RSAConference2019
San Francisco | March 4–8 | Moscone Center

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

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


Thoughts are
my own
Use at your own risk

Content as of January 2019

What the $%$# are we doing here?

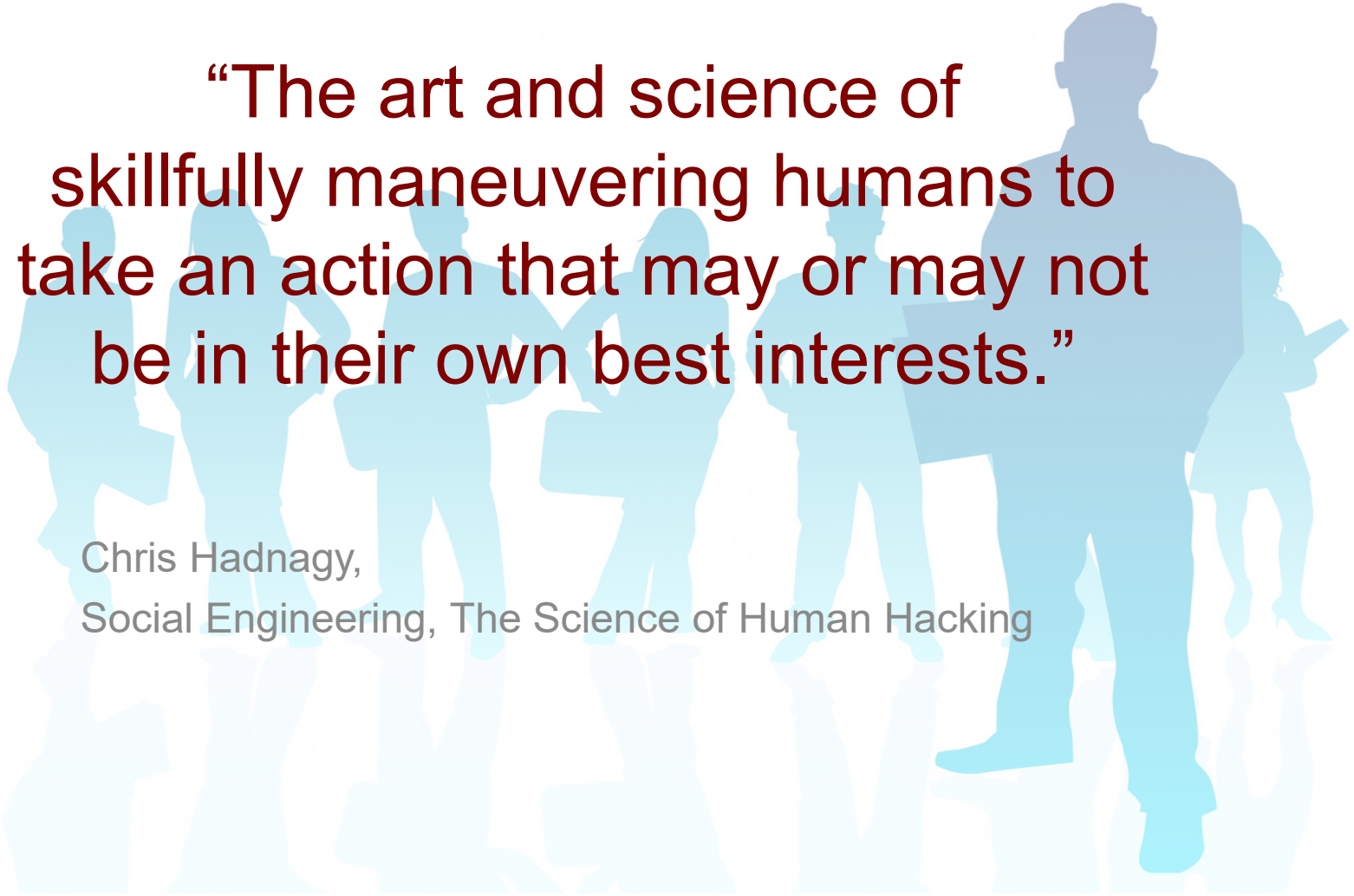
How to be really dangerous…

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



"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…

STOP | THINK | CONNECT™

https://www.stopthinkconnect.org/

LOCK DOWN YOUR LOGIN

https://www.lockdownyourlogin.com/

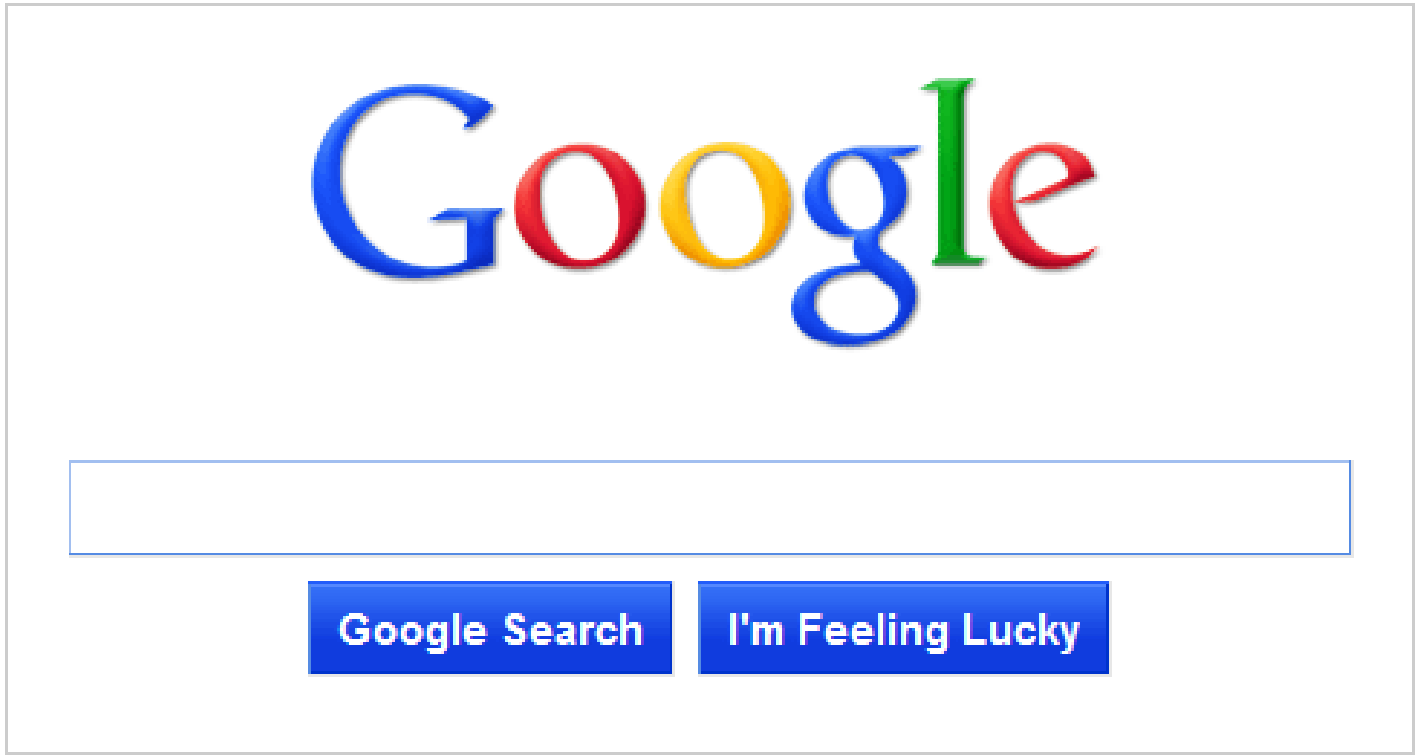
StaySafeOnline
Powered by: National Cyber Security Alliance

https://staysafeonline.org/

if you SEE something | SAY something™

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

#1 Technical Tool

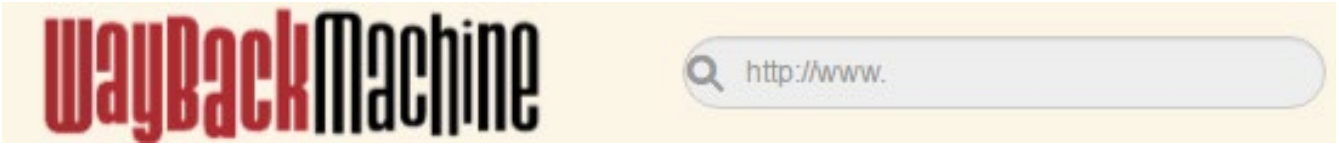


https://www.google.com/advanced_search

Time Travel

- Google Cache

- Archive.org – Wayback Machine



Lists of tools, tips, & tricks

- SecTools
- Tools Watch – Top Security Tools
- OlderGeeks
- HowToGeek.com, Geek School

