

RSA®Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: TECH-08, Tuesday, Feb 25, 11AM

Cybersecurity Tips, Tools and Techniques Updated for 2020



Ron Woerner, CISSP, CISM

Professor, Bellevue University

President, Cyber-AAA, LLC

@ronw123

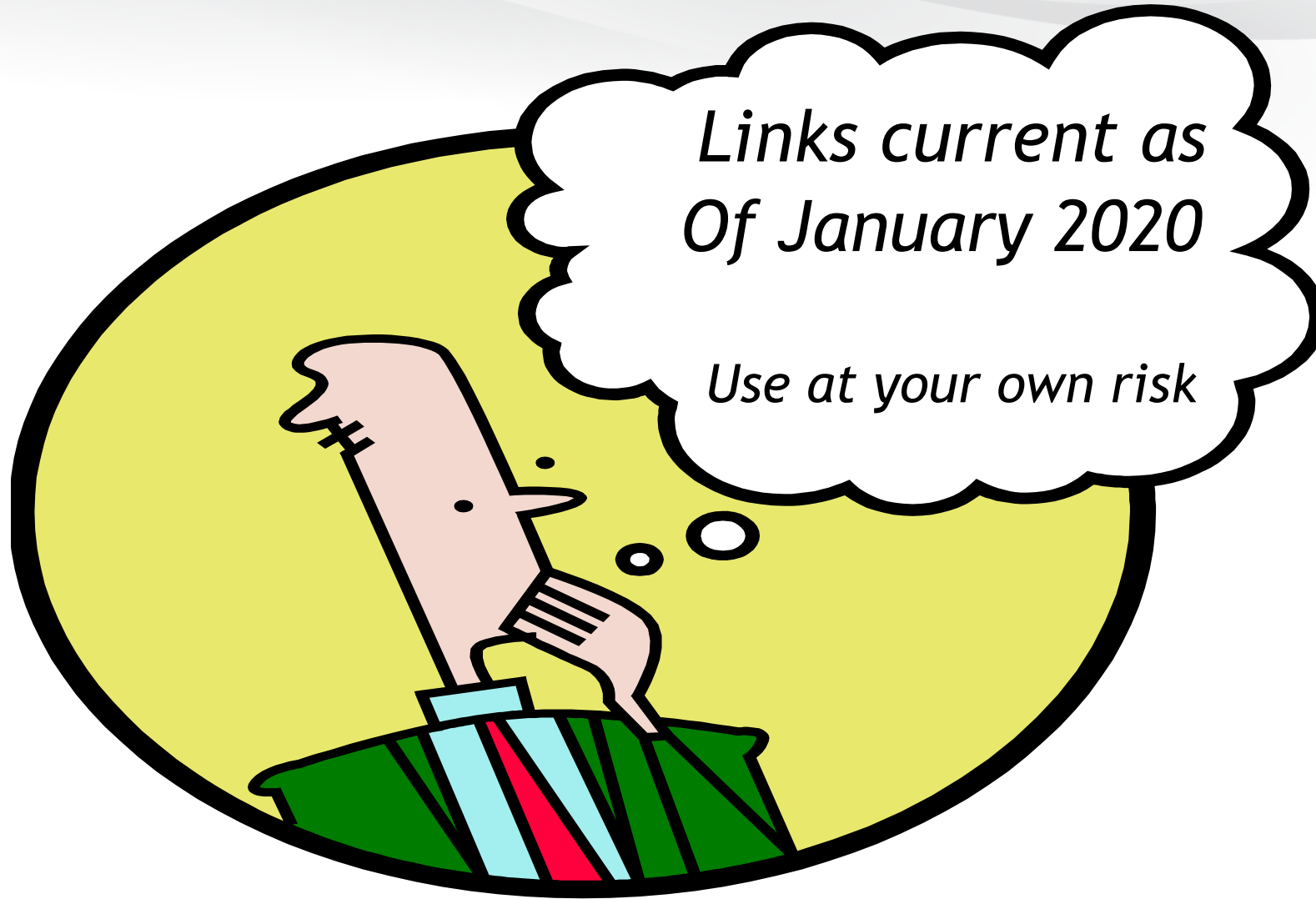


#RSAC



WhoAml – Ron Woerner, CISSP, CISM

- Cyber-AAA, LLC, President / Chief Trusted Advisor / Evangelist
- Bellevue University, Cybersecurity Professor
- 20+ years experience in IT / Security
- TEDx Speaker, [Hackers Wanted](#)
- LinkedIn Learning Instructor
- 18th time speaking at RSAC - 3rd time for this topic



RSA®Conference2020

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

How to be really dangerous...

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

Cool technologies

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

“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!

First Some Basics



First Some Basics



- Free is not always “free”
- Do your homework
- Test, test, test

If you only remember 1 slide...

StaySafeOnline

Powered by: National Cyber Security Alliance

<https://staysafeonline.org/>



STOP | THINK | CONNECT™

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



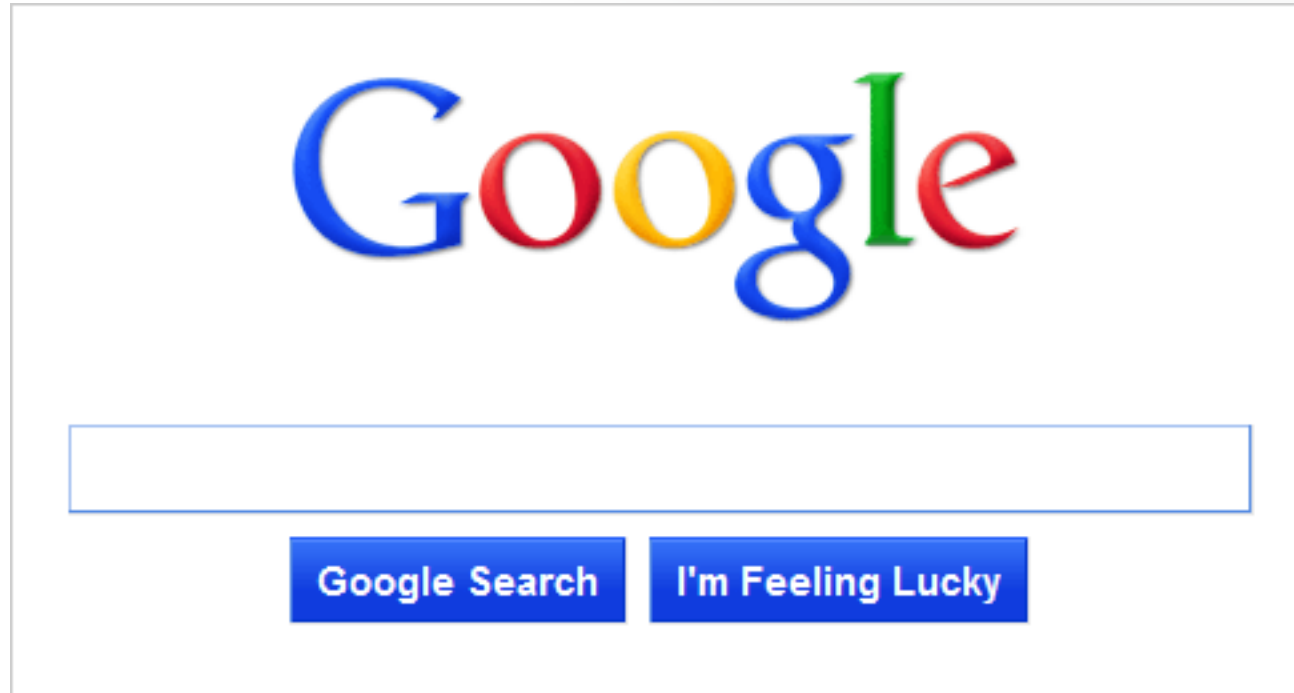
<https://www.dhs.gov/see-something-say-something>



CISA
CYBER+INFRASTRUCTURE

<https://www.cisa.gov/>

#1 Technical Hacking Tool



https://www.google.com/advanced_search

lmgtfy <https://lmgtfy.com/>

Lists of Tools, Tips & Tricks

- [SecTools](#)
- [Peerlyst List of Security Tools](#)
- [OlderGeeks](#)
- [HowToGeek.com](#), [Geek School](#)

