

RSA® Conference 2019

San Francisco | March 4–8 | Moscone Center

The logo consists of the word "BETTER." in a bold, sans-serif font. The letters are white with a subtle gray texture. The background behind the text is a dense, colorful network of thin lines and small dots, primarily in shades of blue, yellow, and orange, resembling a neural network or a complex data visualization.

SESSION ID: TECH-R02

Cybersecurity Tips, Tools, and Techniques for Your Professional Toolbag

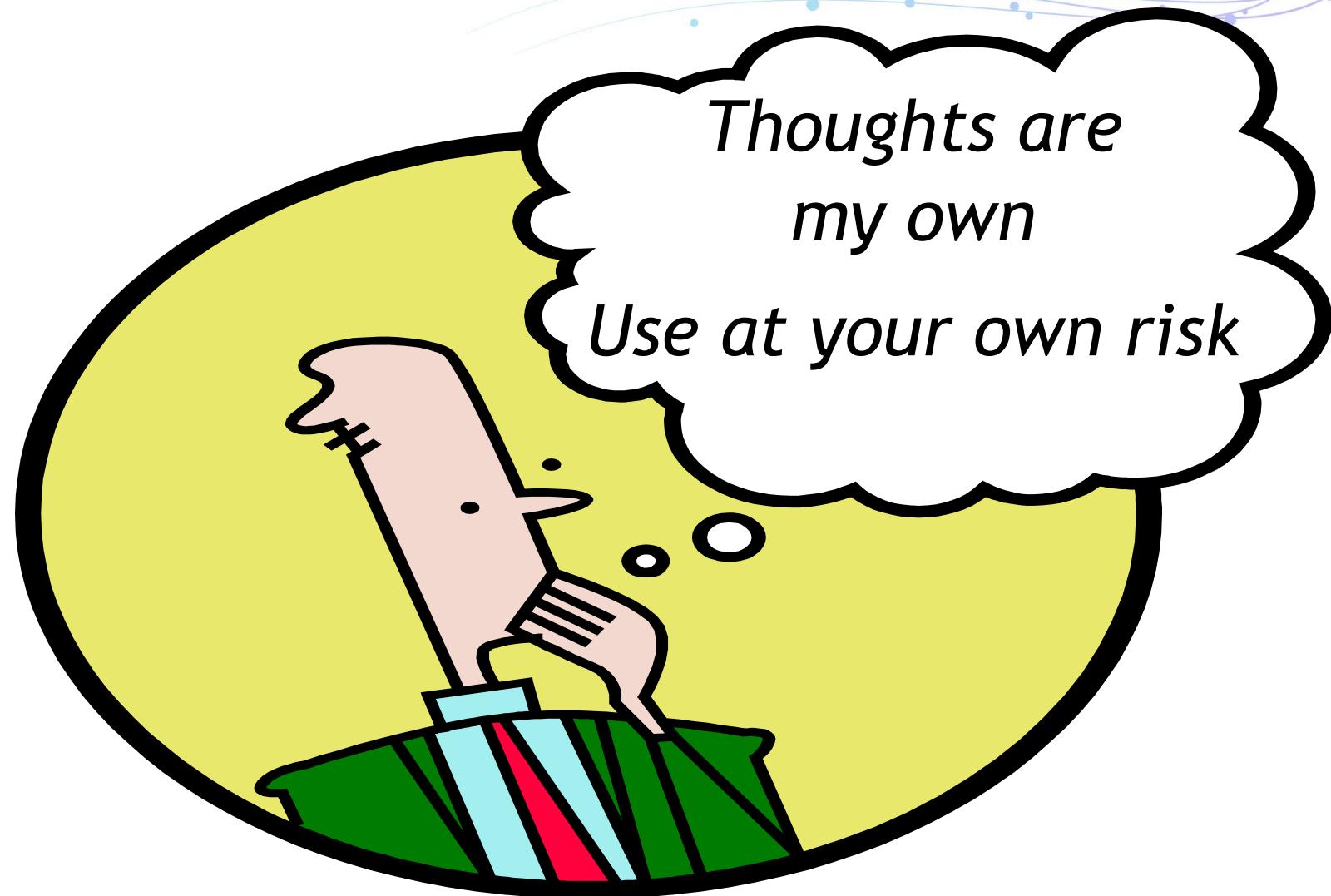
Ron Woerner, CISSP, CISM

Chief Security Advisor
RWX Security Solutions, LLC
@ronw123

#RSAC

Ron Woerner - BIO

- President / Chief Trusted Advisor **RWX Security Solutions**
- Cybersecurity Instructor, Bellevue University
- 25+ years experience in IT / Security
- CISSP, CISM
- Blogger, podcaster & writer
- Given tons'o presentations on security and Internet safety





Content as of January 2019

What the \$%\$# are we doing here?

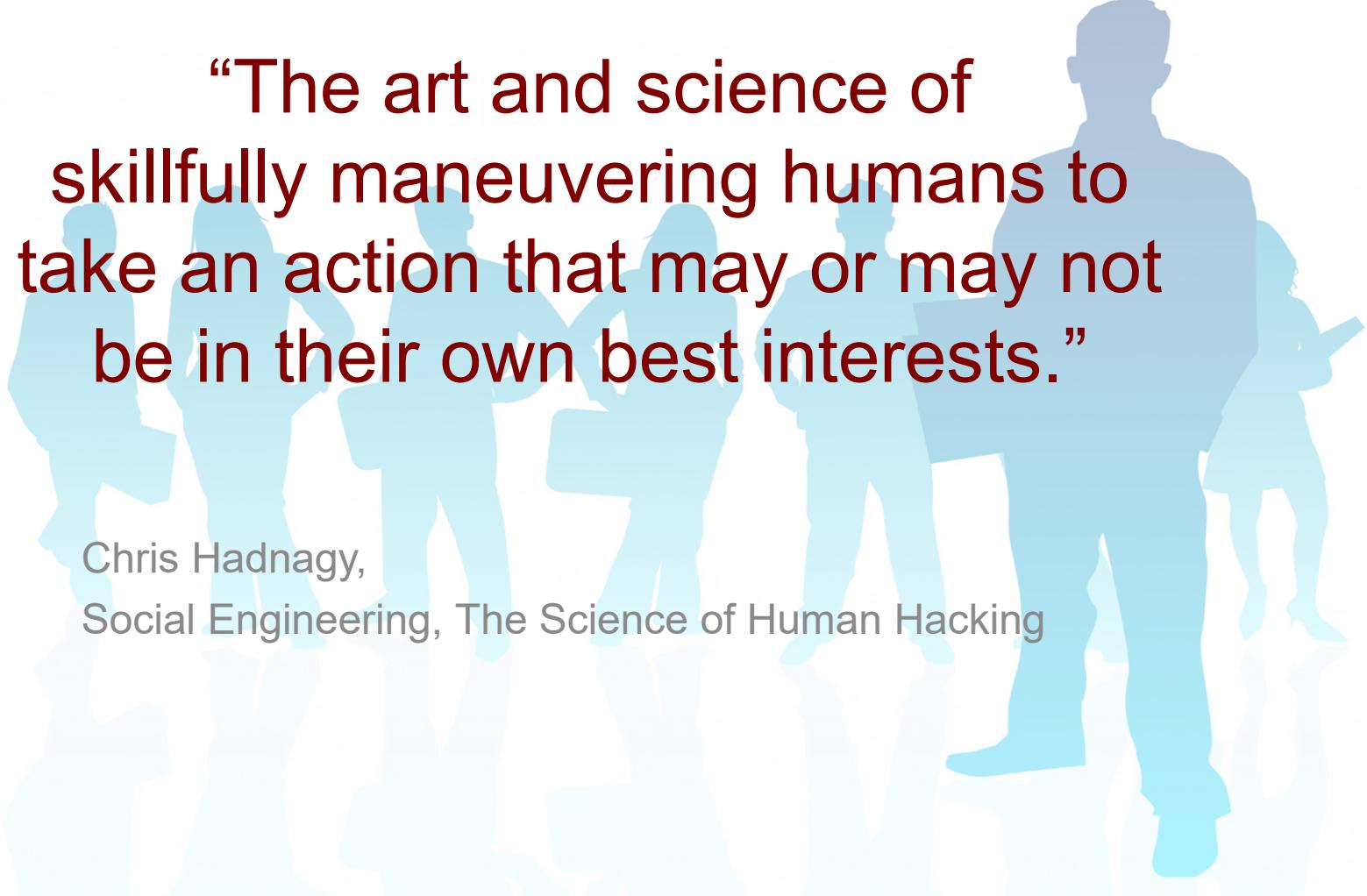
How to be really
dangerous...