Security Checklists / Publications

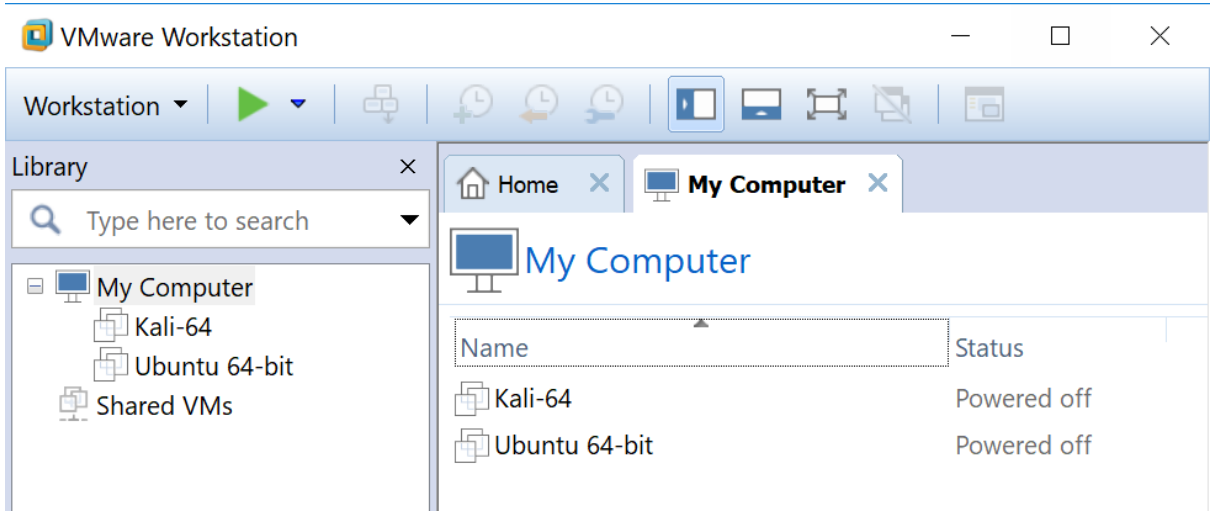
- NIST
  - CSRC: http://csrc.nist.gov/
  - Publications: http://csrc.nist.gov/publications/PubsSPs.html
- Center for Internet Security
  - Controls: https://www.cisecurity.org/controls/
  - Benchmarks: https://www.cisecurity.org/cis-benchmarks/
  - CIS Controls Self-Assessment Tool, or CIS CSAT
- DISA IASE Security Technical Implementation Guides (STIGs): https://iase.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

Personal Labs – Virtual Environments

- Oracle VM VirtualBox
- VMWare Workstation



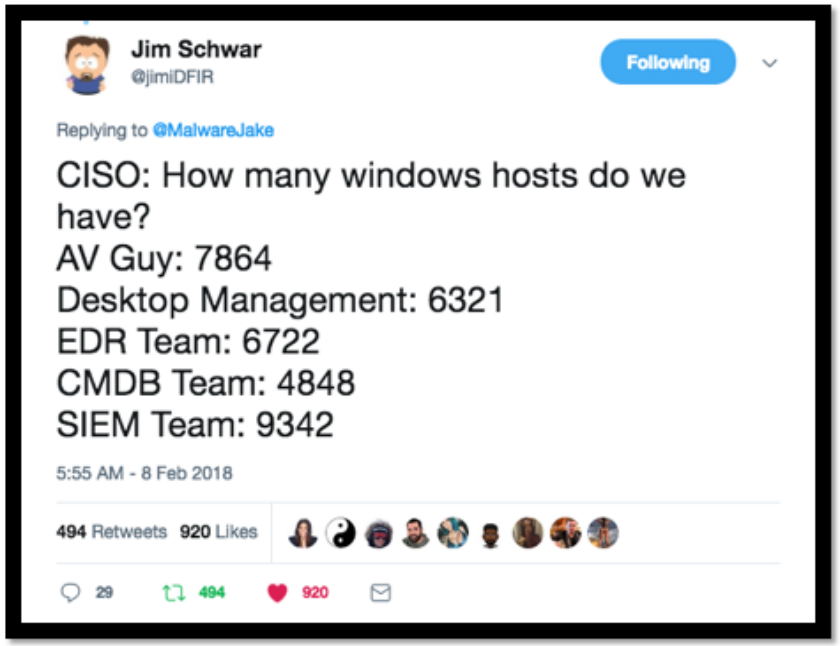
- Windows 10 – Hyper-V
- MacOS Parallels

LifeHacker – How to Set Up a Virtual Machine for Free

System Inventory & Automation

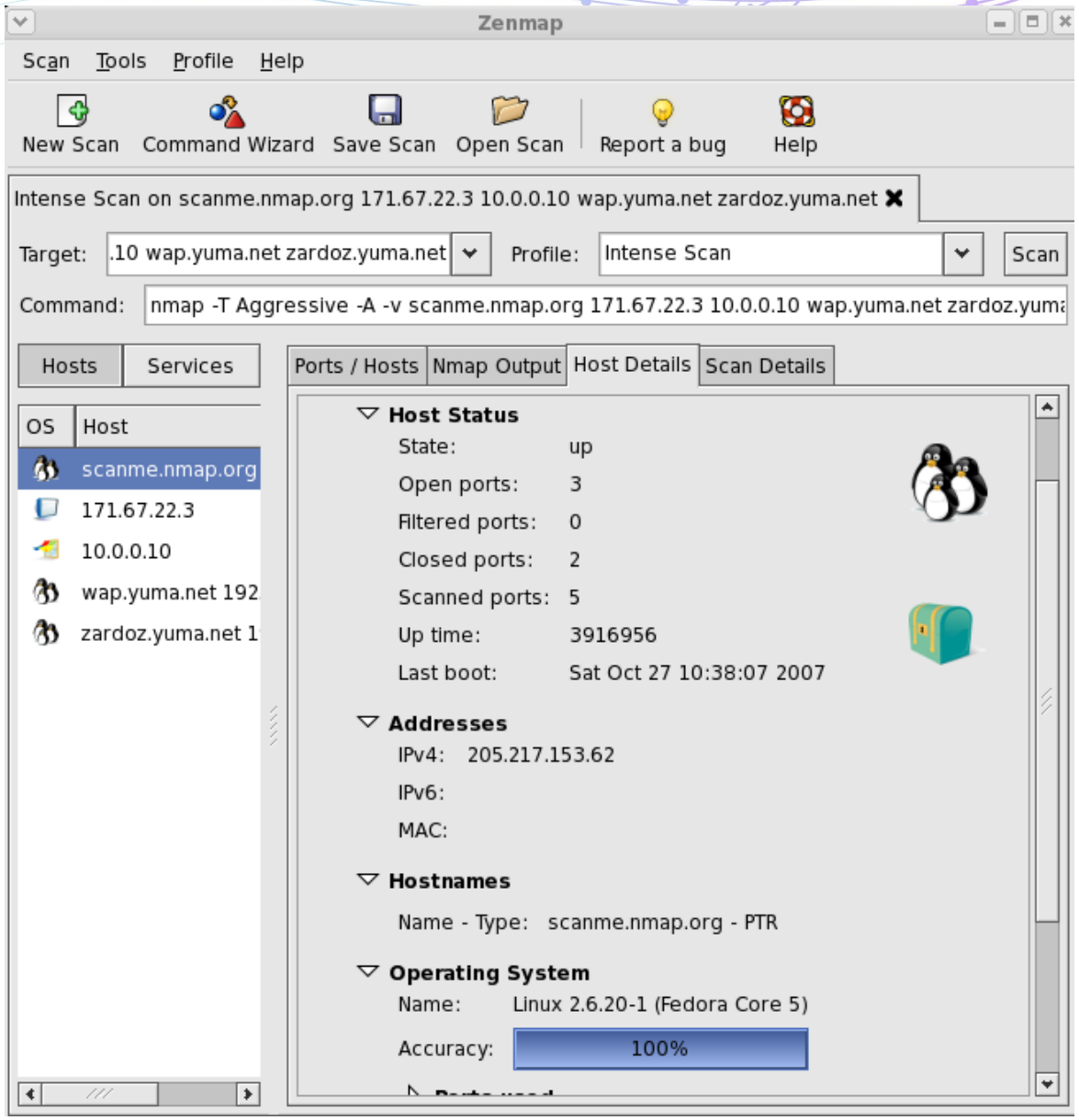
- *"Asset management isn't sexy. Penetration testing and red team and analysis gets all the job reqs, because it's far more flashy. Effective security is boring."* Nathan W Burke