Lists of Hacker Tools

- KitPloit – Top 20 Most Popular Hacking Tools in 2019:
<https://www.kitploit.com/2019/12/top-20-most-popular-hacking-tools-in.html>
- GBHackers – A Complete Penetration Testing & Hacking Tools List: <https://gbhackers.com/hacking-tools-list/>
- Art of Hacking: <https://github.com/The-Art-of-Hacking/h4cker>
New Tools: https://github.com/The-Art-of-Hacking/h4cker/blob/master/new_tools.md

Lists of Hacker Tools



- The Frugal Hacker, Hacking on a Shoestring Budget:
<https://www.peerlyst.com/posts/the-frugal-hacker-hacking-on-a-shoestring-budget-ian-barwise>
- Steve Hollands, My go-to list as a security professional:
<https://www.peerlyst.com/posts/my-go-to-list-as-a-security-professional-steve-hollands>
- Chiheb Chebbi, TOP 20 Tools every Security Professional should have in 2020: <https://www.peerlyst.com/posts/top-20-tools-every-security-professional-should-have-in-2020-chiheb-chebbi>
- Chiheb Chebbi, TOP 20 tools every Blue Teamer should have in 2020: <https://www.peerlyst.com/posts/top-20-tools-every-blue-teamer-should-have-in-2020-chiheb-chebbi>

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://cheatsheetseries.owasp.org/>
GitHub repository - <https://github.com/OWASP/CheatSheetSeries>

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

- DoD Cyber Exchange (Public) - <https://public.cyber.mil/>

DISA IASE Security Technical Implementation Guides (STIGs) - <https://public.cyber.mil/stigs/>

SMB & School Cybersecurity Resources

A curated list of recent information and resources to help U.S. public K-12 school leaders and policymakers navigate cybersecurity and related issues.

<https://k12cybersecure.com/resources/>

General Cybersecurity Resources

- Stamatiou, Paul. (Oct 2019). [Getting Started with Security Keys](#).
- Shelton, Martin. (Oct 2019) [Current Digital Security Resources](#).
- Alberti, Tobia (Oct 2019). [Precisely Private](#).
- [The Digital First Aid Kit](#) by the RaReNet (Rapid Response Network) and CiviCERT.
- [Online Harassment Resources](#) by HeartMob.
- Motherboard. (Nov 2018). [How to Tell if Your Account Has Been Hacked](#)
- Motherboard. (Nov 2018). [The Motherboard Guide to Not Getting Hacked](#)
- Purdy, Kevin. (April 2018). ["The Best Internet Security: Layers of Protection, and Good Habits."](#) Wirecutter.
- Pagano, Floriana & Cheng, Sage (Apr 2018). [A First Look at Digital Security](#). Access Now.
- [Security Planner](#) by the Citizen Lab
- [Firefox Monitor/have i been pwned?](#) (check to see if your accounts have been compromised in a data breach)
- Consumer Reports. (February 2017). [66 Ways to Protect Your Privacy Right Now](#).
- [Surveillance Self-Defense](#) and [Security Education Companion](#), both projects of the Electronic Frontier Foundation
- [Digital Security Training Resources for Security Trainers](#), Winter 2017 Edition
- Quintin, Cooper and Okuda, Soraya. (January 2018). [How to Assess a Vendor's Data Security](#). Electronic Frontier Foundation.
- [privacytools.io](#) – encryption against global mass surveillance
- United States Computer Emergency Readiness Team (US-CERT) [Cybersecurity Tips](#).

Security Awareness Training

- DoD Cyber Exchange – <https://public.cyber.mil/cyber-training/training-catalog/>
- TreeTop Cybersecurity Awareness – <https://www.treetopsecurity.com/slides>
- Wizer – <https://wizer-training.com/>
- CyberPatriot / CyberGenerations – <https://www.uscyberpatriot.org/cybergenerations/cybergenerations-overview>
- SANS – <https://www.sans.org/security-awareness-training/resources>

Finding Products



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

MITRE ATT&CK™ Enterprise Framework

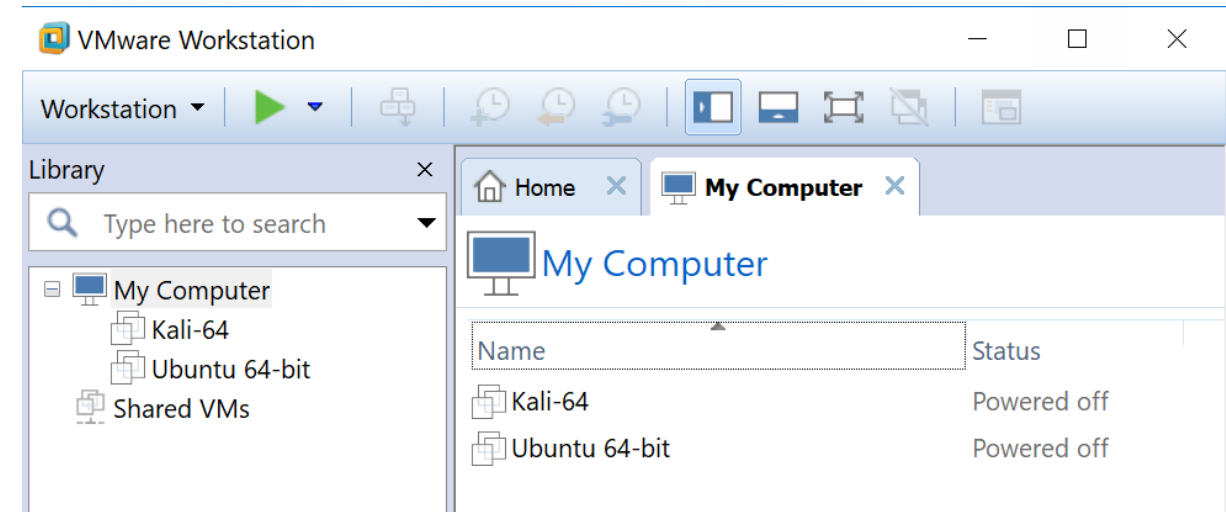
<https://attack.mitre.org/>

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order	Password Filter DLL	System Information	Windows Admin		Remote Access Tools		