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

Cool technologies

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

The Easiest Hack

A background image showing a group of people from behind, walking in a crowd. Some individuals are looking at their phones. The silhouettes are rendered in a light blue color.

“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 Science of Human Hacking

If you only remember 1 slide...



<https://www.stopthinkconnect.org/>



<https://www.lockdownyourlogin.com/>

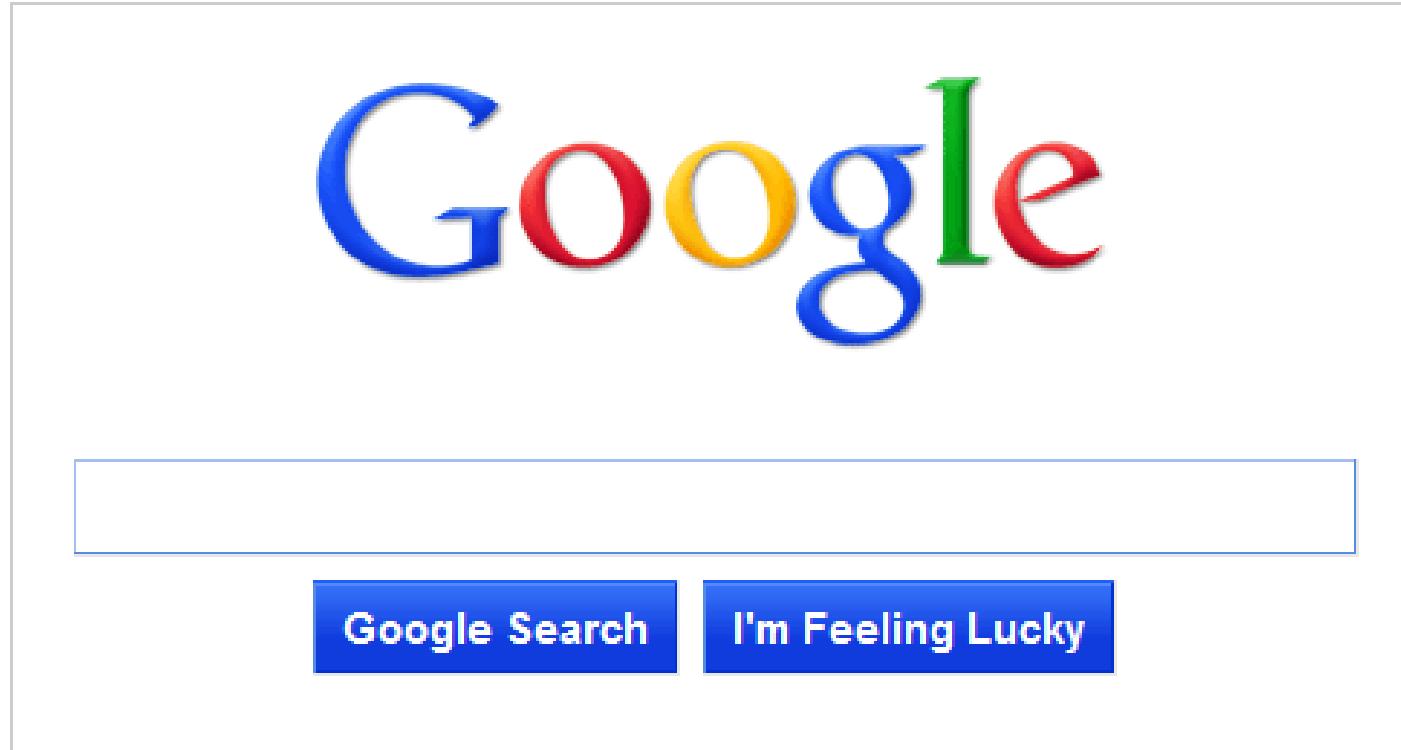


<https://staysafeonline.org/>



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

#1 Technical Tool



https://www.google.com/advanced_search

Time Travel

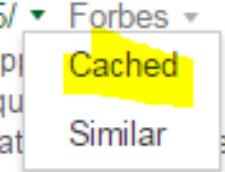
- Google Cache

The Top 10 Security Breaches Of 2015 - Forbes

www.forbes.com/sites/quora/2015/12/.../the-top-10-security-breaches-of-2015/

Dec 31, 2015 - What are the top 10 Cyber security breaches of 2015? originally ap...

Quora: The best answer to any question. ... Data breaches have become a status quo how attackers keep finding paths to infiltrate networks and steal confidential information. ... the top 10 ...



- Archive.org – Wayback Machine



Lists of tools, tips, & tricks

- [SecTools](#)
- Tools Watch – [Top Security Tools](#)
- [OlderGeeks](#)
- [HowToGeek.com](#), [Geek School](#)

Security Checklists / Publications

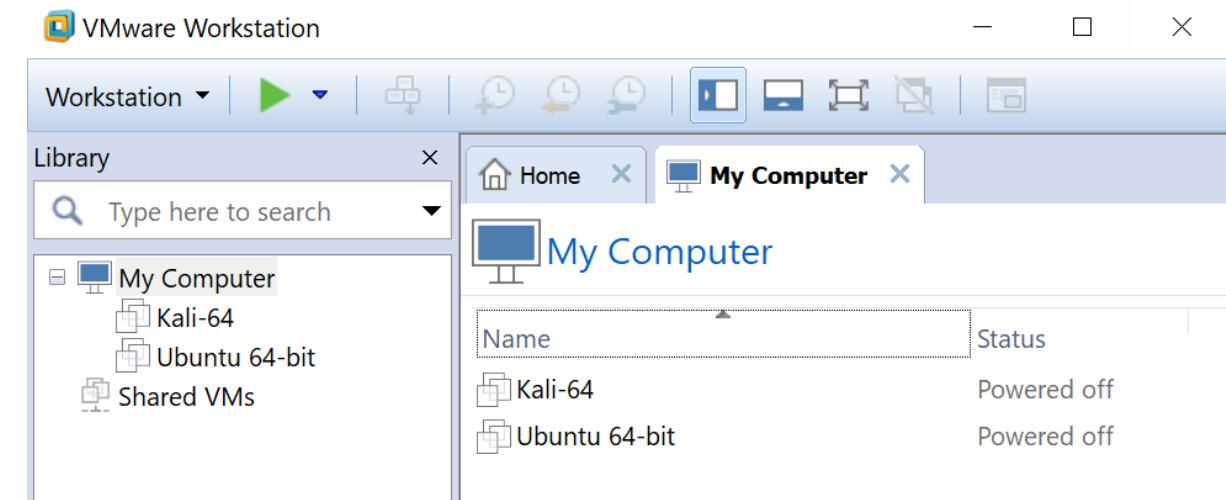
- NIST
 - CSRC: <http://csrc.nist.gov/>
 - Publications: <http://csrc.nist.gov/publications/PubsSPs.html>
- Center for Internet Security
 - Controls: <https://www.cisecurity.org/controls/>
 - Benchmarks: <https://www.cisecurity.org/cis-benchmarks/>
 - [CIS Controls Self-Assessment Tool, or CIS CSAT](#)
- DISA IASE Security Technical Implementation Guides (STIGs):
<https://iasc.disa.mil/stigs/Pages/index.aspx>
- U.S. Cyber Consequences Unit (US-CCU) [Cyber Security Matrix](#)

