1 year ago

192.168.0.1	Router	Netgear	00:18:4D:CC:B8:F5
192.168.0.5	Desktop	Apple	00:17:F2:97:A4:5A
192.168.0.12	Printer	HP	00:0E:7F:96:D3:27
192.168.0.13	TV	Samsung	00:12:FB:5C:93:C1
192.168.0.14	iPhone	Apple	04:1E:64:45:4A:53
192.168.0.15	Laptop	Sony	00:13:A9:5C:93:C2
192.168.0.20	iPod	Apple	04:1E:64:45:4A:54
192.168.0.22	iPad	Apple	04:1E:64:45:4A:55
192.168.0.23	Media Player	THX	00:12:FA:6C:93:C1
192.168.0.40	Console	Sony	00:13:A9:5C:93:C9
192.168.0.101	PC Julius	Dell	00:12:3F:00:AF:01
192.168.0.102	IP Phone Home	Dell	00:12:3F:00:AF:02
192.168.0.103	Laptop Portia	HP	00:13:21:DD:FA:01
192.168.0.104	Fax&Copy	HP	00:13:21:DD:FA:02
192.168.0.106	Mobile Flavius	Apple	04:1E:64:45:4A:59
192.168.0.113	Webcam	Dell	00:12:3F:00:AF:03
192.168.0.114	PC Augustus	Dell	00:12:3F:00:AF:04
192.168.0.120	Laptop Cicero	HP	00:13:21:DD:FA:04
192.168.0.121	Laptop Calpurnia	HP	00:13:21:DD:FA:05

Encryption

- 7-Zip
- AES Crypt
- Office 365



Add to Archive

Archive: Private Document.zip

Archive format: Zip

Compression level: Normal

Compression method: Deflate

Dictionary size: 32 KB

Word size: 32

Solid Block size:

Number of CPU threads: 2 / 2

Memory usage for Compressing: 67 MB

Memory usage for Decompressing: 2 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Options

□ Create SFX archive

□ Compress shared files

Encryption

Enter password:

Reenter password:

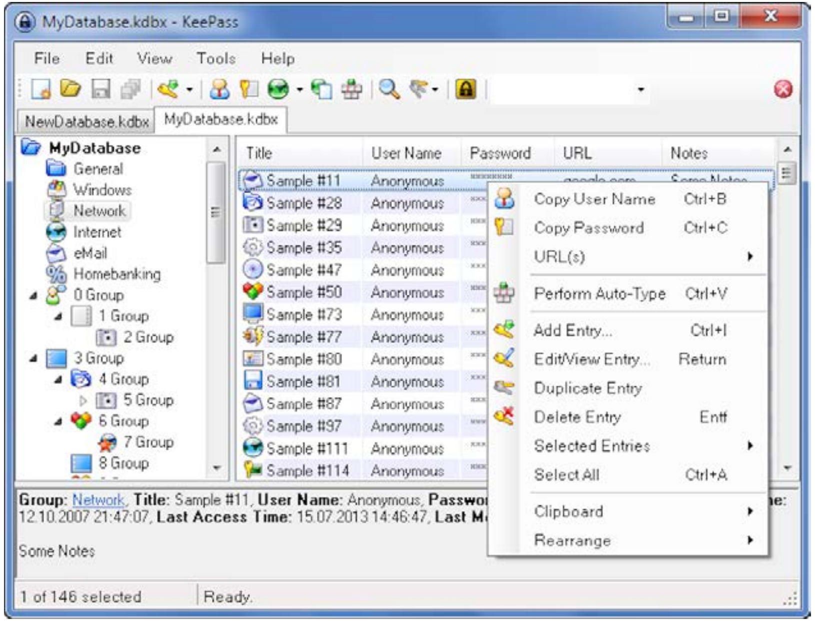
□ Show Password

Encryption method: ZipCrypto

□ Encrypt file names

Password Vaults

- LastPass
- KeePass
- LogMeOnce
- 1Password
- RoboForm
- Dashlane



Title	User Name	Password	URL	Notes
Sample #11	Anonymous	********	google.com	Some Notes
Sample #28	Anonymous	***		
Sample #29	Anonymous	***		
Sample #35	Anonymous	***		
Sample #47	Anonymous	***		
Sample #50	Anonymous	***		
Sample #73	Anonymous	***		
Sample #77	Anonymous	***		
Sample #80	Anonymous	***		
Sample #81	Anonymous	***		
Sample #87	Anonymous	***		
Sample #97	Anonymous	***		
Sample #111	Anonymous	***		
Sample #114	Anonymous	***		

Group: Network, **Title:** Sample #11, **User Name:** Anonymous, **Passwo** **e:**
12.10.2007 21:47:07, **Last Access Time:** 15.07.2013 14:46:47, **Last M**

Some Notes

1 of 146 selected | Ready.