attack.mitre.org/tactics/TA0005/

Personal Labs – Virtual Environments

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



LifeHacker – How to Set Up a Virtual Machine for Free

Linux Distro

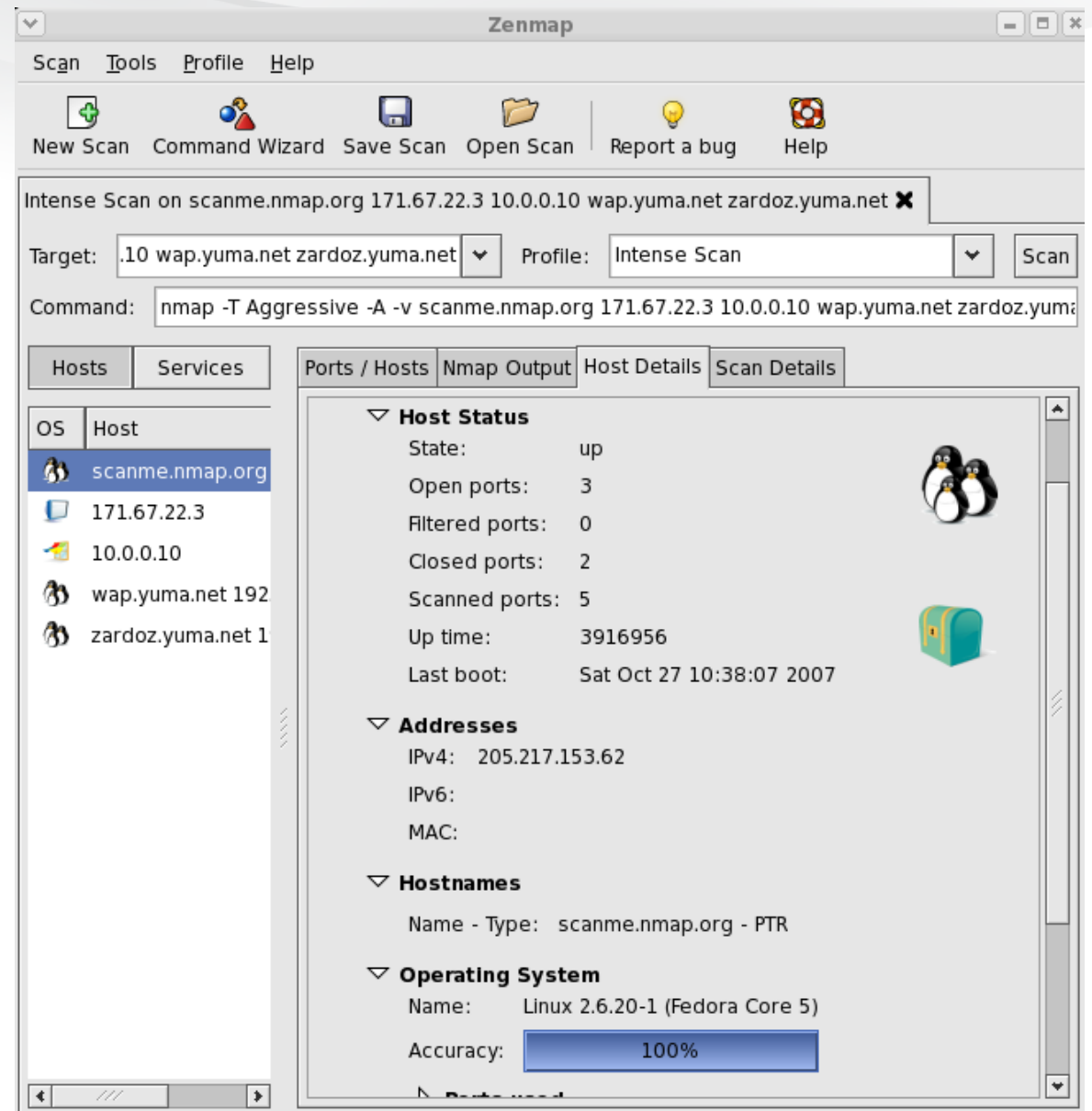
Linux Distros

- DistroWatch – <https://distrowatch.com/>
- Foss – <https://itsfoss.com/best-linux-distributions/>
- DigitalTrends – <https://www.digitaltrends.com/computing/best-linux-distros/>



Network Mapping

Nmap / ZenMap



Network Mapping

Fing

(iOS & Android)

The screenshot shows the Fing app interface on a mobile device. At the top, it says 'Overlook Wi-Fi' and 'Wireless with Internet'. Below this is a list of discovered devices, each with an icon, IP address, device name, manufacturer, and MAC address. The devices include a Router, Desktop, Printer, TV, iPhone, Laptop, iPod, iPad, Media Player, Console, PC Julius, IP Phone Home, Laptop Portia, Fax&Copy, Mobile Flavius, Webcam, PC Augustus, Laptop Cicero, and Laptop Calpurnia.

Icon	IP Address	Device Name	Manufacturer	MAC Address
Router	192.168.0.1	Router	Netgear	00:18:4D:CC:8B:F5
Desktop	192.168.0.5	Desktop	Apple	00:17:F2:97:A4:5A
Printer	192.168.0.12	Printer	HP	00:0E:7F:96:D3:27
TV	192.168.0.13	TV	Samsung	00:12:FB:5C:93:C1
iPhone	192.168.0.14	iPhone	Apple	04:1E:64:45:4A:53
Laptop	192.168.0.15	Laptop	Sony	00:13:A9:5C:93:C2
iPod	192.168.0.20	iPod	Apple	04:1E:64:45:4A:54
iPad	192.168.0.22	iPad	Apple	04:1E:64:45:4A:55
Media Player	192.168.0.23	Media Player	THX	00:12:FA:6C:93:C1
Console	192.168.0.40	Console	Sony	00:13:A9:5C:93:C9
PC Julius	192.168.0.101	PC Julius	Dell	00:12:3F:00:AF:01
IP Phone Home	192.168.0.102	IP Phone Home	Dell	00:12:3F:00:AF:02
Laptop Portia	192.168.0.103	Laptop Portia	HP	00:13:21:DD:FA:01
Fax&Copy	192.168.0.104	Fax&Copy	HP	00:13:21:DD:FA:02
Mobile Flavius	192.168.0.106	Mobile Flavius	Apple	04:1E:64:45:4A:59
Webcam	192.168.0.113	Webcam	Dell	00:12:3F:00:AF:03
PC Augustus	192.168.0.114	PC Augustus	Dell	00:12:3F:00:AF:04
Laptop Cicero	192.168.0.120	Laptop Cicero	HP	00:13:21:DD:FA:04
Laptop Calpurnia	192.168.0.121	Laptop Calpurnia	HP	00:13:21:DD:FA:05

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/>

VPNs

Algo VPN with DigitalOcean

1. Create an account on a cloud hosting provider like [DigitalOcean](#)
2. [Download](#) Algo VPN on your local computer, unzip it
3. Install the dependencies with the [command lines](#) on this page
4. Run the installation wizard
5. Double click on the configuration profiles in the configs directory

Commercial

- [Hotspot Shield](#) 
- [Tunnel Bear](#) 
- [Windscribe](#) 
- Deeper Network
<https://deeper.network/>

DNS Servers

- Google Public DNS – 8.8.8.8 and 8.8.4.4
- Cloudflare – 1.1.1.1 and 1.0.0.1
- Quad9 – 9.9.9.9 and 149.112.112.112
- OpenDNS (Cisco) – 208.67.222.222 and 208.67.220.220
- Verisign – 64.6.64.6 and 64.6.65.6

Windows Administration






SysInternals Suite

- Autoruns
- Process Explorer
- Process Monitor

Video:

Mark Russinovich,
Malware Hunting

Sysinternals Suite

06/27/2019 • 2 minutes to read •      +1

By Mark Russinovich

Updated: September 20, 2019

[Download Sysinternals Suite](#) (25.9 MB) [Download Sysinternals Suite for Nano Server](#) (5.1 MB)
[Download Sysinternals Suite for ARM64](#) (164 KB)

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](#), [VMMMap](#), [VolumeID](#), [Whols](#), [WinObj](#), [ZoomIt](#)

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



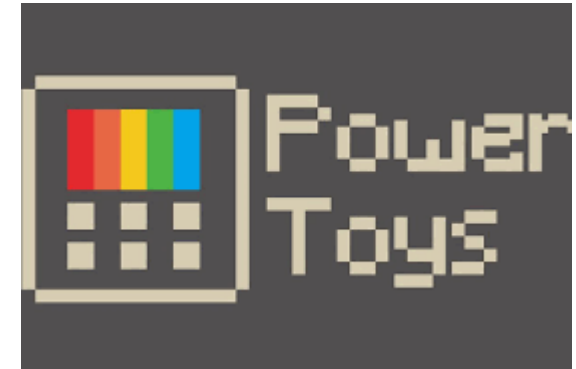
Windows Administration

PowerShell Core (v6)

- Overview – <https://docs.microsoft.com/en-us/powershell/scripting/overview>
- Installation - <https://docs.microsoft.com/en-us/powershell/scripting/install/installing-powershell>
- Github - <https://github.com/powershell/powershell>