Cheat Sheets

- Peerlyst – [Complete List of InfoSec Cheat Sheets](#)
- Lenny Zeltser – IT and Information Security Cheat Sheets:
<https://zeltser.com/cheat-sheets/>
- Malware Archeology (Auditing) –
<https://www.malwarearchaeology.com/cheat-sheets/>
- OWASP –
[https://www.owasp.org/index.php/OWASP Cheat Sheet Series](https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series)

Personal Labs – Virtual Environments

- Oracle VM VirtualBox
- VMWare Workstation
- Windows 10 – Hyper-V
- MacOS Parallels



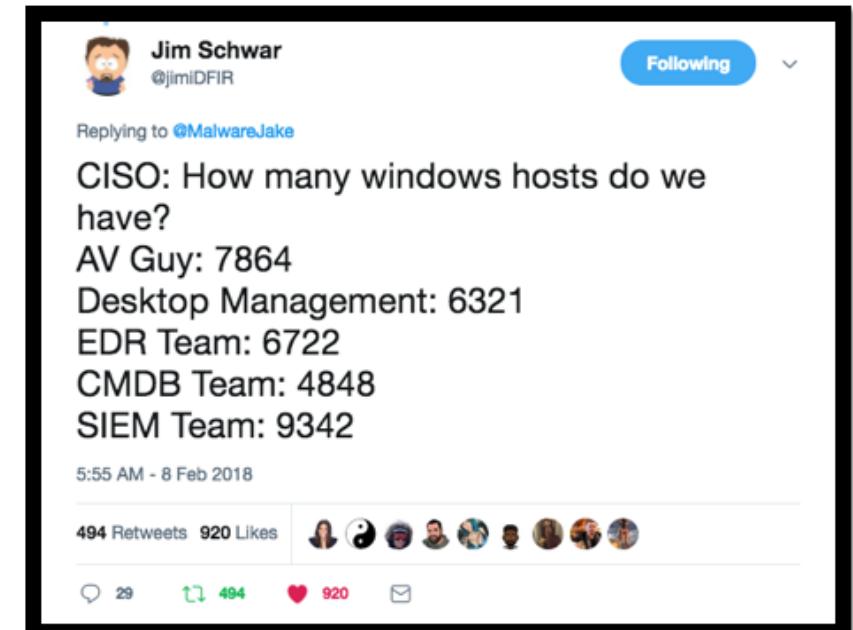
LifeHacker – How to Set Up a Virtual Machine for Free

System Inventory & Automation

- “Asset management isn’t sexy. Penetration testing and red team and analysis gets all the job reqs, because it’s far more flashy. Effective security is boring.”
Nathan W Burke

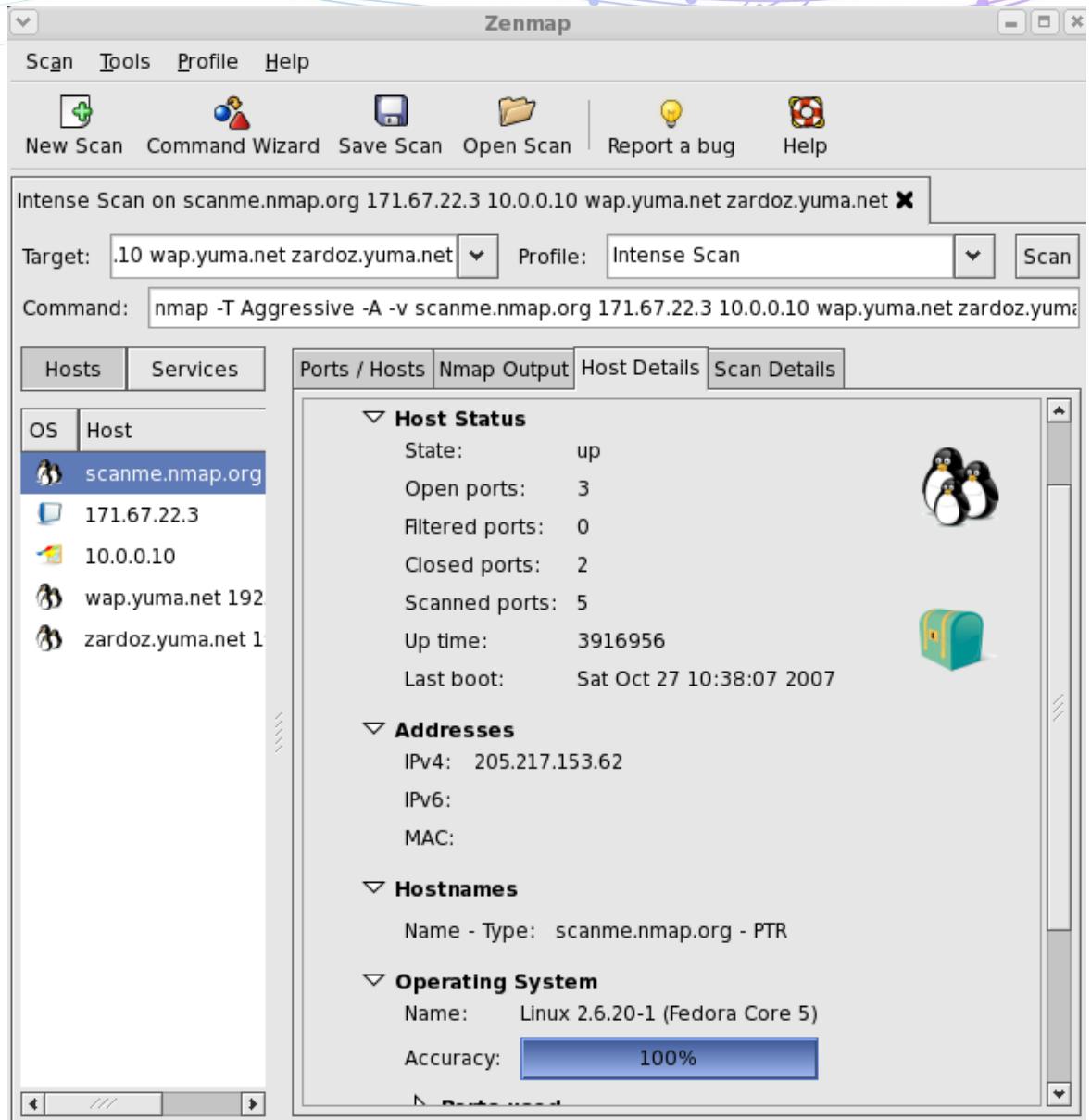
- Center for Internet Security
CSC Basic Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets



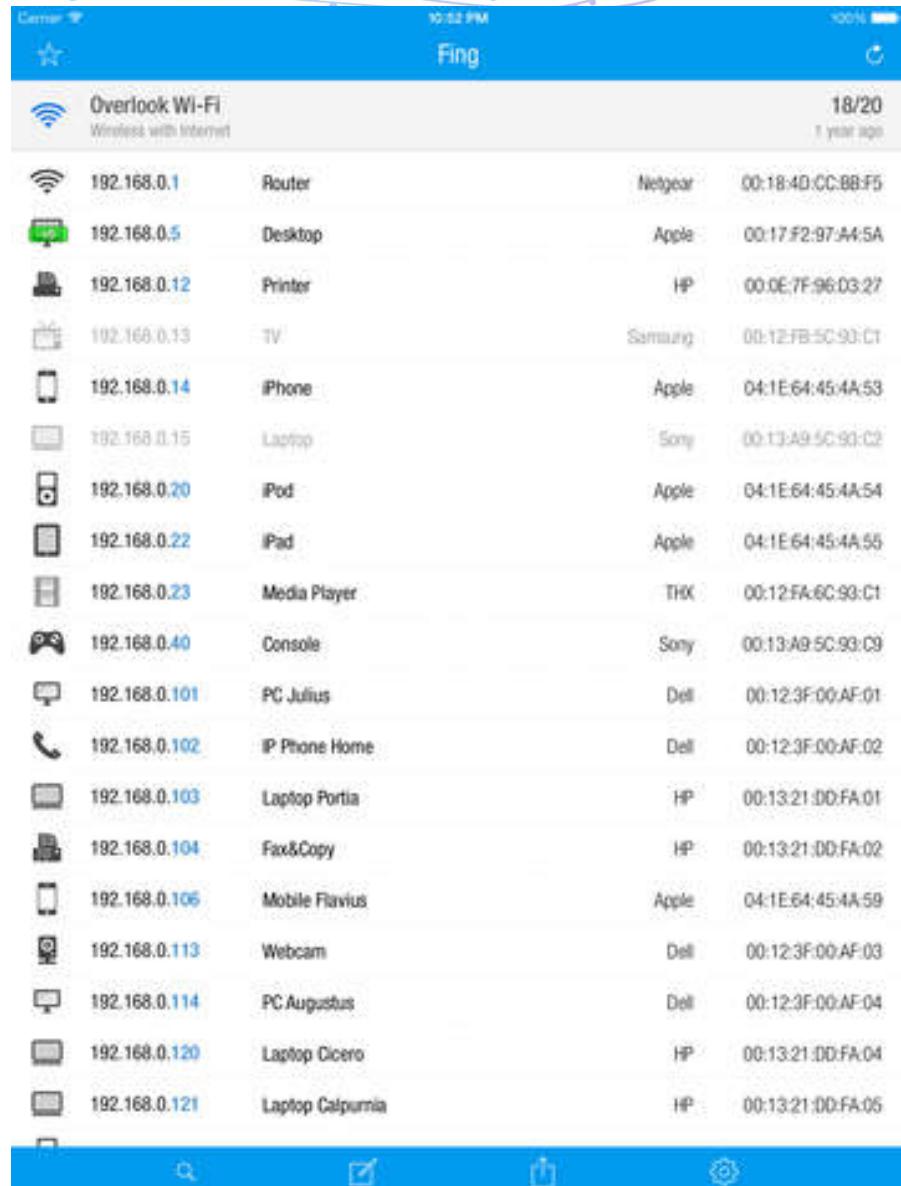
Network Mapping

Nmap / ZenMap



Network Mapping

Fing
(iOS & Android)



The screenshot shows the Fing mobile application interface. At the top, there's a blue header bar with the text "Overlook Wi-Fi" and "Fing". Below the header is a table listing 20 devices connected to the network. Each row contains an icon representing the device type, its IP address (e.g., 192.168.0.1 to 192.168.0.121), its name or model, its manufacturer, and its MAC address.

192.168.0.1	Router	Netgear	00:18:4D:CC:BB:F5	
192.168.0.5	Desktop	Apple	00:17:F2:97:A4:5A	
192.168.0.12	Printer	HP	00:0E:7F:96:03:27	
192.168.0.13	TV	Samsung	00:12:FB:5C:90:C1	
192.168.0.14	iPhone	Apple	04:1E:64:45:4A:53	
192.168.0.15	Laptop	Sony	00:13:A9:5C:90: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:90:C1	
192.168.0.40	Console	Sony	00:13:A9:5C:90:C0	
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	00:13:21:00:FA:01	
192.168.0.104	Fax&Copy	HP	00:13:21:00: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	00:13:21:00:FA:04	
192.168.0.121	Laptop Calpurnia	HP	00:13:21:00:FA:05	

Network Enumeration

Shodan (<https://www.shodan.io/>) – Search engine for Internet-connected devices.

The screenshot shows the Shodan search interface with the query "bellevue.edu" entered in the search bar. The results page displays the following information:

- TOTAL RESULTS**: 4
- TOP COUNTRIES**: United States (4)
- SSL Certificate**:
 - Issued By: DigiCert SHA2 High Assurance Server CA
 - Common Name: *.bellevue.edu
 - Organization: DigiCert Inc
- Supported SSL Versions**: SSLv3, TLSv1, TLSv1.1, TLSv1.2
- Details**:
 - vpa02pps01.bellevue.edu (Cox Communications, United States, Omaha)
 - starttls button
- Logs**: 220 vpa02pps01.bellevue.edu ESMTP Mon, 30 Apr 2018 01:30:10 -0500

Network Enumeration

Censys (<https://www.censys.io/>) - Find and analyze every reachable server and device on the Internet.

The screenshot shows the Censys search interface. At the top, there is a logo, a search bar set to "IPv4 Hosts" with the query "bellevue.edu", and links for "Register" and "Sign In". Below the search bar, there are navigation links: "Results" (which is underlined), "Map", "Metadata", "Report", and "Docs". On the left, there is a "Quick Filters" section with a note about Data Definitions, an "Autonomous System:" dropdown set to "26 ASN-CXA-ALL-CCI-22773-RDC - Cox Communications Inc., US", and a "RACKSPACE - Rackspace" link. The main area displays search results for "IPv4 Hosts" with 35 results on page 1/2. The first result is for IP 66.37.231.42, which is associated with the domain bell-3-42.bellevue.edu. It shows details like being owned by Cox Communications Inc. (22773) in Bellevue, Nebraska, United States, using port 443/https, and having certificates for *.bellevue.edu, bellevue.edu, and VPW802DIR01.bellevue.edu. A specific search term, "443.https.tls.certificate.parsed.names: bellevue.edu", is highlighted with a yellow box. The second result is for IP 66.37.229.47, associated with vpa02pps01.bellevue.edu, also owned by Cox Communications Inc. (22773) in La Vista, Nebraska, United States, using port 25/smtp.