Anonymous Browsing

https://tails.boum.org/

Proxy Resources

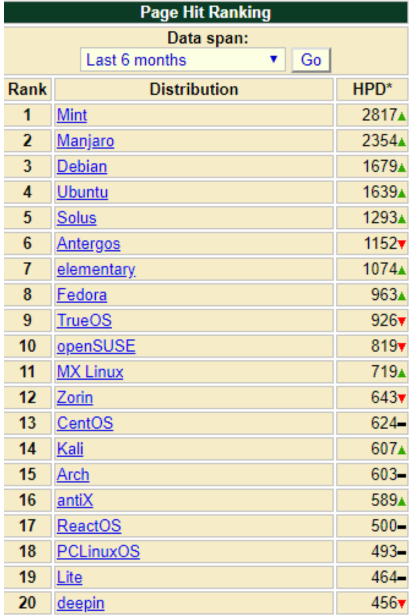
- Anonymouse: This service allows you to surf the web without revealing any personal information.
- 250 Working Proxies: the biggest list I've ever seen of anonymous proxies.

Security Testing

- OWASP Zed Attack Proxy (ZAP)
- Portswigger Burp Suite
- GuardiCore Infection Monkey
- Metasploit

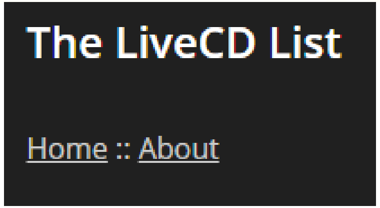
Linux

https://distrowatch.com/

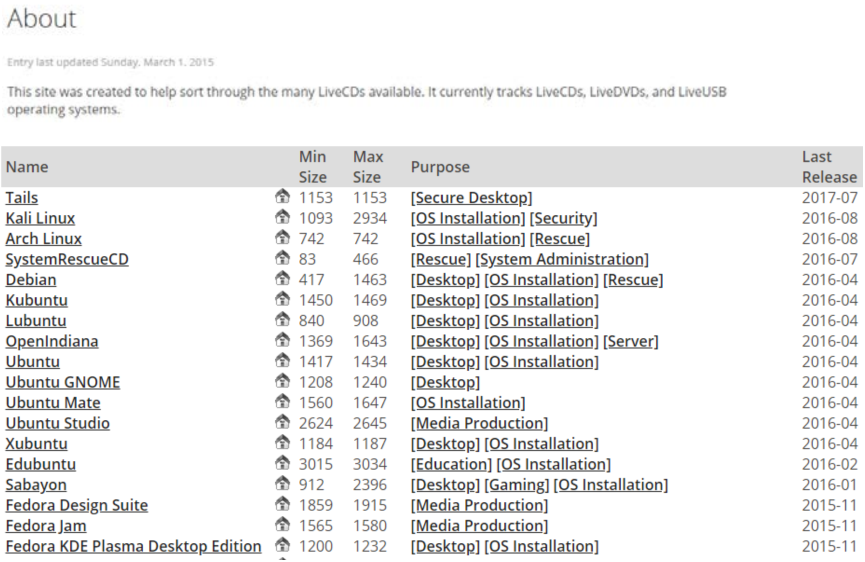


Rank	Distribution	HPD*
1	Mint	2817▲
2	Manjaro	2354▲
3	Debian	1679▲
4	Ubuntu	1639▲
5	Solus	1293▲
6	Antergos	1152▼
7	elementary	1074▲
8	Fedora	963▲
9	TrueOS	926▼
10	openSUSE	819▼
11	MX Linux	719▲
12	Zorin	643▼
13	CentOS	624–
14	Kali	607▲
15	Arch	603–
16	antiX	589▲
17	ReactOS	500–
18	PCLinuxOS	493–
19	Lite	464–
20	deepin	456▼