PowerToys <https://github.com/microsoft/PowerToys>

- Windows Key Shortcut Guide
- FancyZones
- PowerRename



Linux on Windows

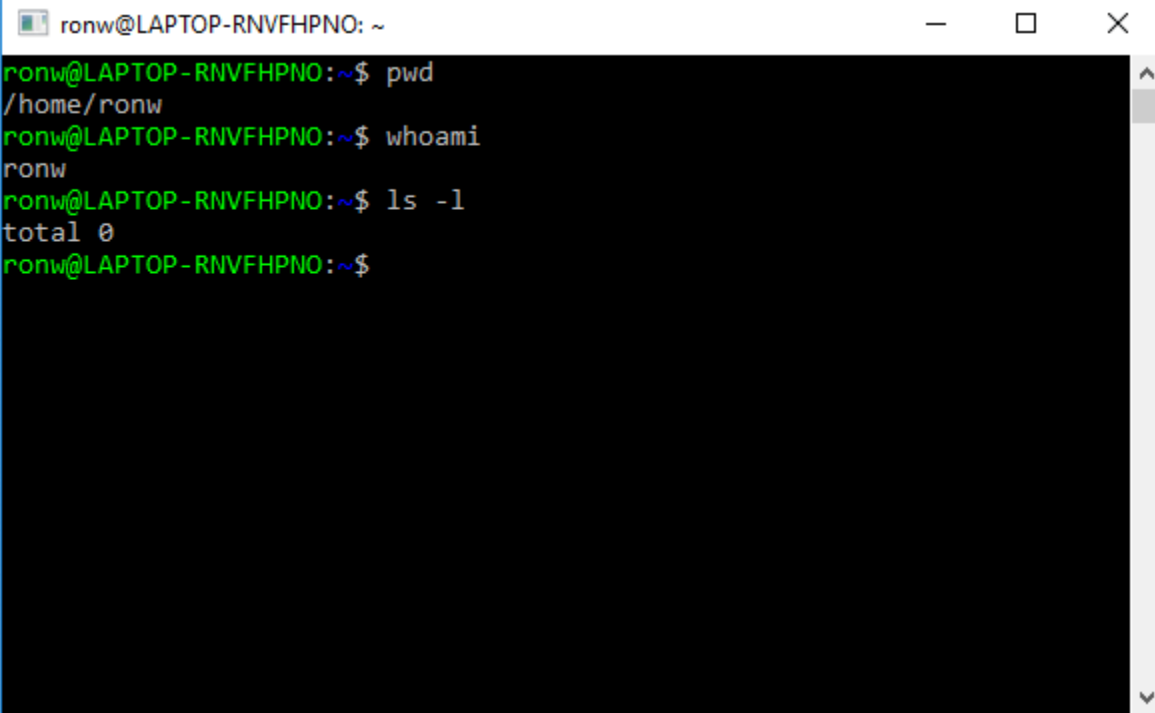
Windows Subsystem for Linux

<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/>



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

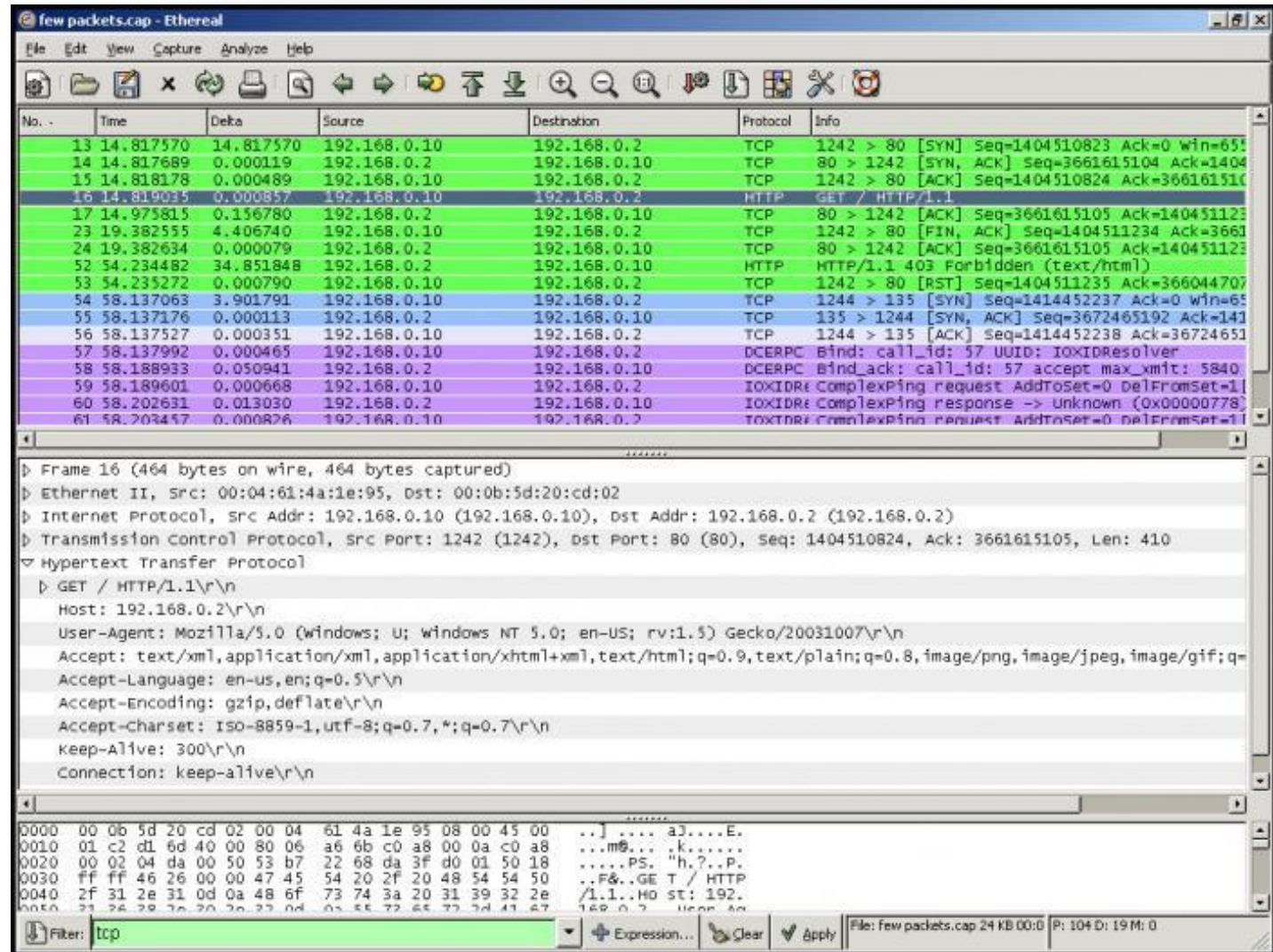

Network Evaluation / Troubleshooting



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

Introduction video

TcpDump



Network Security Monitoring

Zeek (fka Bro): <https://www.zeek.org/>

Why Choose Zeek? Zeek is a powerful network analysis framework that is much different from the typical IDS you may know. (Zeek is the new name for the long-established Bro system. Note that parts of the system retain the "Bro" name, and it also often appears in the documentation and distributions.)

Adaptable

Zeek's domain-specific scripting language enables site-specific monitoring policies.

Efficient

Zeek targets high-performance networks and is used operationally at a variety of large sites.

Flexible

Zeek is not restricted to any particular detection approach and does not rely on traditional signatures.

Forensics

Zeek comprehensively logs what it sees and provides a high-level archive of a network's activity.

In-depth Analysis

Zeek comes with analyzers for many protocols, enabling high-level semantic analysis at the application layer.

Highly Stateful

Zeek keeps extensive application-layer state about the network it monitors.

Open Interfaces

Zeek interfaces with other applications for real-time exchange of information.

Open Source

Zeek comes with a BSD license, allowing for free use with virtually no restrictions.

SELKS: <https://www.stamus-networks.com/open-source/>

A Live ISO dedicated to Suricata

SELKS is both Live and installable Network Security Management ISO based on Debian implementing and focusing on a complete and ready to use Suricata IDS/IPS ecosystem with its own graphic rule manager. From start to analysis of IDS/IPS and NSM events in 30 sec. The name comes from its major components:

- Suricata
- Elasticsearch
- Logstash
- Kibana
- Scirius Community Edition
- EveBox