Autonomous System:	Host IP	Domain	Owner	Location	Ports
26 ASN-CXA-ALL-CCI-22773-RDC - Cox Communications Inc., US	66.37.231.42	bell-3-42.bellevue.edu	Cox Communications Inc. (22773)	Bellevue, Nebraska, United States	443/https
RACKSPACE - Rackspace	66.37.229.47	vpa02pps01.bellevue.edu	Cox Communications Inc. (22773)	La Vista, Nebraska, United States	25/smtp

Network Vulnerability Detection



Home Projects Qualys.com Contact

HOW WELL DO YOU KNOW SSL?

If you want to learn more about the technology that protects the Internet, you've come to the right place.



[Test your server »](#)
Test your site's certificate and configuration



[Test your browser »](#)
Test your browser's SSL implementation



[SSL Pulse »](#)
See how other web sites are doing



[Documentation »](#)
Learn how to deploy SSL/TLS correctly

<https://www.ssllabs.com/>

Network Vulnerability Detection

- Titania Nipper Studio: <https://www.titania.com/products/nipper-studio>
- Solarwinds: <https://www.solarwinds.com/downloads>
 - [Firewall Browser](#)
 - [Network Configuration Manager](#)
 - [IP Address Manager](#)
- Firewall Audit Tool: <https://www.wallparse.com/>



FIREWALL AUDIT TOOL

Firewall Review, Analysis and Normalization

Windows Administration

SysInternals Suite

- Autoruns
- Process Explorer
- Process Monitor

Video:

Mark Russinovich,
Malware Hunting

Sysinternals Suite

06/13/2017 • 2 minutes to read • Contributors  all

By Mark Russinovich

Updated: December 18, 2018

[Download Sysinternals Suite](#) (23.2 MB)

[Download Sysinternals Suite for Nano Server](#) (4.6 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](#), [LMDMDump](#), [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](#), [VMMMap](#), [VolumID](#), [Whois](#), [WinObj](#), [ZoomIt](#)

[Download Sysinternals Suite](#) (22.6 MB)

[Download Sysinternals Suite for Nano Server](#) (4.7 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



Windows Administration

Windows Update Agent (WUA)

[Using WUA to Scan for Updates Offline](#), which includes a sample .vbs script. For a PowerShell alternative, see [Using WUA to Scan for Updates Offline with PowerShell](#).

Replaces MBSA

PowerShell

- [Using Windows PowerShell](#)
- [PowerShell.exe Command-Line Help](#)

Linux on Windows

Windows Subsystem for Linux

<https://docs.microsoft.com/en-us/windows/wsl/about>

Run bash.exe

[HTG Article:](#)

<https://www.howtogeek.com/270810/how-to-quickly-launch-a-bash-shell-from-windows-10s-file-explorer/>



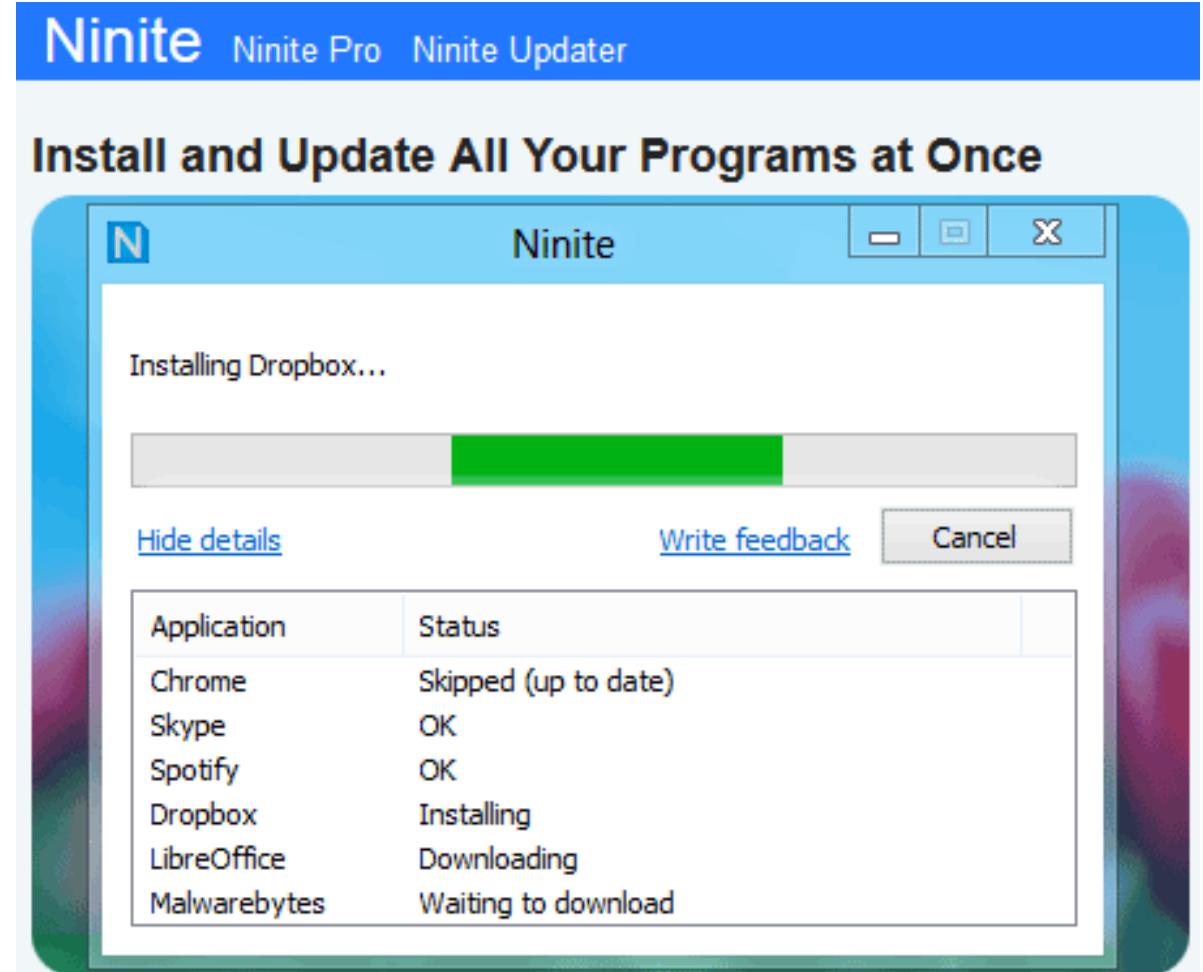
A screenshot of a Windows terminal window titled 'ronw@LAPTOP-RNVFHPNO: ~'. The window contains the following text:

```
ronw@LAPTOP-RNVFHPNO:~$ pwd  
/home/ronw  
ronw@LAPTOP-RNVFHPNO:~$ whoami  
ronw  
ronw@LAPTOP-RNVFHPNO:~$ ls -l  
total 0  
ronw@LAPTOP-RNVFHPNO:~$
```