The Geek Stuff



https://livecdlist.com/



About

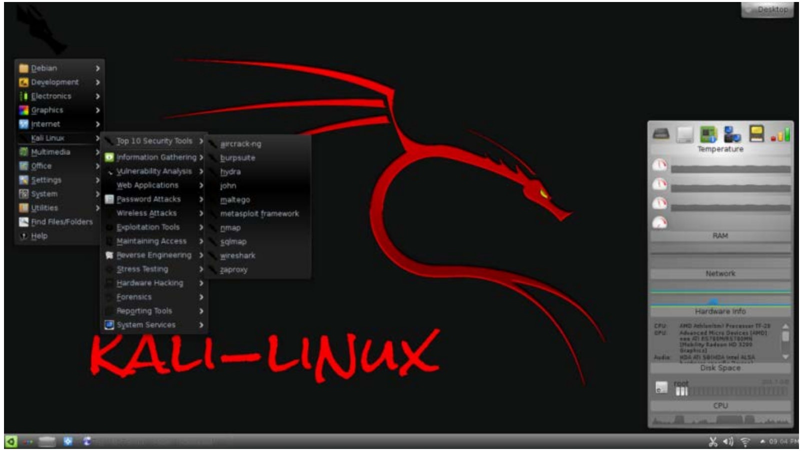
Entry last updated Sunday, March 1, 2015

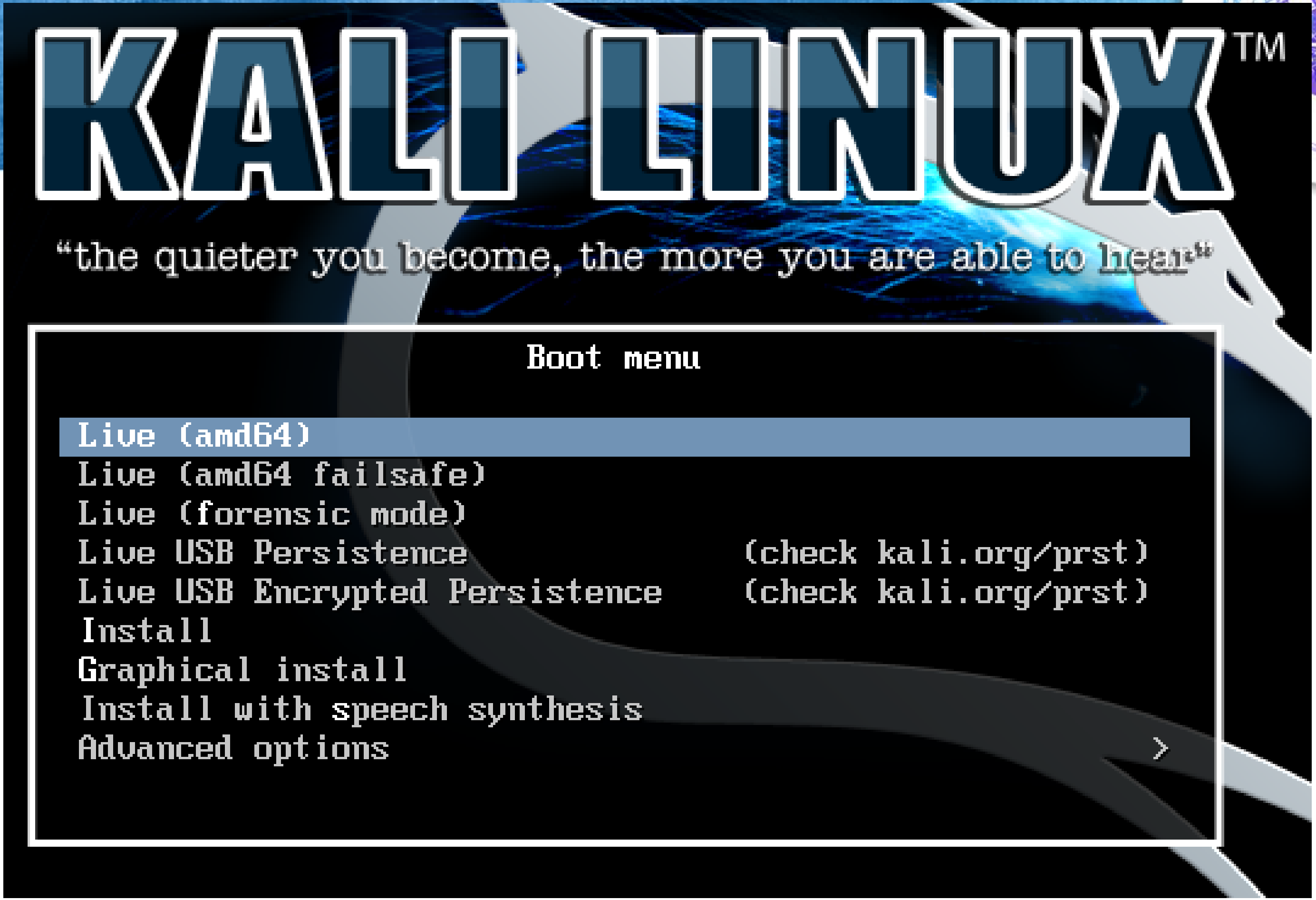
This site was created to help sort through the many LiveCDs available. It currently tracks LiveCDs, LiveDVDs, and LiveUSB operating systems.