HT to

 **BLACK HILLS** | Information Security

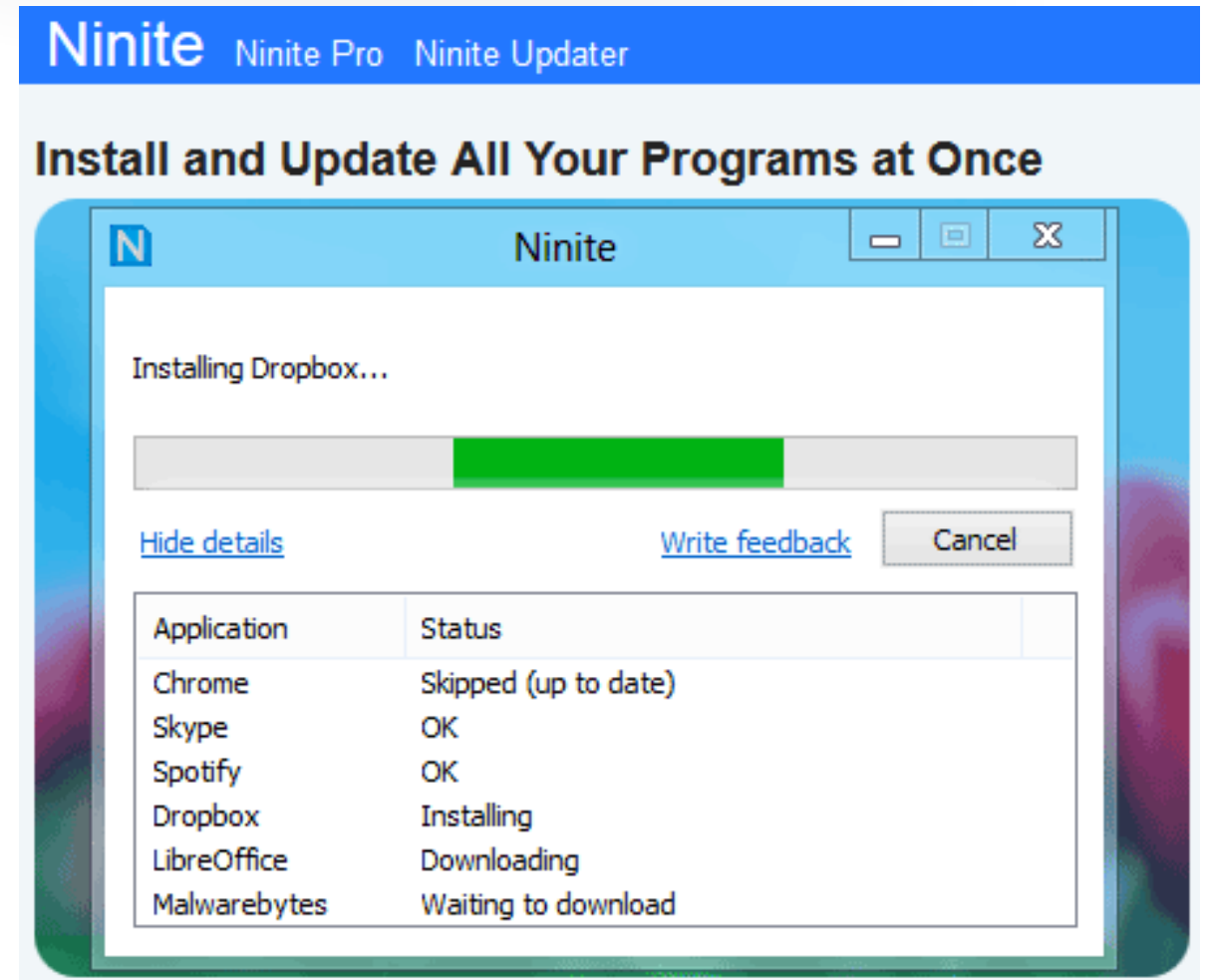
 **ACTIVE** | COUNTERMEASURES

<https://www.activecountermeasures.com/free-tools/>

Patching & Updating

Ninite

<https://ninite.com/>



Patching & Updating

SNIPE-IT

<https://snipeitapp.com/>



Chocolatey *

<https://chocolatey.org/>

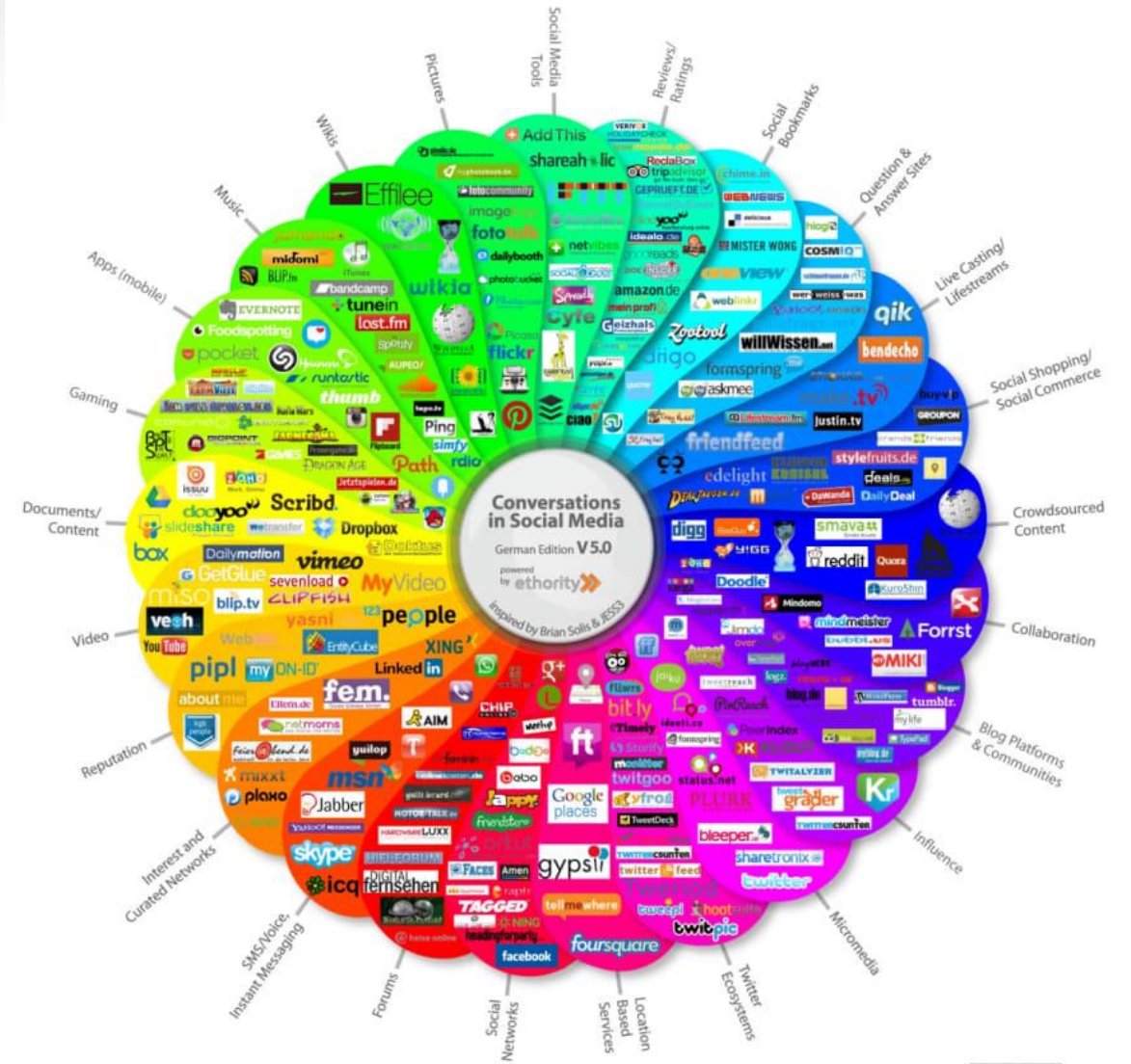


BatchPatch*

<https://batchpatch.com/>

Open Source Intelligence

OSInt Process and Tools –
<https://www.peerlyst.com/posts/open-source-intelligence-osint-reconnaissance-ian-barwise>



Conversations in Social Media – Version 5.0 – 09.2012 by ethority | <http://social-media-prisma.ethority.de> | <http://www.twitter.com/ethority> | Contact us for updates: prisma@ethority.de



Social Engineering - OSInt

- OSInt Framework – <https://osintframework.com/>
- Sublist3r, Enumerate website subdomains – <https://github.com/aboul3la/Sublist3r>
- Spiderfoot – <https://www.spiderfoot.net/>
- Maltego – <https://www.paterva.com/>
- Cree.py, Geolocation Information Aggregator – <http://www.geocreepy.com/>
- Peek You - www.peakyou.com