- Center for Internet Security
  CSC Basic Controls
  1. Inventory and Control of Hardware Assets
  2. Inventory and Control of Software Assets



Network Mapping

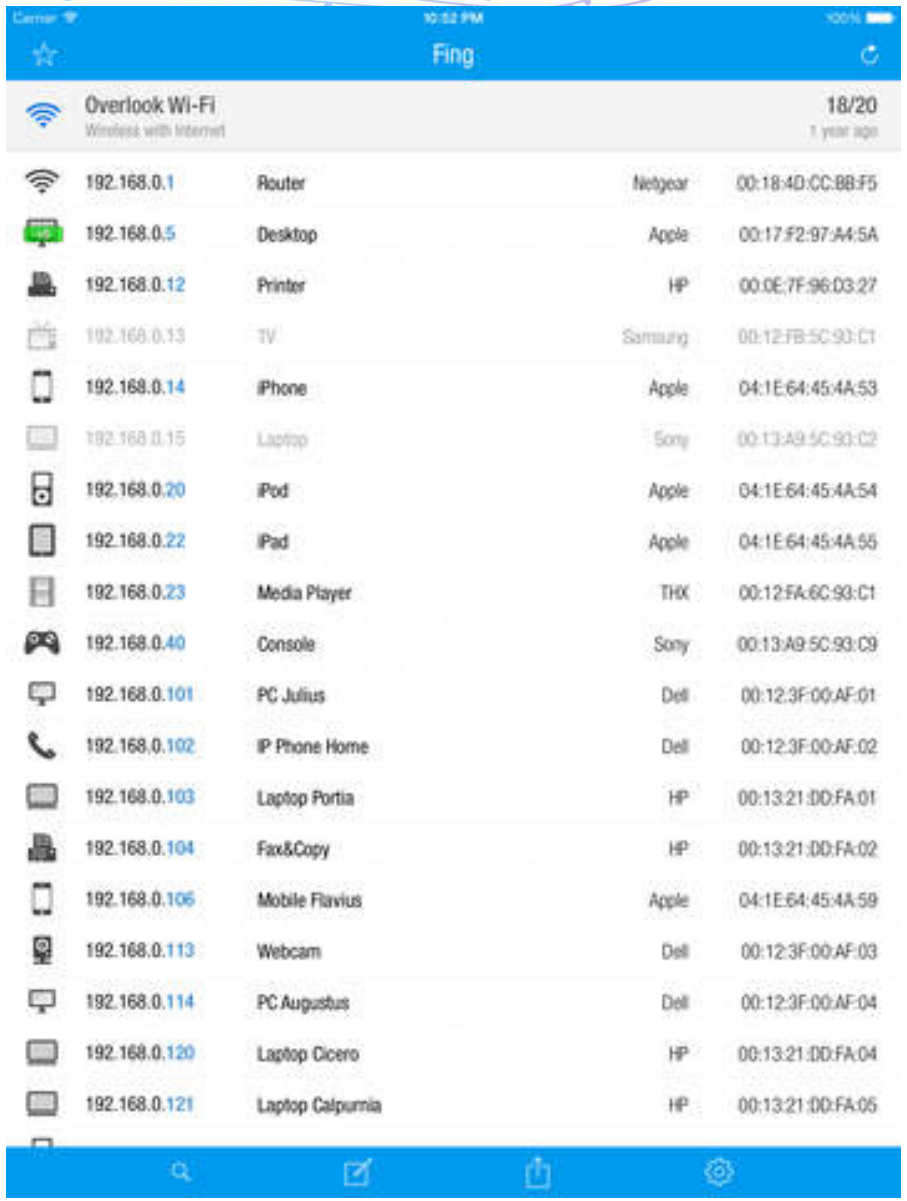
Nmap / ZenMap



Network Mapping

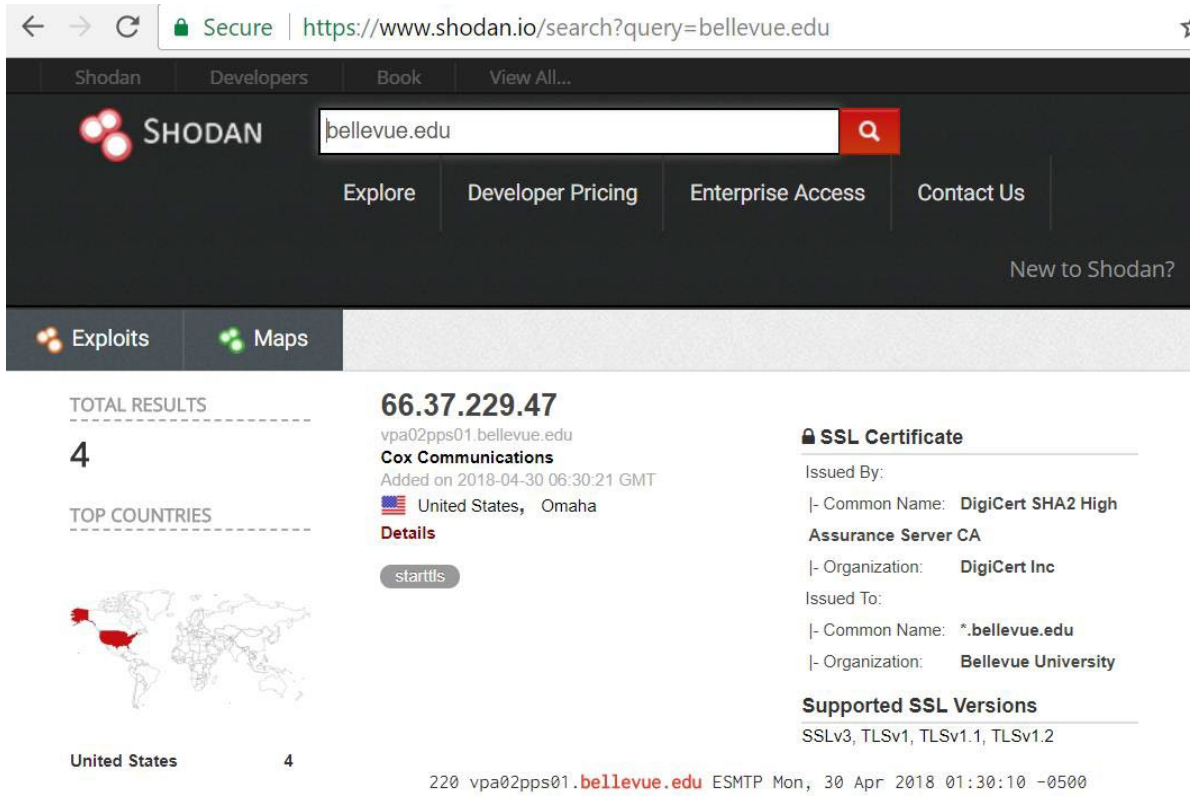
Fing

(iOS & Android)