Patching & Updating

Ninite

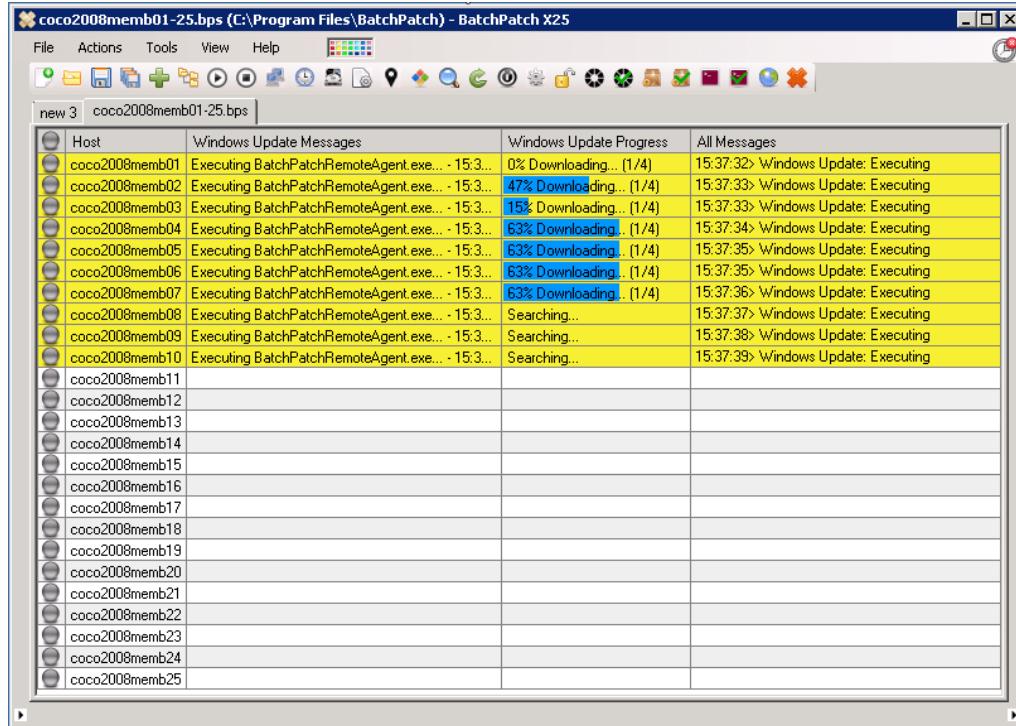
(<https://ninite.com/>)



Patching & Updating

BatchPatch

<https://batchpatch.com/>



Chocolatey

<https://chocolatey.org/>



Network Evaluation / Troubleshooting



Introduction video

TcpDump

A screenshot of the Wireshark application window titled "few packets.cap - Ethereal". The main pane displays a list of network packets captured from a file named "few packets.cap". The columns include No., Time, Deka, Source, Destination, Protocol, and Info. The "Info" column shows detailed packet descriptions, such as TCP SYN and ACK segments, HTTP GET requests, and DCERPC Bind calls. Below the list, a expanded view of packet 16 is shown, displaying the full Ethernet frame, IP header, TCP header, and the raw HTTP GET request payload. The payload includes headers like Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Accept-Charset, and Connection. At the bottom of the window, there is a status bar with a "tcp" filter, search and expression fields, and file statistics.

Linux Distros



DistroWatch.com
Put the fun back into computing. Use Linux, BSD.

Type Distribution Name Go Select Distribution Go
 Go Random Distribution

<https://distrowatch.com/>

The LiveCD List

[Home](#) :: [About](#)

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

Linux / Unix Security

- Hardening Linux Systems - <https://www.beyondtrust.com/blog/harden-unix-linux-systems-close-security-gaps/>
- Linode's [Getting Started with SELinux Guide](#)
- [The Geek Stuff](#)