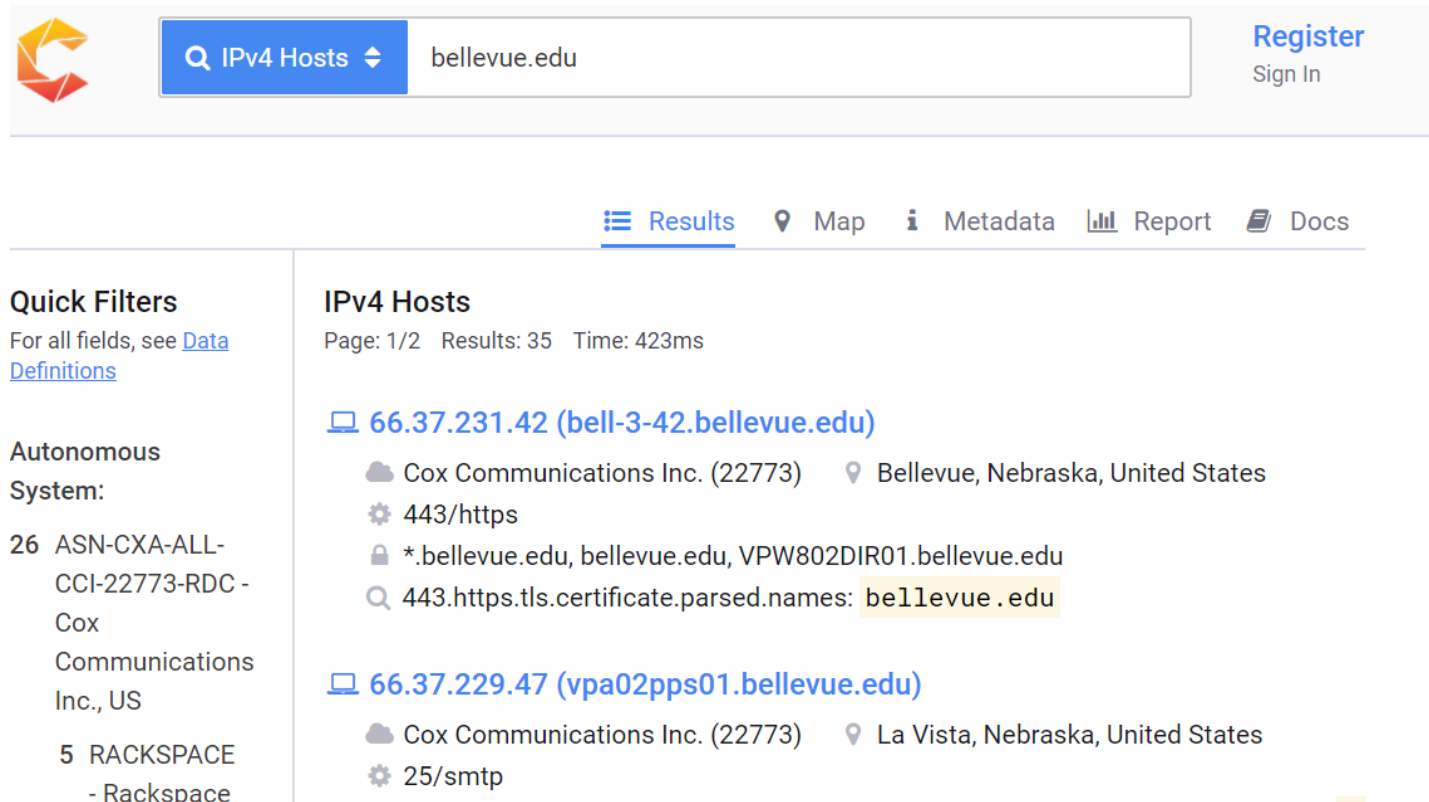
Social Engineering - OSInt

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

The screenshot shows the Shodan search engine interface. The browser address bar displays 'Secure | https://www.shodan.io/search?query=bellevue.edu'. The Shodan logo is visible, along with a search bar containing 'bellevue.edu' and a red search button. Navigation links include 'Explore', 'Developer Pricing', 'Enterprise Access', and 'Contact Us'. A 'New to Shodan?' link is also present. Below the navigation bar, there are tabs for 'Exploits' and 'Maps'. The search results section shows 'TOTAL RESULTS' as 4. Under 'TOP COUNTRIES', a world map highlights the United States with a red dot, and the text 'United States 4' is displayed. The main result is for IP address '66.37.229.47', which is associated with 'vpa02pps01.bellevue.edu' and 'Cox Communications'. It was added on '2018-04-30 06:30:21 GMT' and is located in the 'United States, Omaha'. A 'Details' link and a 'starttls' button are provided. To the right, an 'SSL Certificate' section shows it was issued by 'DigiCert SHA2 High Assurance Server CA' to '*.bellevue.edu' by 'DigiCert Inc'. The 'Supported SSL Versions' are listed as 'SSLv3, TLSv1, TLSv1.1, TLSv1.2'.

Social Engineering - OSInt

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 search bar with the text 'IPv4 Hosts' and a dropdown arrow, followed by the input 'bellevue.edu'. To the right of the search bar are links for 'Register' and 'Sign In'. Below the search bar, there is a navigation bar with tabs for 'Results', 'Map', 'Metadata', 'Report', and 'Docs'. The 'Results' tab is selected. On the left side, there is a 'Quick Filters' section with a link to 'Data Definitions'. Below this is an 'Autonomous System:' section listing two systems: '26 ASN-CXA-ALL-CCI-22773-RDC - Cox Communications Inc., US' and '5 RACKSPACE - Rackspace'. The main content area displays 'IPv4 Hosts' results. It shows 'Page: 1/2', 'Results: 35', and 'Time: 423ms'. The first result is '66.37.231.42 (bell-3-42.bellevue.edu)'. It lists the provider as 'Cox Communications Inc. (22773)' located in 'Bellevue, Nebraska, United States'. It also shows the port '443/https' and the certificate names '*.bellevue.edu, bellevue.edu, VPW802DIR01.bellevue.edu'. The second result is '66.37.229.47 (vpa02pps01.bellevue.edu)'. It lists the provider as 'Cox Communications Inc. (22773)' located in 'La Vista, Nebraska, United States' and shows the port '25/smtp'.

Quick Filters
For all fields, see [Data Definitions](#)

Autonomous System:

- 26 ASN-CXA-ALL-CCI-22773-RDC - Cox Communications Inc., US
- 5 RACKSPACE - Rackspace

IPv4 Hosts
Page: 1/2 Results: 35 Time: 423ms

[66.37.231.42 \(bell-3-42.bellevue.edu\)](#)
Cox Communications Inc. (22773) Bellevue, Nebraska, United States
443/https
*.bellevue.edu, bellevue.edu, VPW802DIR01.bellevue.edu
443.https.tls.certificate.parsed.names: bellevue.edu

[66.37.229.47 \(vpa02pps01.bellevue.edu\)](#)
Cox Communications Inc. (22773) La Vista, Nebraska, United States
25/smtp

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/>



Social Engineering Toolkit (SET)

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

```
Welcome to the Social-Engineer Toolkit (SET). The one
stop shop for all of your social-engineering needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

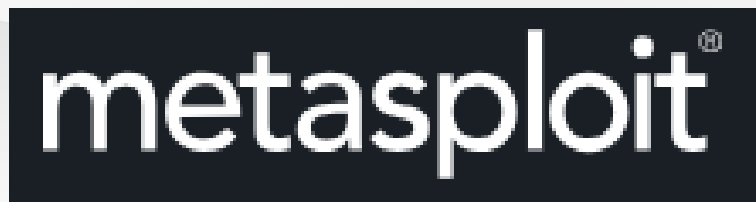
Select from the menu:

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) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules

99) Return back to the main menu.

SET> 2
```


Pen Testing Framework



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

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

<https://blog.tryhackme.com/metasploit/>

A screenshot of a terminal window titled "root@kali: ~". The terminal shows the command "msfconsole" being executed, which starts the Metasploit framework. It displays a ASCII art logo for Metasploit, followed by version information "metasploit v4.16.57-dev" and a list of available exploits, auxiliary modules, payloads, encoders, and nops. It also mentions a free trial for Metasploit Pro with a URL. The prompt "msf >" is visible at the bottom.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfconsole  
# cowsay++  
< metasploit >  
-----  
      \  ('oo')_____) \  
       (  )_____)  \  
        ||--||  *  
  