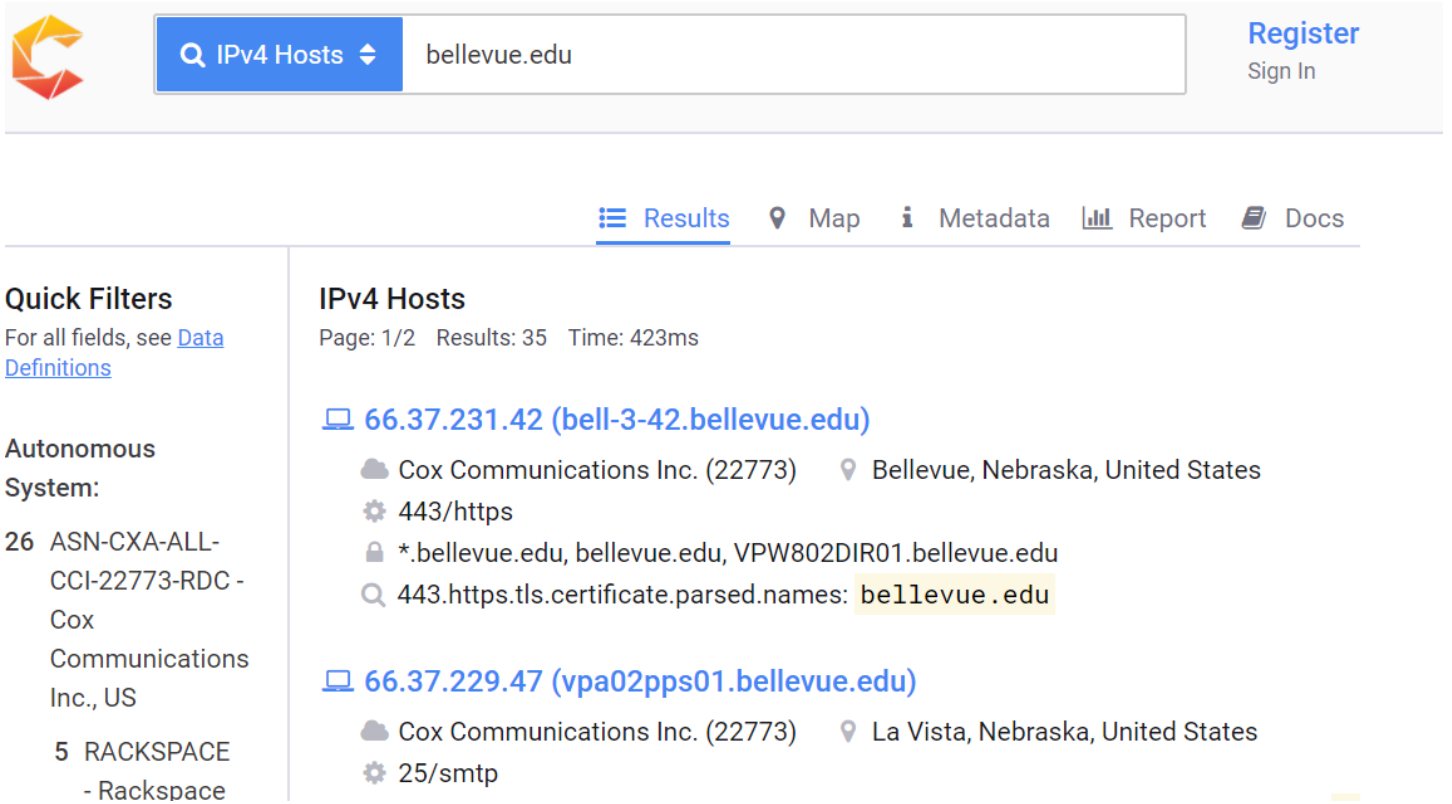
Network Enumeration

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

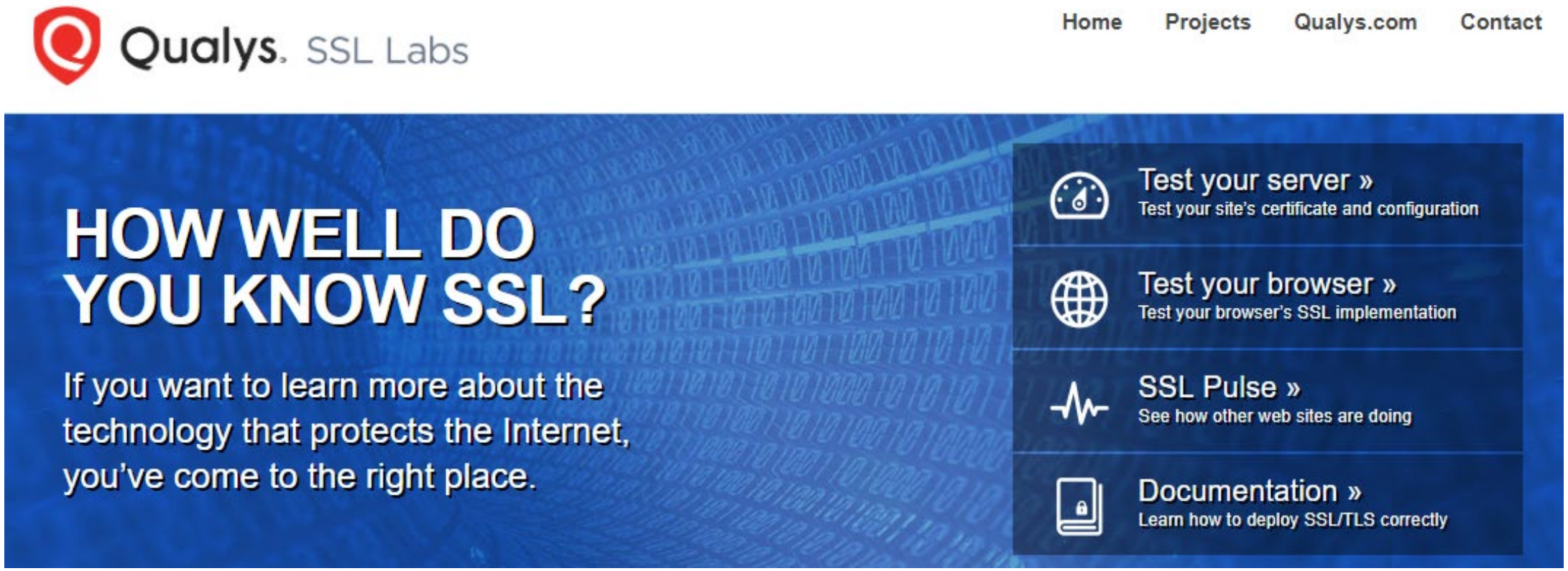


Network Enumeration

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



Network Vulnerability Detection



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, 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)