Security / Pen Testing Distros

- Kali

<https://www.kali.org/downloads/>

- Parrot Security OS

<https://www.parrotsec.org/download-security.php>

- Tails

<https://tails.boum.org/>



Pen Testing Framework



<https://www.metasploit.com/>



Taking notes in notepad? Have Metasploit Pro track & report your progress and findings -- learn more on <http://rapid7.com/metasploit>

```
=[ metasploit v4.10.0-2014082003 [core:4.10.0.pre.2014082003 api:1.0.0] ]
+ ---=[ 1331 exploits - 722 auxiliary - 214 post      ]
+ ---=[ 340 payloads - 35 encoders - 8 nops        ]
+ ---=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

msf >

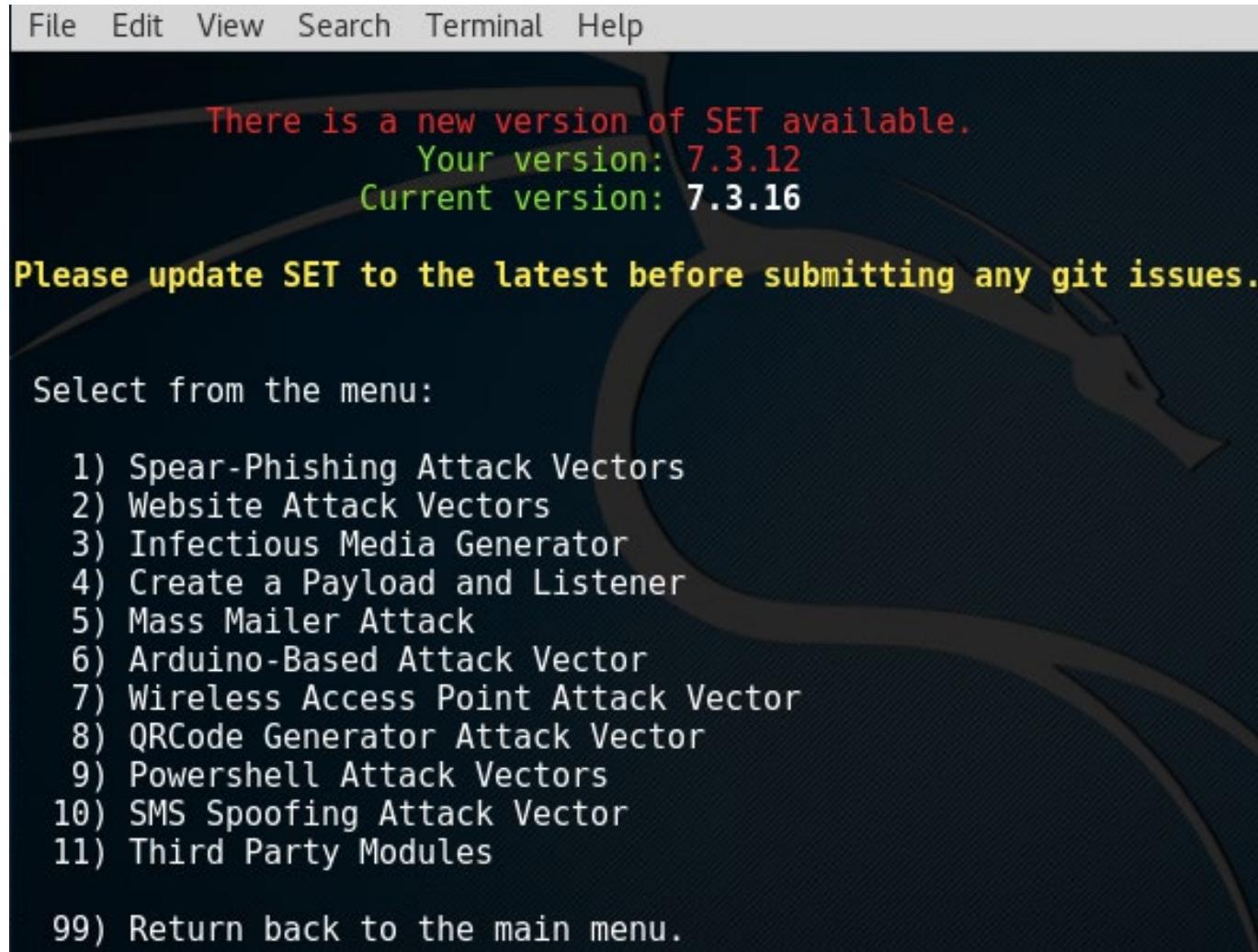
<https://www.offensive-security.com/metasploit-unleashed/requirements/>

Social Engineering

- IntelTechniques (OSInt) – <https://inteltechniques.com/menu.html>
- Maltego – <https://www.paterva.com/>
- Cree.py – Geolocation Information Aggregator, <http://www.geocreepy.com/>
- Peek You - www.peekyou.com

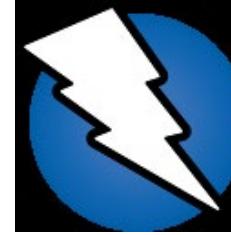
Social Engineering Toolkit (SET)

<https://www.trustedsec.com/social-engineer-toolkit-set/>



Security Testing

- OWASP Zed Attack Proxy (ZAP)



- Portswigger Burp Suite



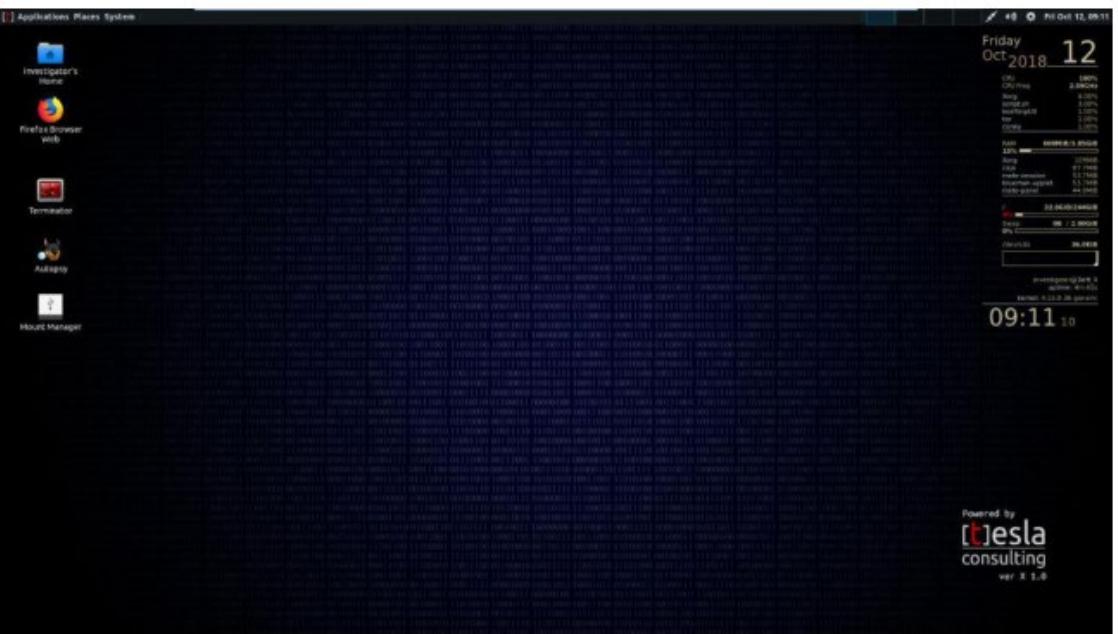
- Vega



- Netsparker

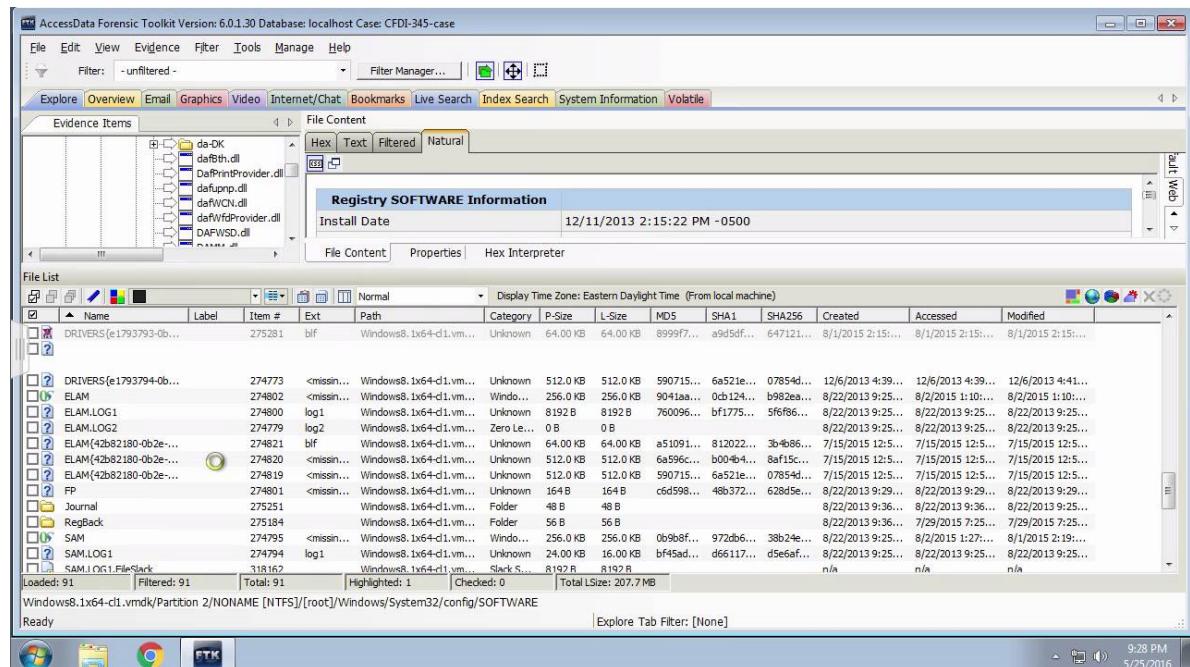


- GuardiCore Infection Monkey



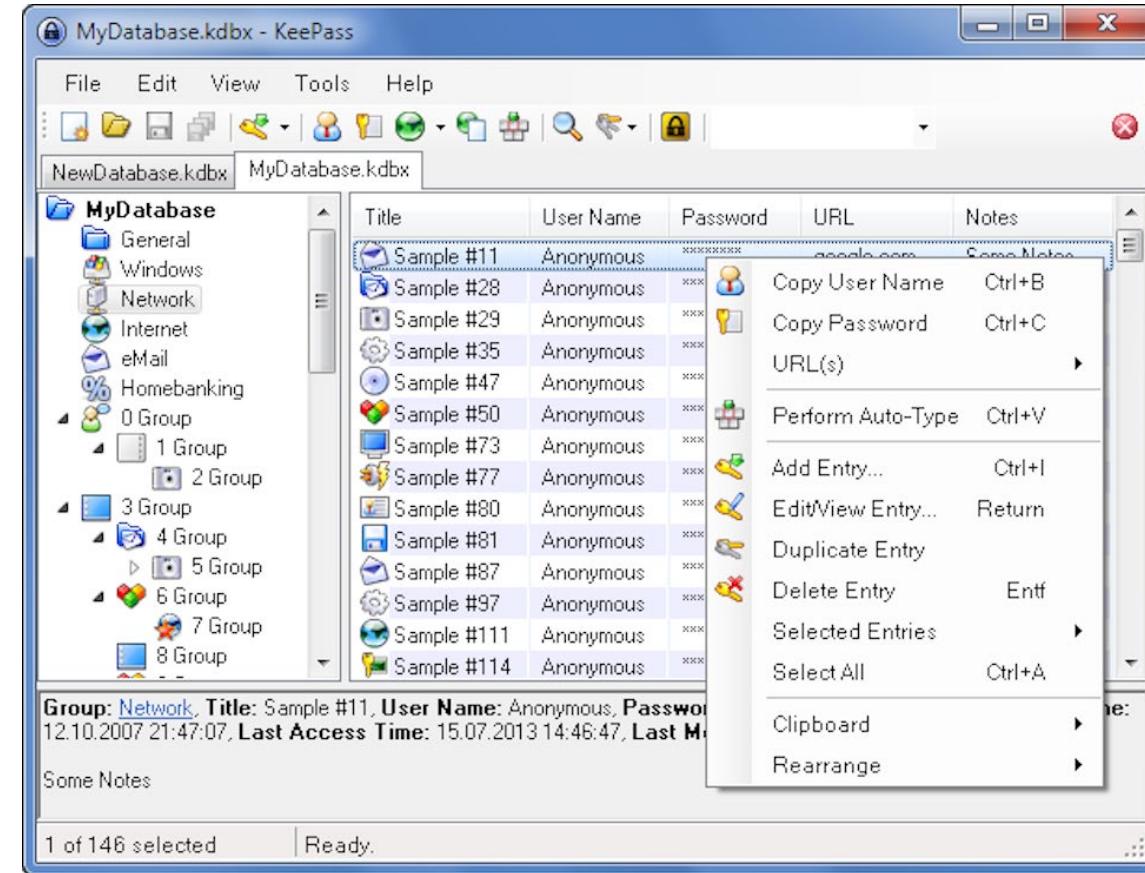
Digital Forensics

- DEFT X
- OSForensics
- FTK
- WinHex



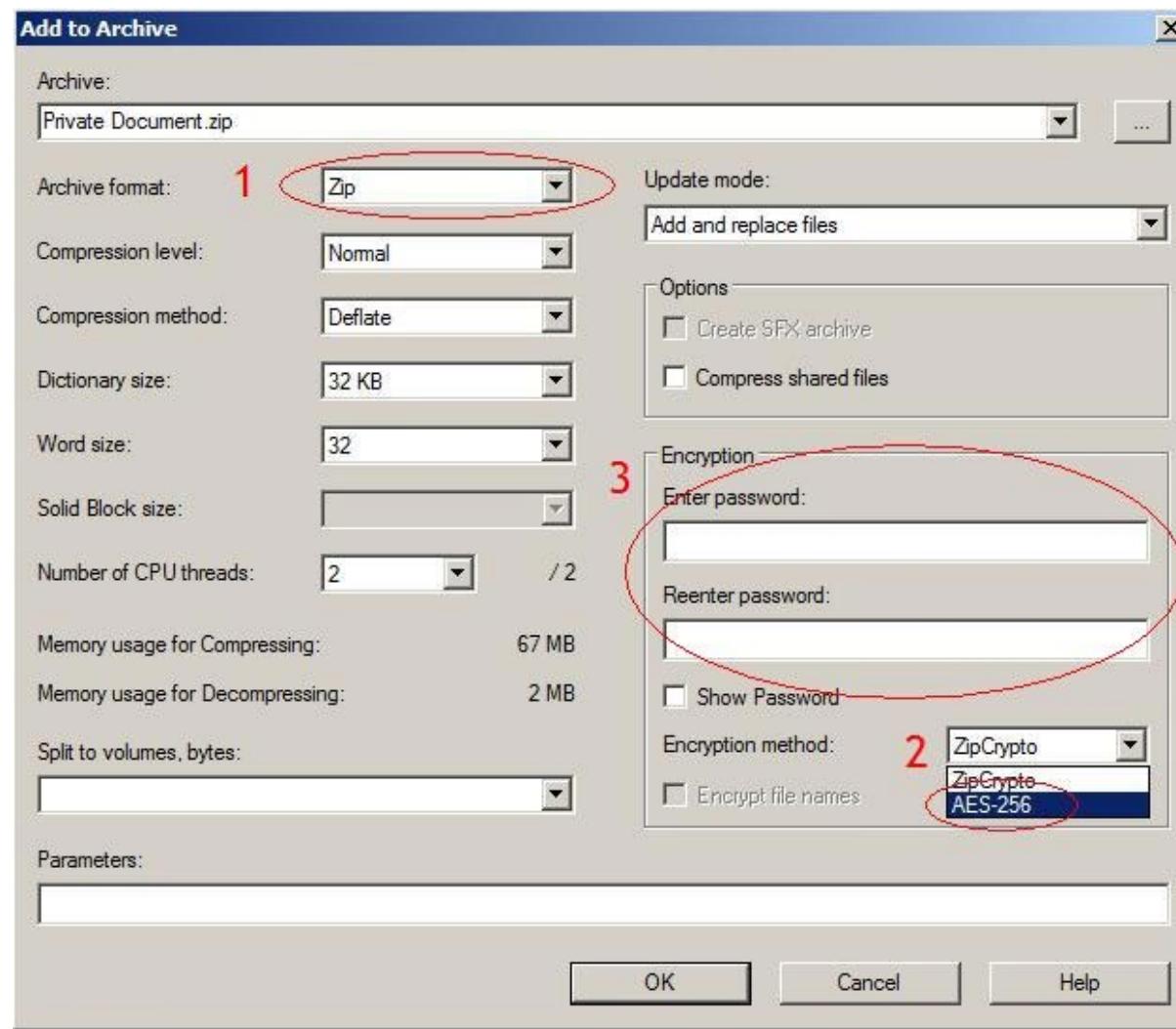