Name		Min Size	Max Size	Purpose	Last Release
Tails	⌂	1153	1153	[Secure Desktop]	2017-07
Kali Linux	⌂	1093	2934	[OS Installation] [Security]	2016-08
Arch Linux	⌂	742	742	[OS Installation] [Rescue]	2016-08
SystemRescueCD	⌂	83	466	[Rescue] [System Administration]	2016-07
Debian	⌂	417	1463	[Desktop] [OS Installation] [Rescue]	2016-04
Kubuntu	⌂	1450	1469	[Desktop] [OS Installation]	2016-04
Lubuntu	⌂	840	908	[Desktop] [OS Installation]	2016-04
OpenIndiana	⌂	1369	1643	[Desktop] [OS Installation] [Server]	2016-04
Ubuntu	⌂	1417	1434	[Desktop] [OS Installation]	2016-04
Ubuntu GNOME	⌂	1208	1240	[Desktop]	2016-04
Ubuntu Mate	⌂	1560	1647	[OS Installation]	2016-04
Ubuntu Studio	⌂	2624	2645	[Media Production]	2016-04
Xubuntu	⌂	1184	1187	[Desktop] [OS Installation]	2016-04
Edubuntu	⌂	3015	3034	[Education] [OS Installation]	2016-02
Sabayon	⌂	912	2396	[Desktop] [Gaming] [OS Installation]	2016-01
Fedora Design Suite	⌂	1859	1915	[Media Production]	2015-11
Fedora Jam	⌂	1565	1580	[Media Production]	2015-11
Fedora KDE Plasma Desktop Edition	⌂	1200	1232	[Desktop] [OS Installation]	2015-11

Kali Linux

- Kali Linux is a Debian-derived Linux distribution, designed for digital forensics and penetration testing.
- Kali Linux is preinstalled with numerous penetration-testing programs.
- Kali Linux can be run from a hard disk, live CD, or live USB. It is a supported platform of the Metasploit Project's Metasploit Framework, a tool for developing and executing security exploits.

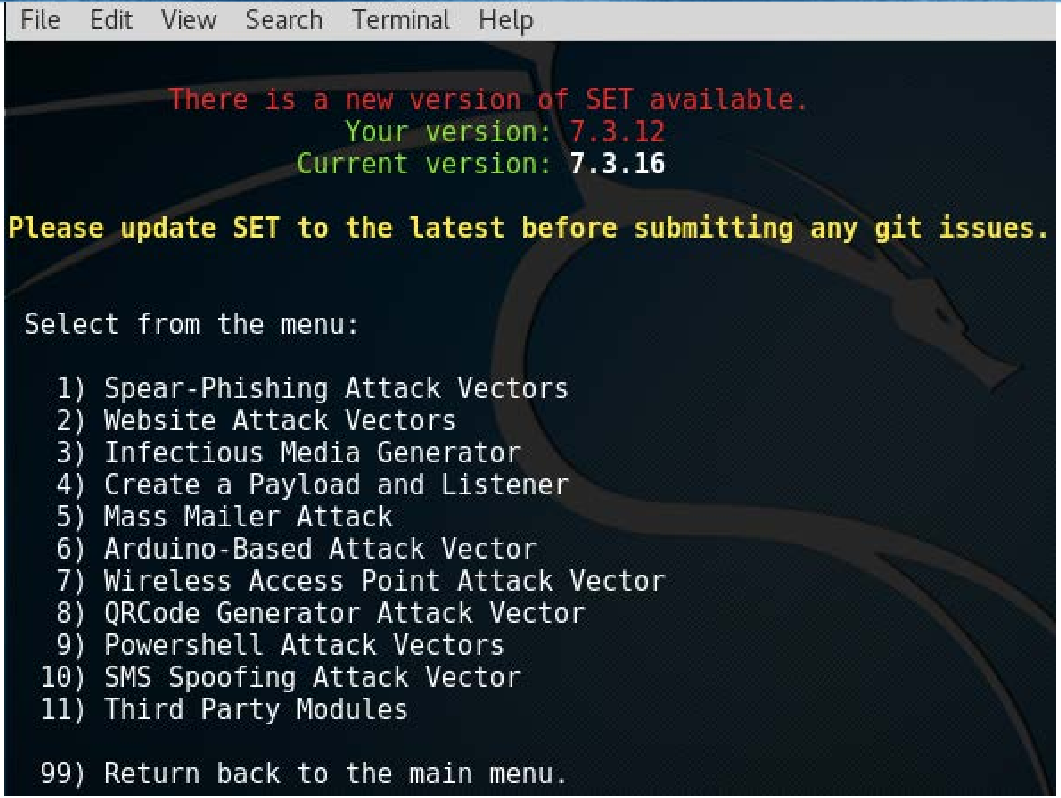




```
Boot menu

Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Live USB Persistence                 (check kali.org/prst)
Live USB Encrypted Persistence       (check kali.org/prst)
Install
Graphical install
Install with speech synthesis
Advanced options                                          >
```