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

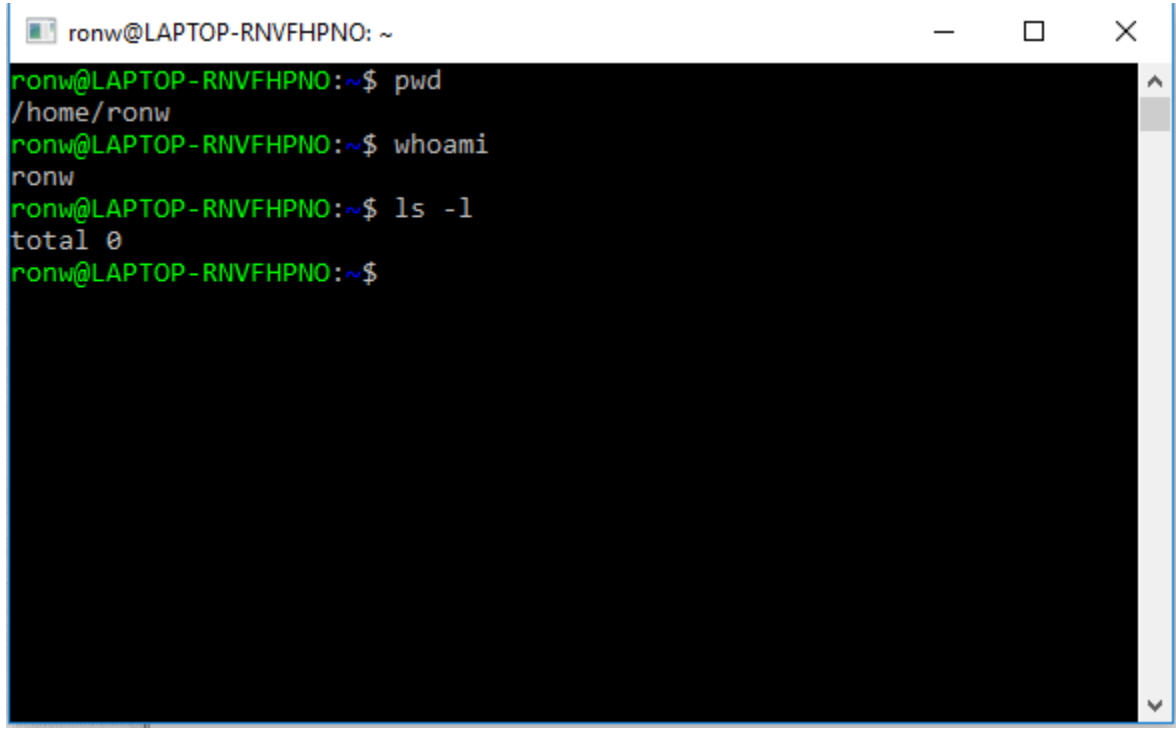
Linux on Windows

Windows Subsystem for Linux

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

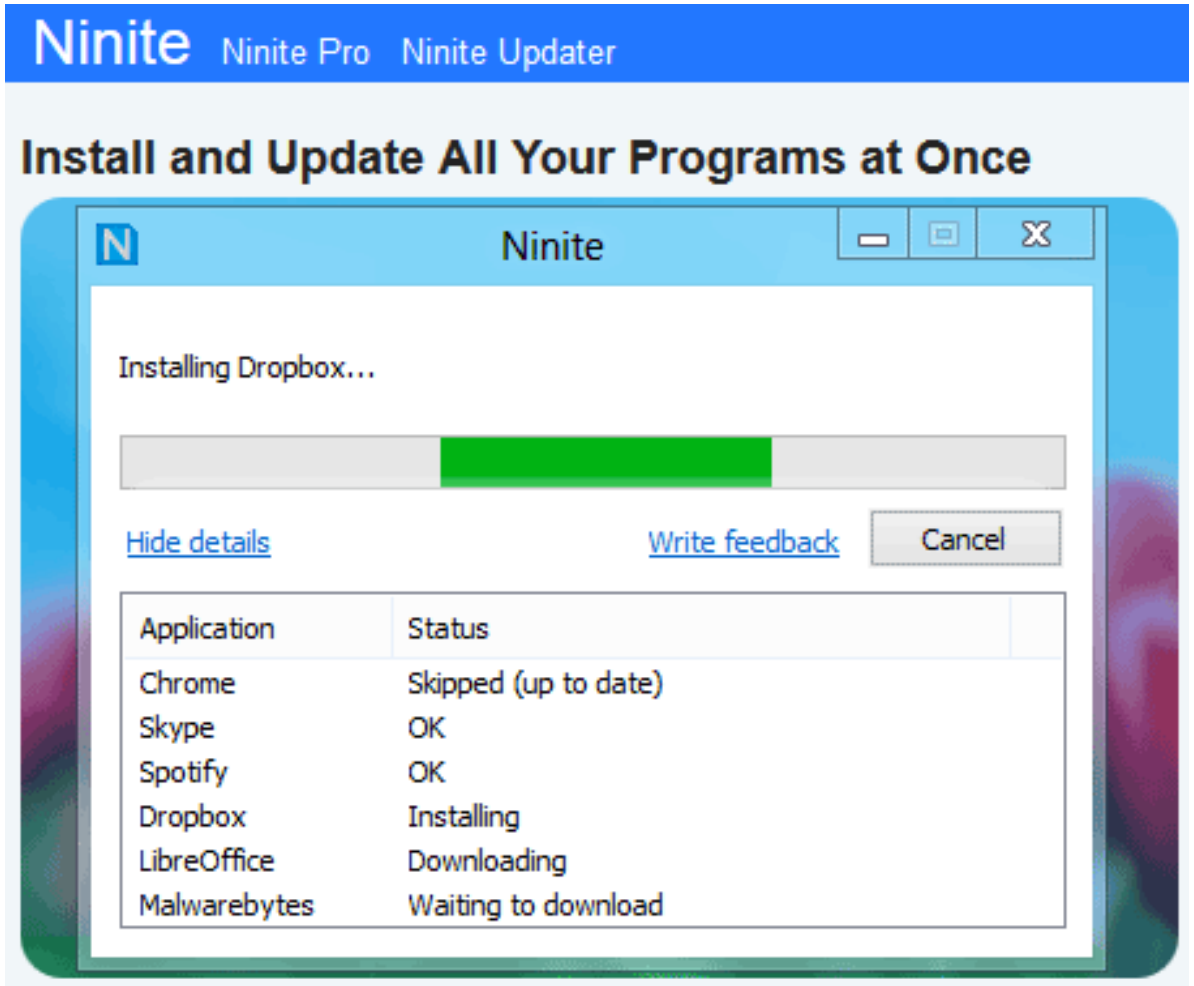
Run bash.exe

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



Patching & Updating

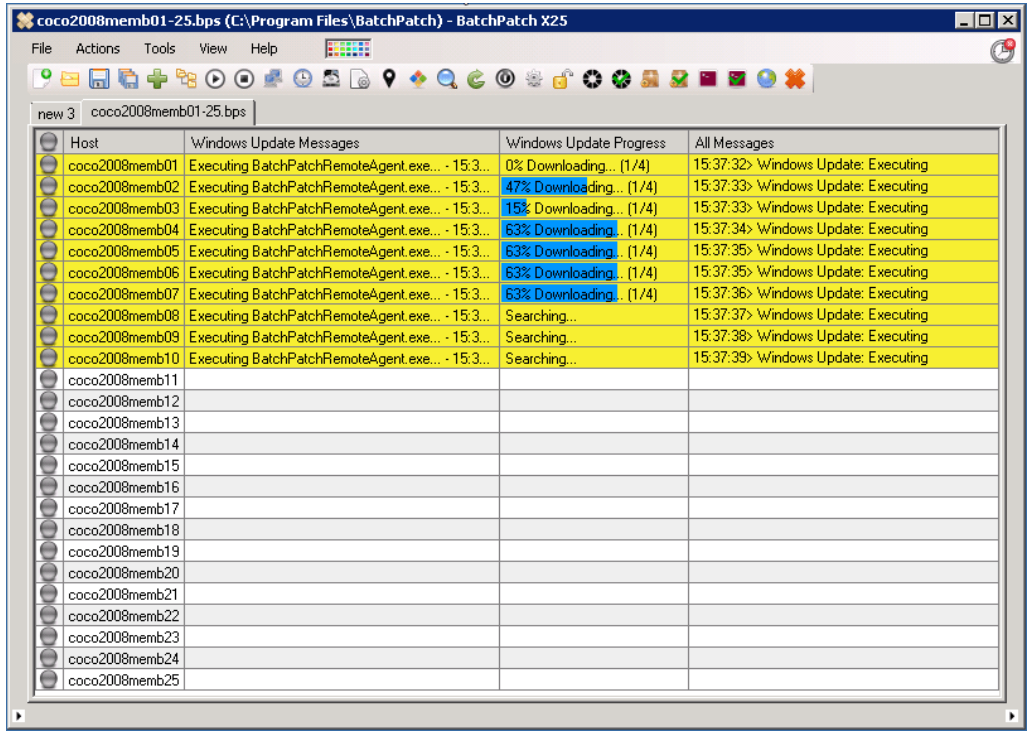
Ninite
(https://ninite.com/)



Patching & Updating

BatchPatch

https://batchpatch.com/



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/

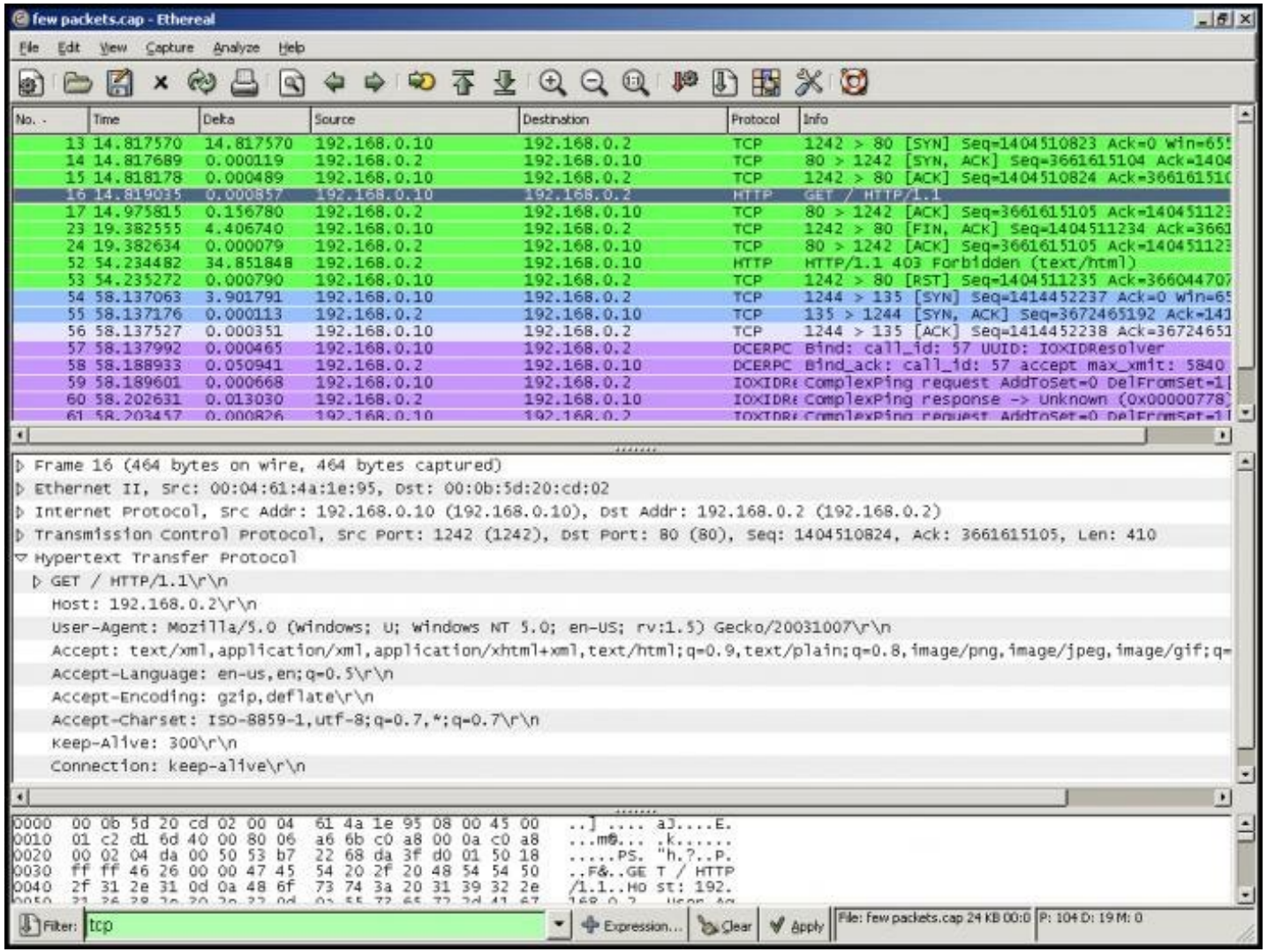
Chocolatey
Software Management Automated