Personal Security – Password Vaults

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



Personal Security – Encryption

- 7-Zip
 - AES Crypt
 - Veracrypt



Security Awareness

StaySafeOnline

Powered by: National Cyber Security Alliance



National Cybersecurity
Awareness Month



CyberAware

<https://staysafeonline.org/ncsam/>

Security Books

CYBERSECURITY

CANON



A Rock & Roll Hall of Fame for Cybersecurity Books

To identify a list of must-read books for all cybersecurity practitioners – be they from industry, government or academia – where the content is timeless, genuinely represents an aspect of the community that is true and precise, reflects the highest quality and, if not read, will leave a hole in the cybersecurity professional's education that will make the practitioner incomplete.

<https://cybercanon.paloaltonetworks.com/>

What Else?

ما هي الأمور الأخرى؟

Help add to the list

“Apply Slide”

- Immediate:
 - Pick 1 or 2 tools / techniques
 - Play / Try it out / Experiment
- Next 4-6 Weeks (rinse and repeat in 3 & 6 mos):
 - Review this slide deck
 - Pick more tools (3-5)
 - Experiment with tools in a virtual environment
 - Review the awareness websites

Share!

RSA®Conference2019

Cybersecurity Tips, Tools, & Techniques

Ron Woerner, CISSP, CISM

[ron.woerner @ rwxsecurity.com](mailto:ron.woerner@rwxsecurity.com)

Twitter: [@ronw123](https://twitter.com/ronw123)

RWX Security Solutions

I HAVE NO SPECIAL
TALENTS. I AM ONLY
**PASSIONATELY
CURIOSUS.**

-ALBERT EINSTEIN