      =[ metasploit v4.16.57-dev ]  
+ -- --=[ 1767 exploits - 1007 auxiliary - 307 post ]  
+ -- --=[ 537 payloads - 41 encoders - 10 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > 
```

Security Testing

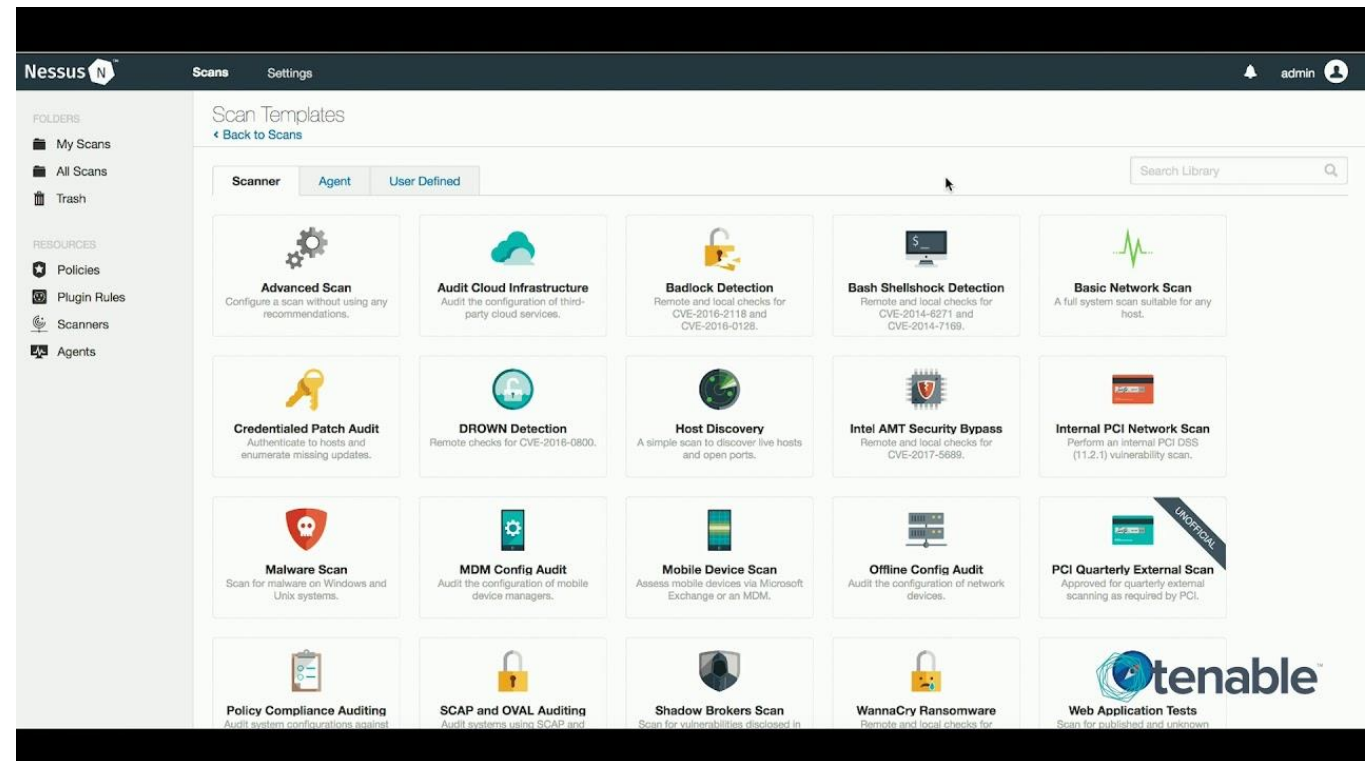


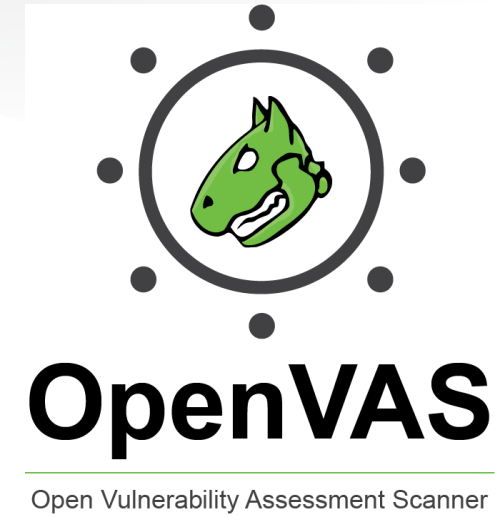
Personal use

Scan up to 16 IPs

<https://www.tenable.com/products/nessus/nessus-essentials>

Note: Registration required





<http://www.openvas.org/index.html>

Security Testing

- OWASP Zed Attack Proxy (ZAP)
- Portswigger Burp Suite*
- Vega
- Netsparker*
- GuardiCore Infection Monkey



*Trial versions

Digital Forensics / Incident Response

- SANS SIFT
- The Sleuth Kit (+Autopsy)
- Digital Forensics Framework (4 years old)
- CAINE (Computer Aided INvestigative Environment)
- Access Data FTK
- TheHive

Malware Analysis

- Zeltser's List – <https://zeltser.com/automated-malware-analysis/>
- Volatility – <https://github.com/volatilityfoundation/volatility>
- Cuckoo Sandbox – <https://cuckoosandbox.org/>

AntiVirus

VirusTotal – <https://www.virustotal.com/>

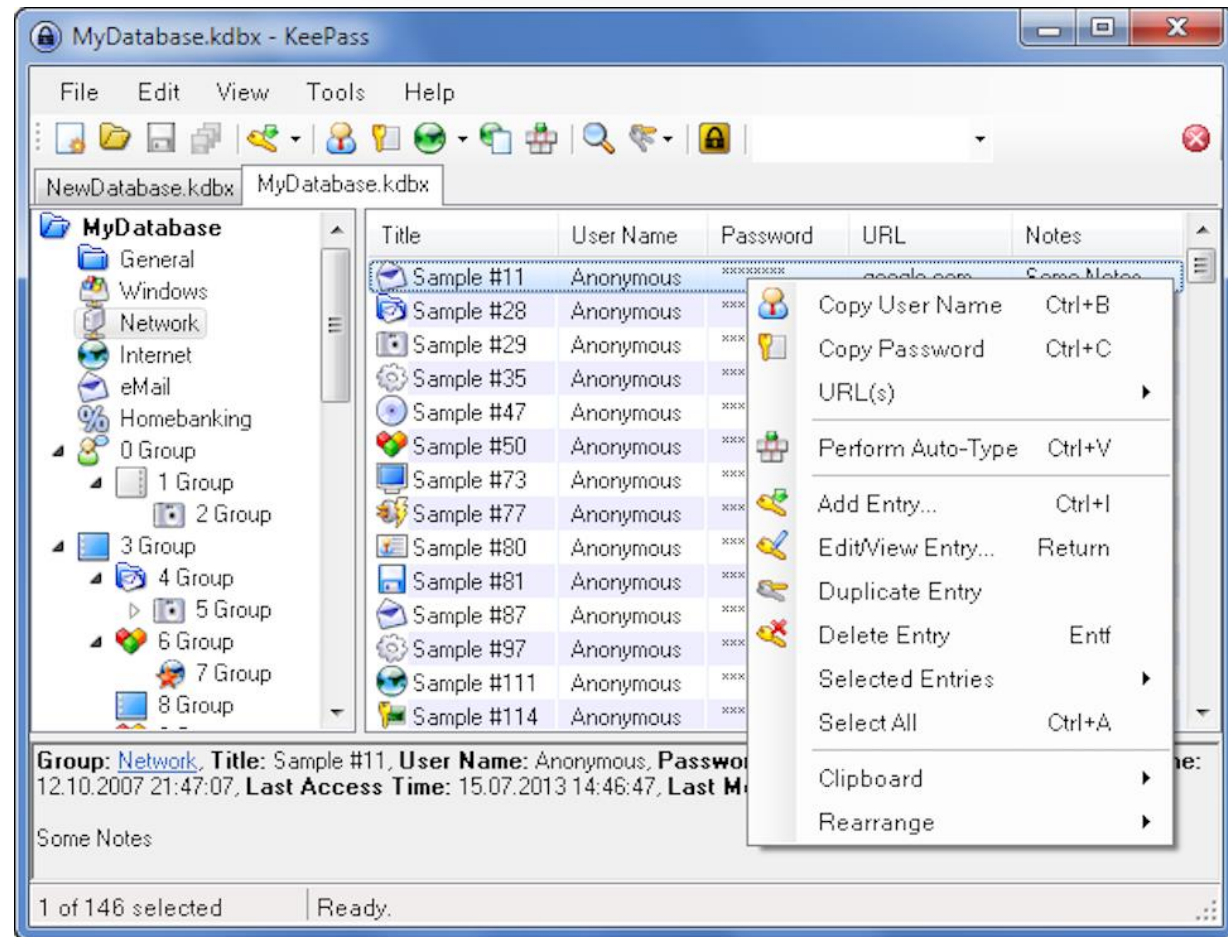
Free AV Products*

- *The Best Free Antivirus Protection for 2020*, PC Mag
<https://www.pcmag.com/roundup/267984/the-best-free-antivirus-protection>
- *Best antivirus software 2020: Free and paid*, Tom's Guide
<https://www.tomsguide.com/us/best-free-antivirus,review-6003.html>

*Free for personal use (not business)

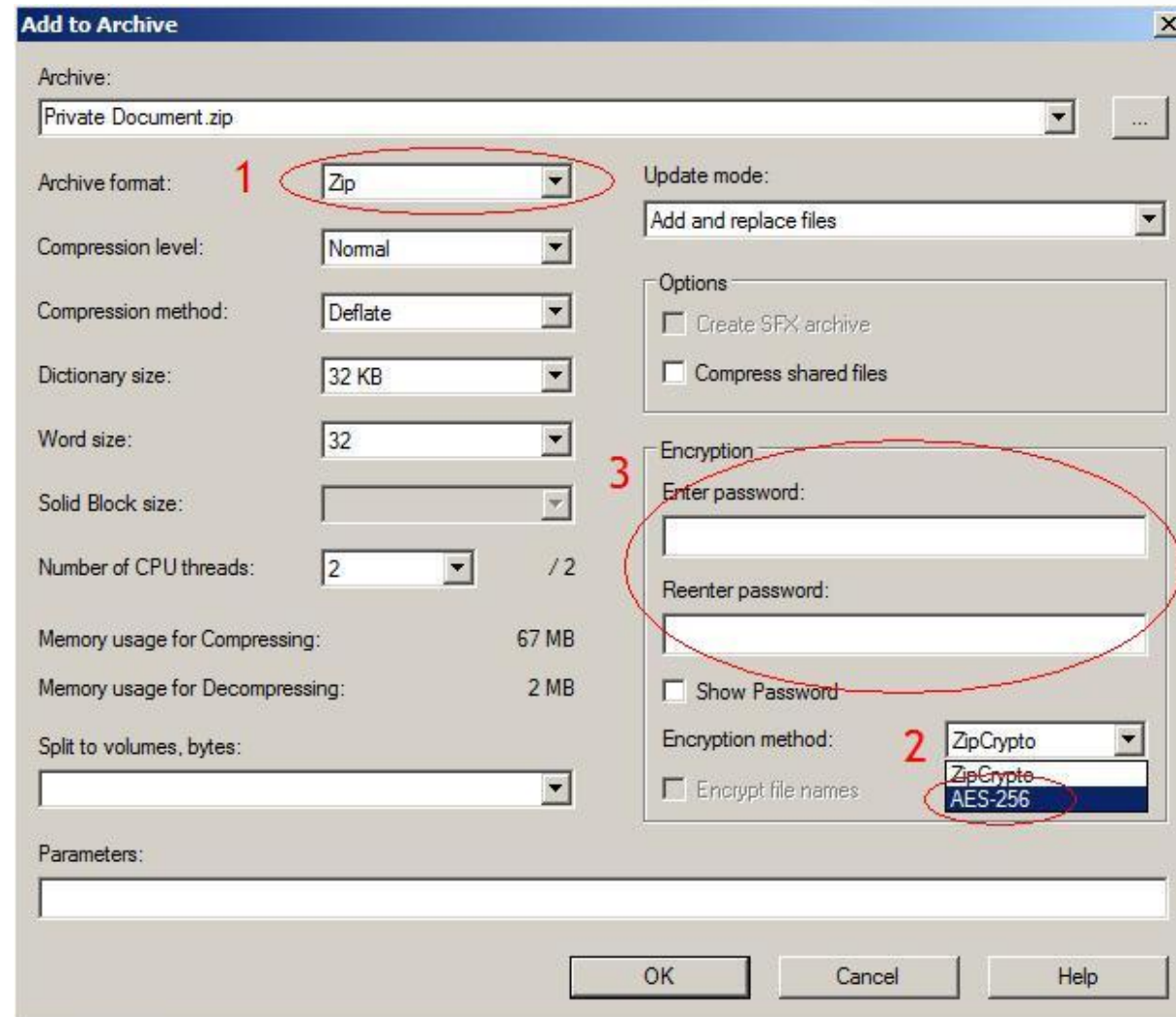
Personal Security – Password Vaults

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