Network Evaluation / Troubleshooting

WIRESHARK

Introduction video

TcpDump



RWX Security Solutions

RSAConference2019

Linux Distros

https://distrowatch.com/

The LiveCD List

Home :: About

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.

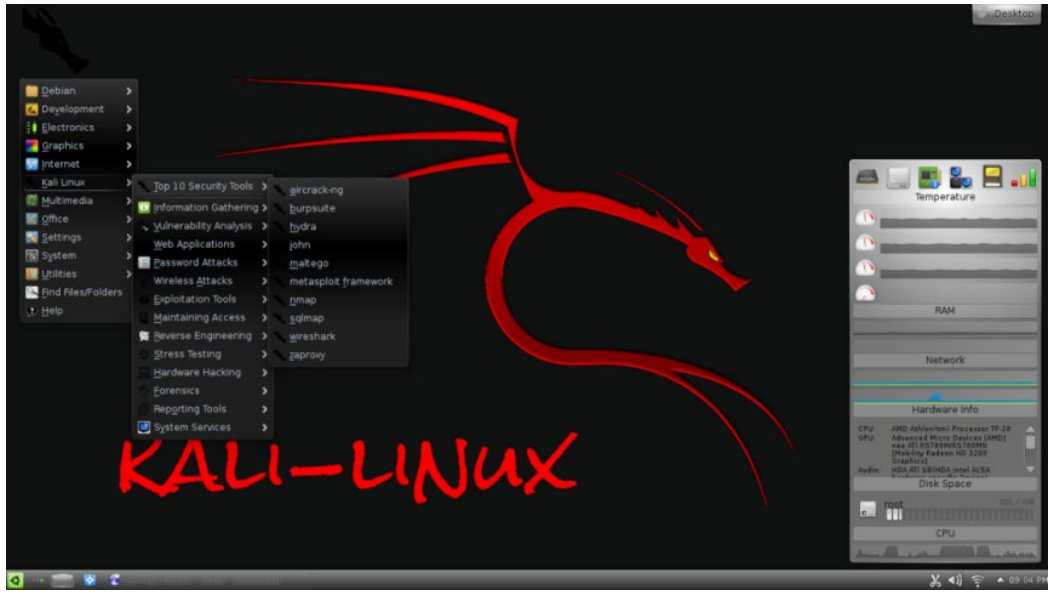
Name	Min Size	Max Size	Purpose	Last Release
Tails	1153	1153	[Secure Desktop]	2017-07
Kali Linux	1093	2934	[OS Installation] [Security]	2016-08
Arch Linux	742	742	[OS Installation] [Rescue]	2016-08
SystemRescueCD	83	466	[Rescue] [System Administration]	2016-07
Debian	417	1463	[Desktop] [OS Installation] [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