Social Engineering Toolkit (SET)



```
            There is a new version of SET available.
                        Your version: 7.3.12
                     Current version: 7.3.16

Please update SET to the latest before submitting any git issues.


 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) SMS Spoofing Attack Vector
  11) Third Party Modules

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

Cheat Sheets

- Lenny Zeltser – IT and Information Security Cheat Sheets: https://zeltser.com/cheat-sheets/
- Malware Archeology (Auditing): https://www.malwarearchaeology.com/cheat-sheets/

Finding People

- Google
- LinkedIn
- Cree.py – Geolocation Information Aggregator, http://www.geocreepy.com/
- Peek You - www.peekyou.com

More Lists

- Sectools.org
- Tools Watch– Top Security Tools
- SANS Twenty Critical Security Controls
- Lifehacker
- HowToGeek
- Eric Ligman Collection of FREE Microsoft eBooks
  - 2014, 2015, 2016, 2017

Checklists

- NIST
  - CSRC: http://csrc.nist.gov/
  - Publications: http://csrc.nist.gov/publications/PubsSPs.html
  - Baldrige Cybersecurity Excellence Builder
- U.S. Cyber Consequences Unit (US-CCU) Cyber Security Matrix

What else?

“Apply” Slide

Immediate

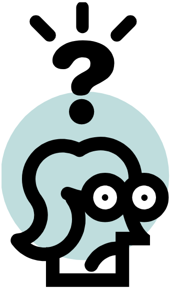
- Pick 1 or 2 tools
- Play / Try it out / Experiment

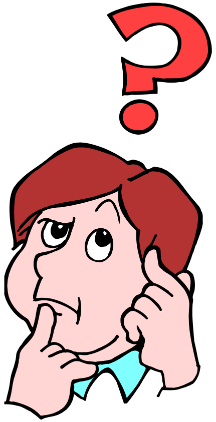
Next 3 mos.

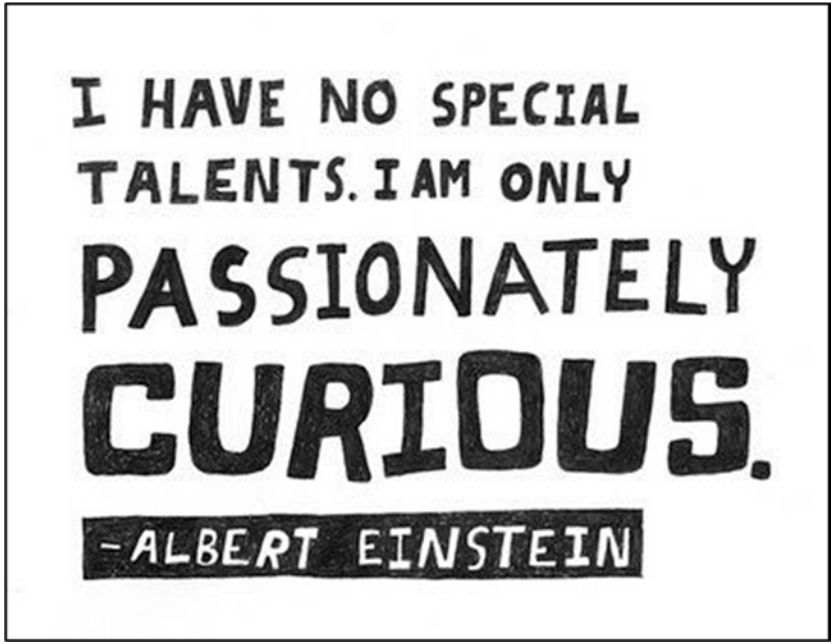
- Review this slide deck
- Pick more tools (3-5)
- Experiment with tools in a virtual environment
- Review the awareness websites

Share!

Questions???







I HAVE NO SPECIAL TALENTS. I AM ONLY PASSIONATELY CURIOUS.

-ALBERT EINSTEIN

HOMEWORK

Get out and play

Ron Woerner, CISSP, CISM

rwoerner @ directdefense.com

Twitter: @ronw123

By working together and helping each other, we all become stronger