Personal Security – Encryption

- 7-Zip
- AES Crypt
- Veracrypt



Hardware

Raspberry Pi:

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



Hak5: <https://shop.hak5.org/>



Pineapple WiFi

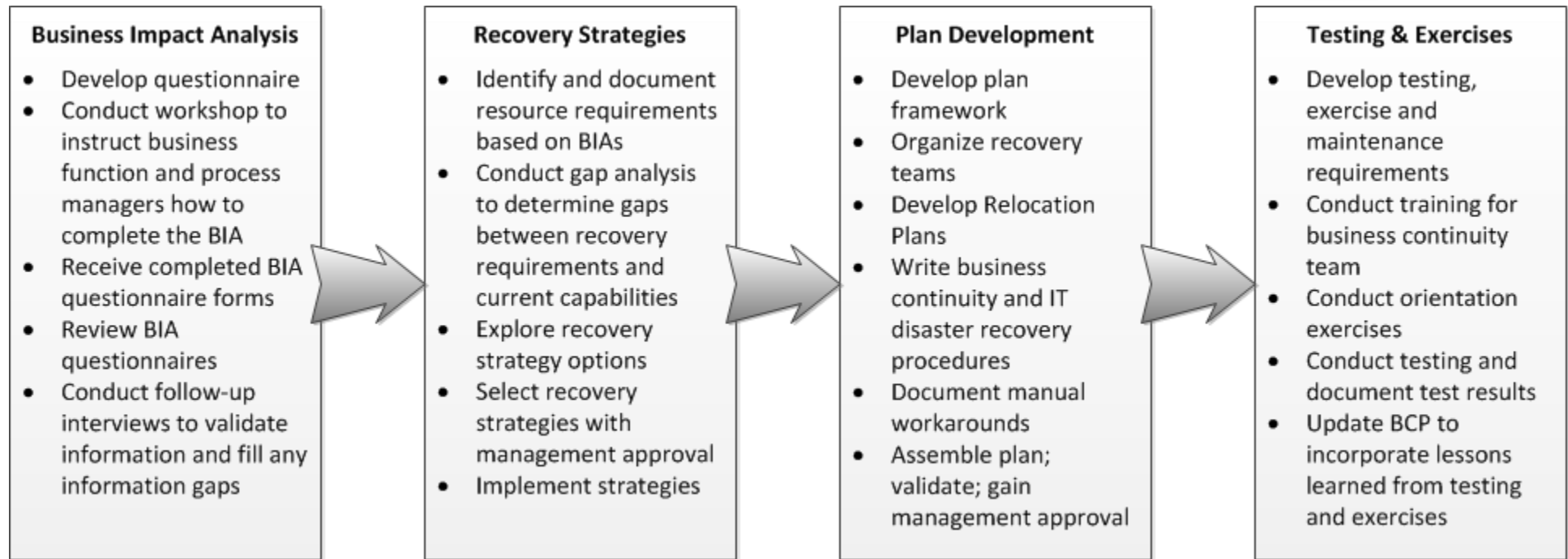


Packet Squirrel



Rubber Ducky

Business Continuity Planning



DHS – [Ready.Gov](https://www.ready.gov)

Business Continuity Planning Suite

Business Continuity Training

Business Continuity Plan Generator

Disaster Recovery Plan Generator (IT Recovery)

Business Continuity Plan Exercise

<https://www.ready.gov/business-continuity-planning-suite>

Going for Help



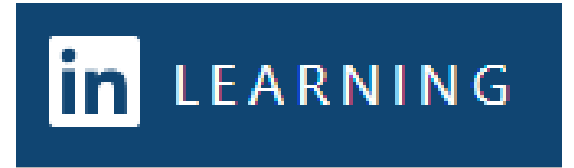
- FBI Internet Crimes Complaint Center (IC3): <https://www.ic3.gov/default.aspx>
- The [Cybersecurity and Infrastructure Security Agency \(CISA\)](#)
- US-CERT Incident Reporting System: <https://www.us-cert.gov/forms/report>
- State Patrol and Local Police
- Your bank & insurance

Security Careers / Certifications



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

Heat Map &
Career Pathway



CompTIA

(ISC)²

CYBRARY

Security Books



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

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.

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

SHARE!

Cybersecurity Tips, Tools, & Techniques

Ron Woerner, CISSP, CISM

ron.woerner @ rwxsecurity.com

[Cyber-AAA.com](https://www.cyber-aaa.com)

Twitter: @ronw123

LinkedIn: <https://www.linkedin.com/in/ronwoerner/>

I HAVE NO SPECIAL
TALENTS. I AM ONLY
**PASSIONATELY
CURIOUS.**
-ALBERT EINSTEIN