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

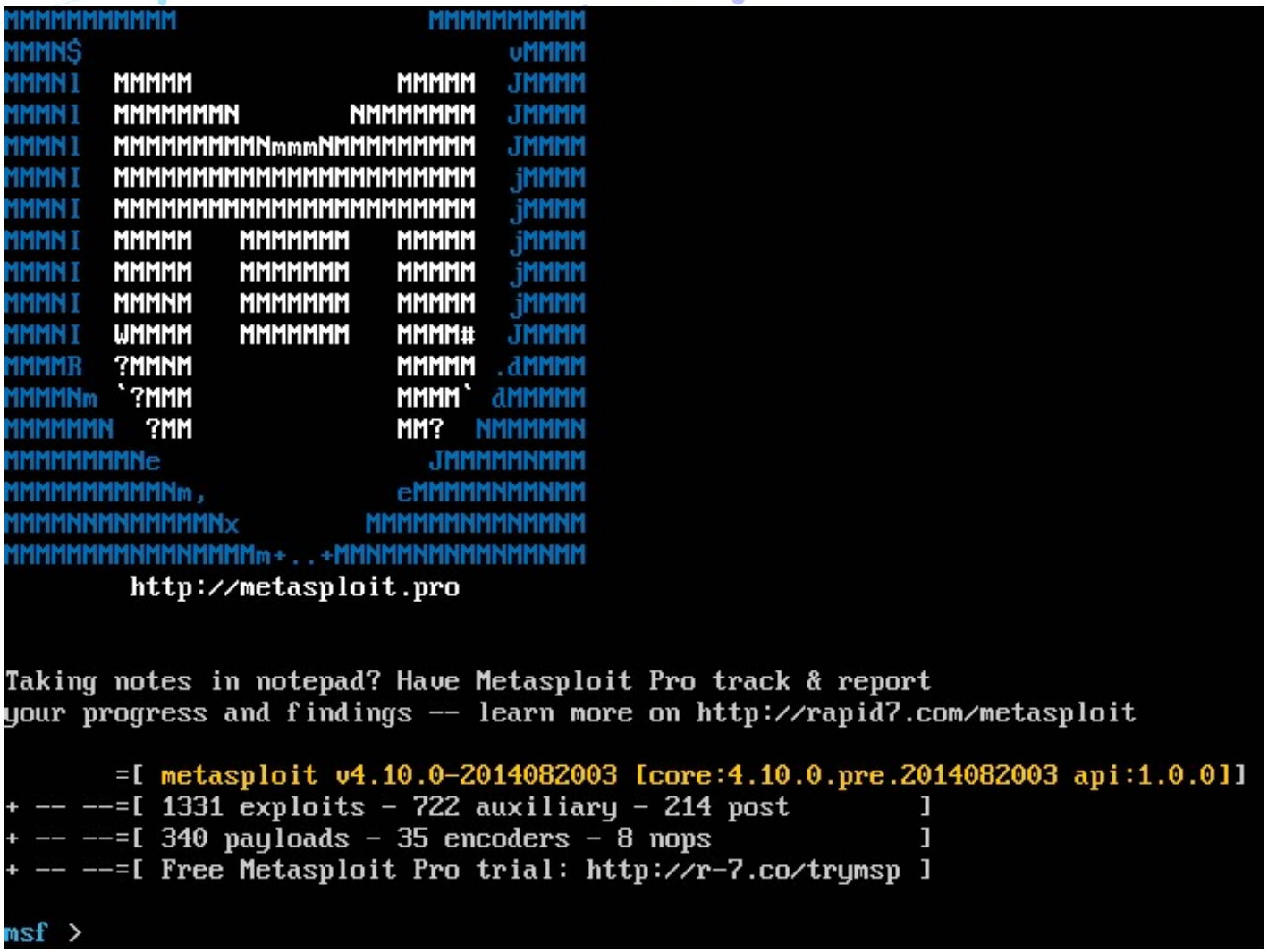
- Tails
  https://tails.boum.org/

Tails
theamnesicincognitolivesystem

Pen Testing Framework

metasploit®

https://www.metasploit.com/



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

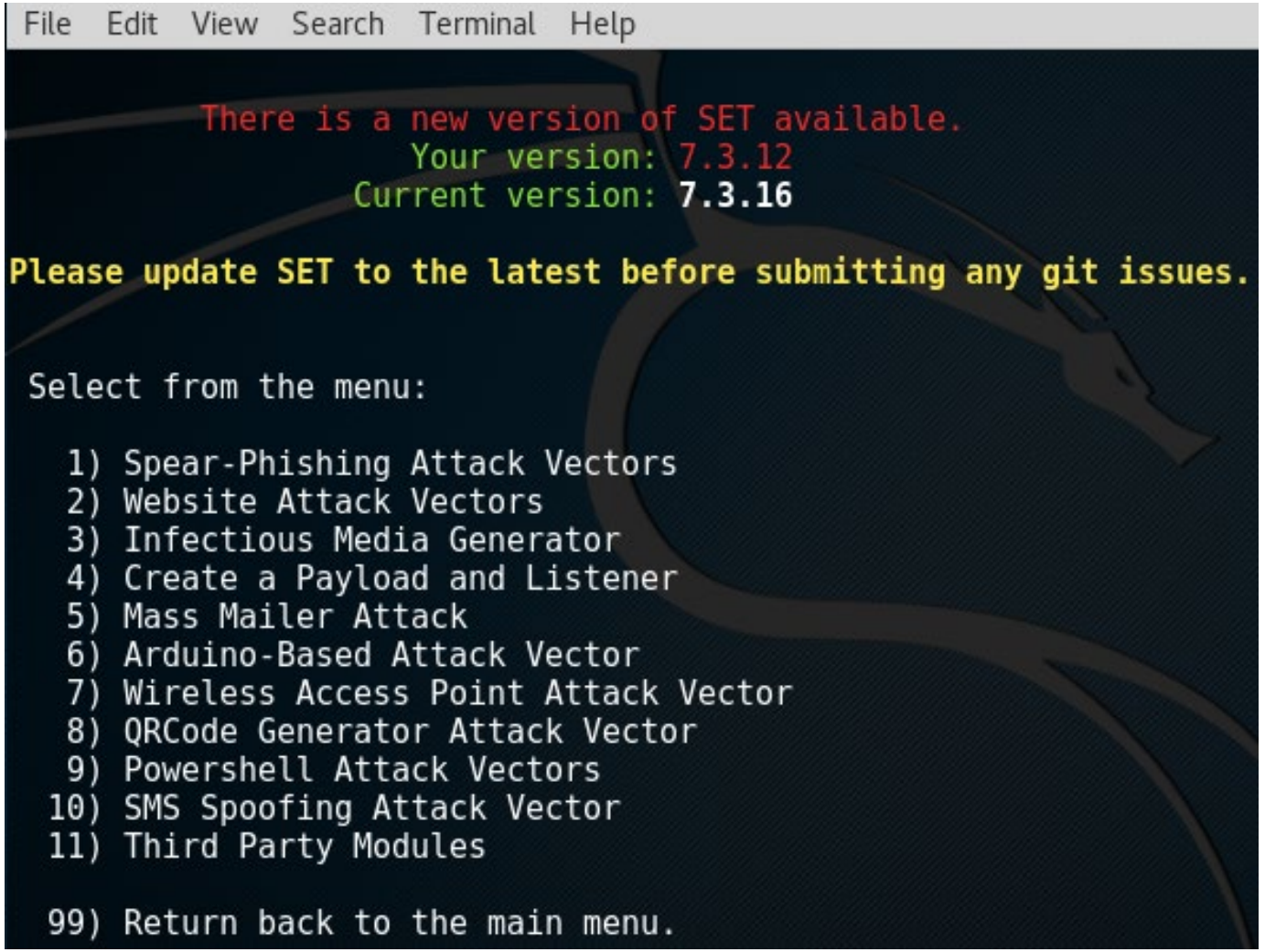
RWX Security Solutions

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

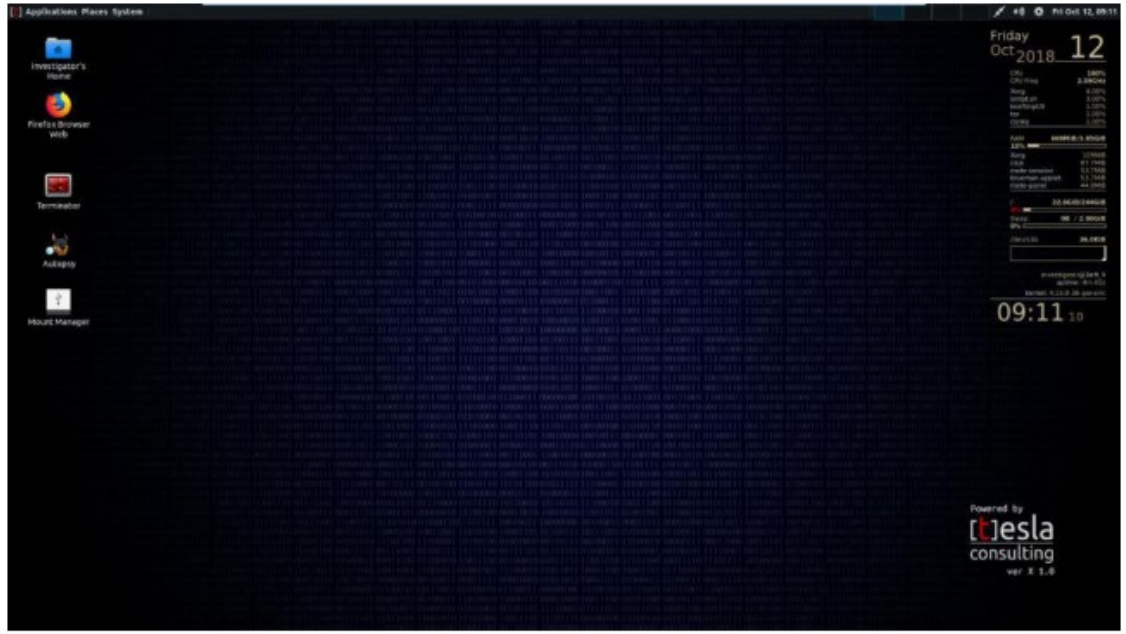
- Vega

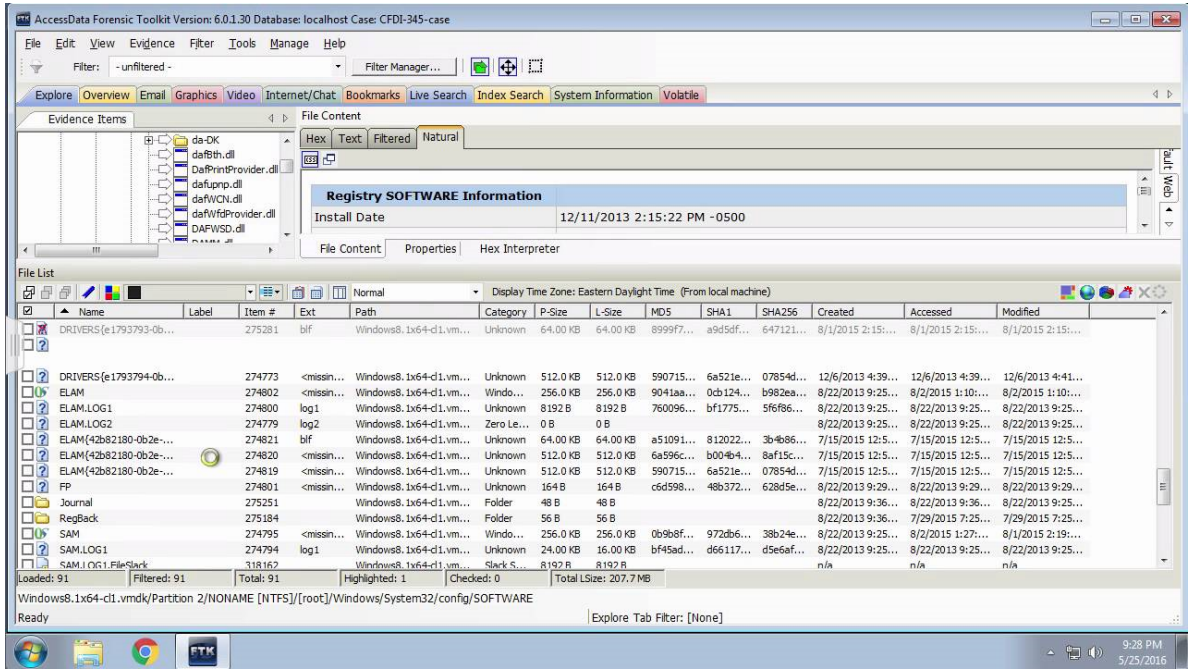
- Netsparker

- GuardiCore Infection Monkey

Digital Forensics

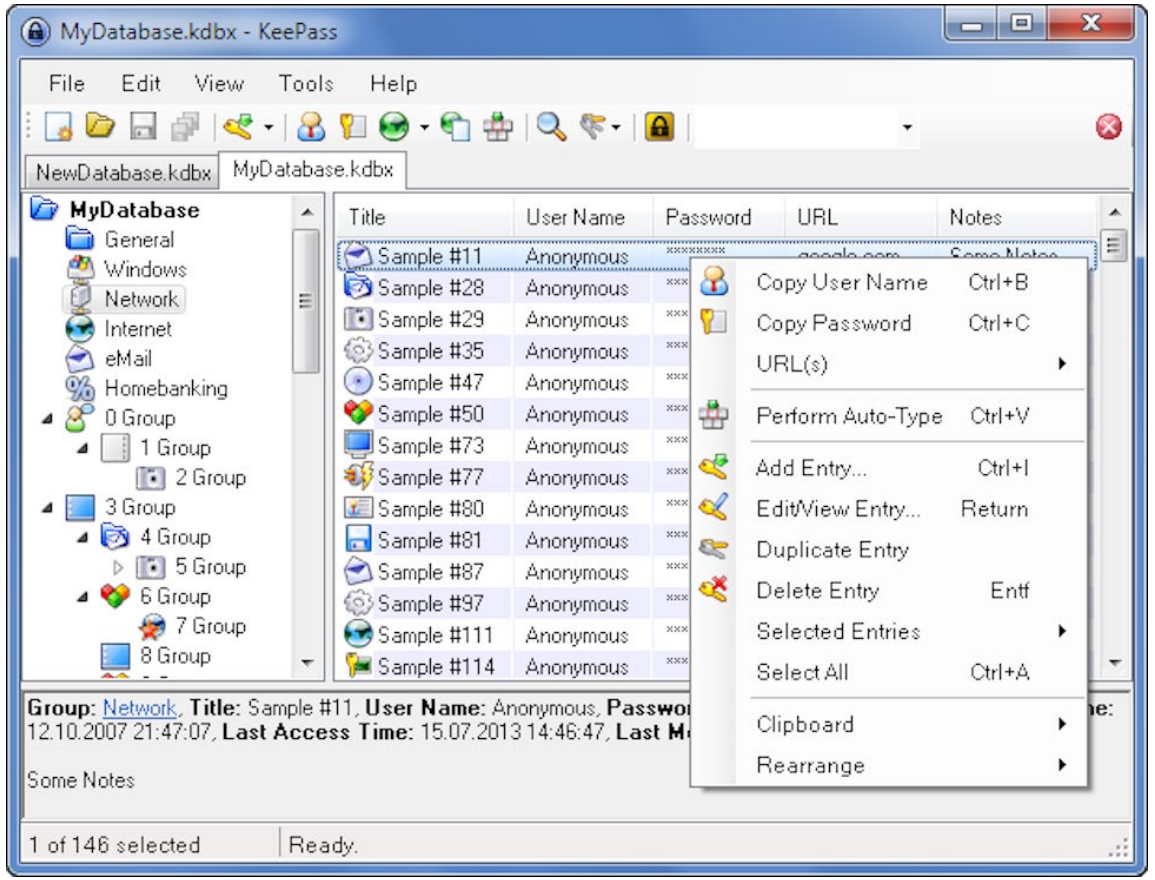
- DEFT X
- OSForensics
- FTK
- WinHex





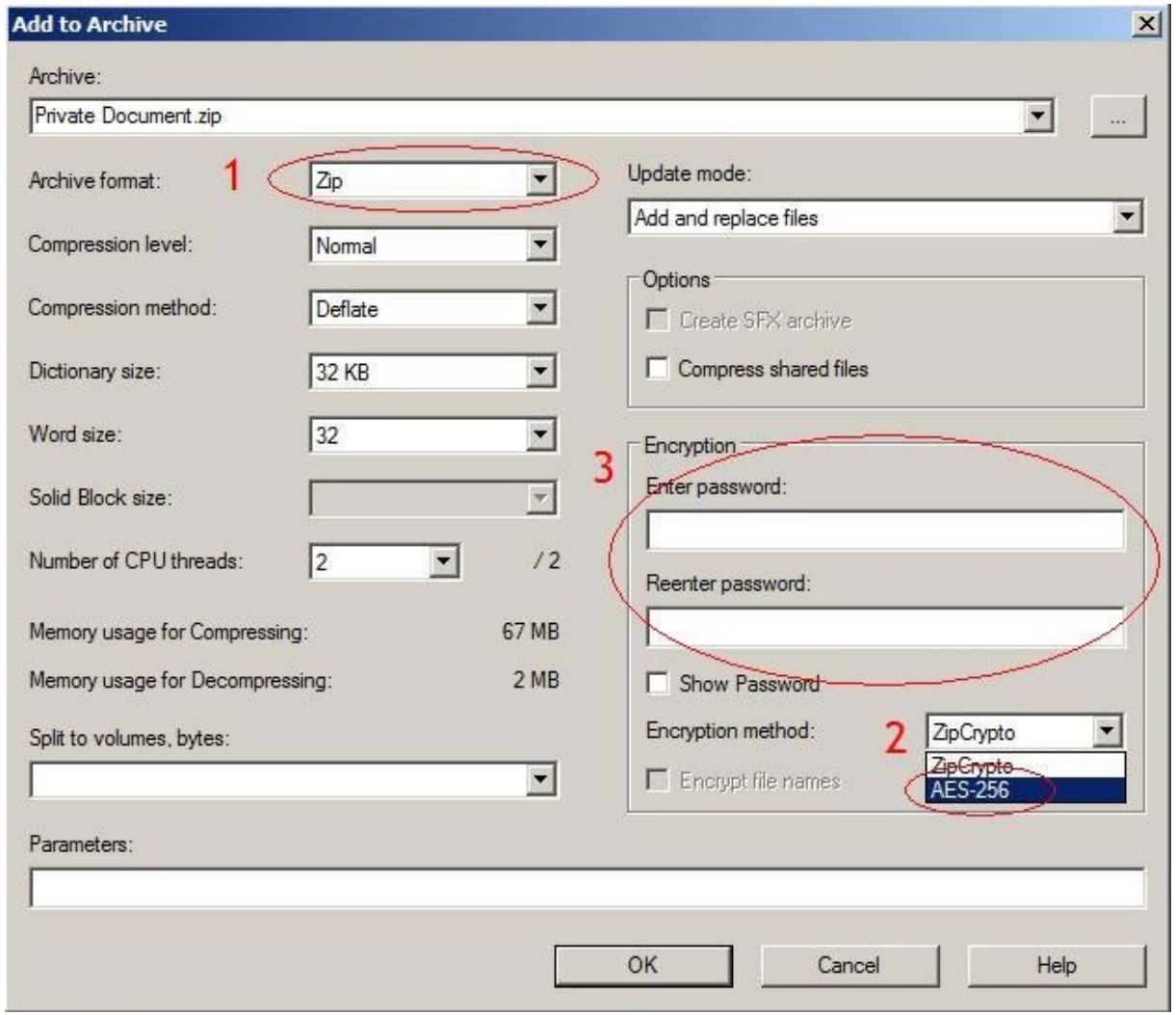
Personal Security – Password Vaults

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



Personal Security – Encryption

- 7-Zip
- AES Crypt
- Veracrypt



RWX Security Solutions

Security Awareness

StaySafeOnline
Powered by: National Cyber Security Alliance

National Cybersecurity Awareness Month

CyberAware

https://staysafeonline.org/ncsam/

Security Books

CYBERSECURITY CANON

paloalto

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?

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

RSAConference2019

Cybersecurity Tips, Tools, & Techniques

Ron Woerner, CISSP, CISM

ron.woerner @ rwxsecurity.com

Twitter: @ronw123

RWX Security Solutions