RSAConference2020

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

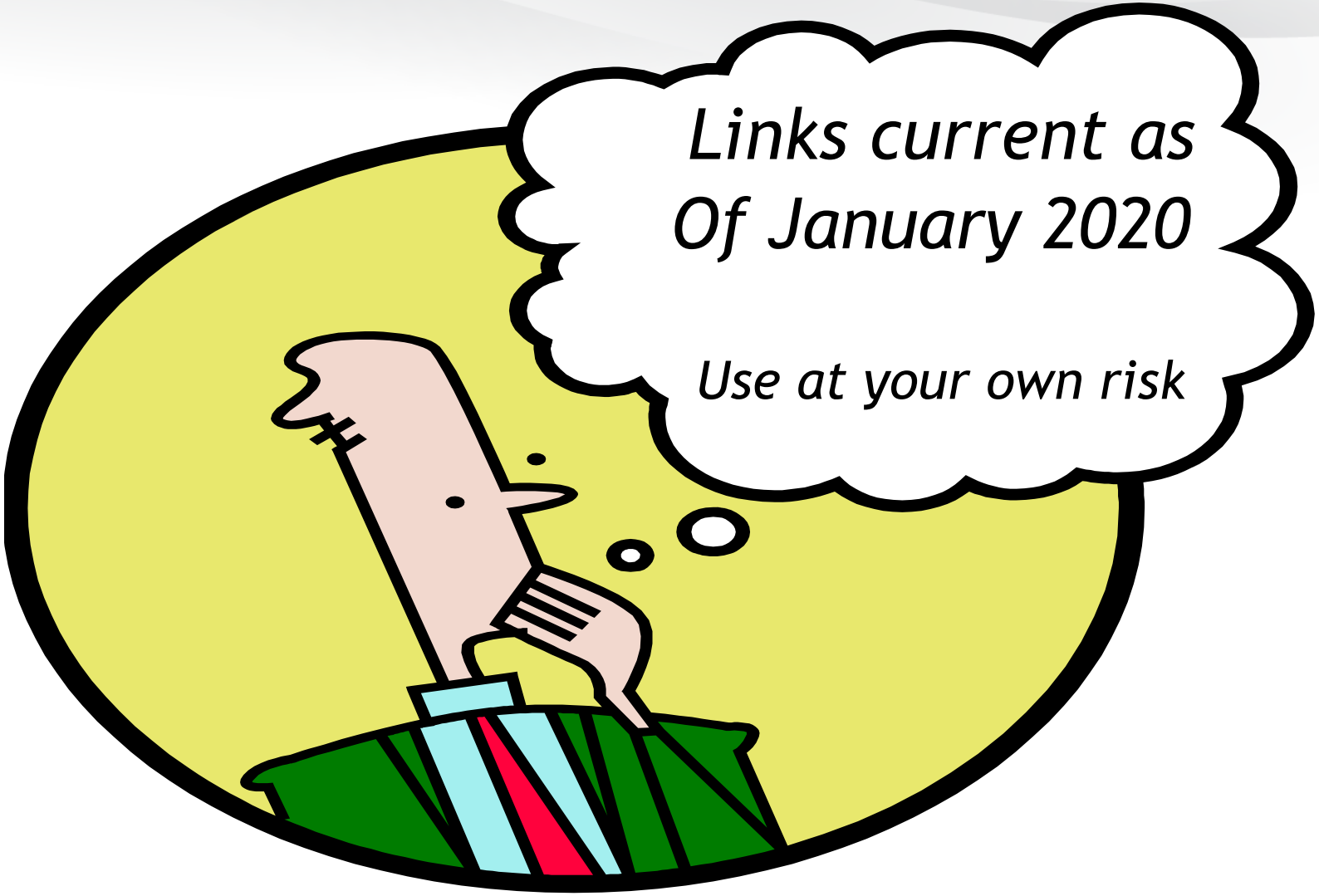
BELLEVUE UNIVERSITY

Cyber AAA
cyber-aaa.com

See it on the
RSAC App

WhoAmI – 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


Links current as
Of January 2020
Use at your own risk

RSAConference2020

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.

"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

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/

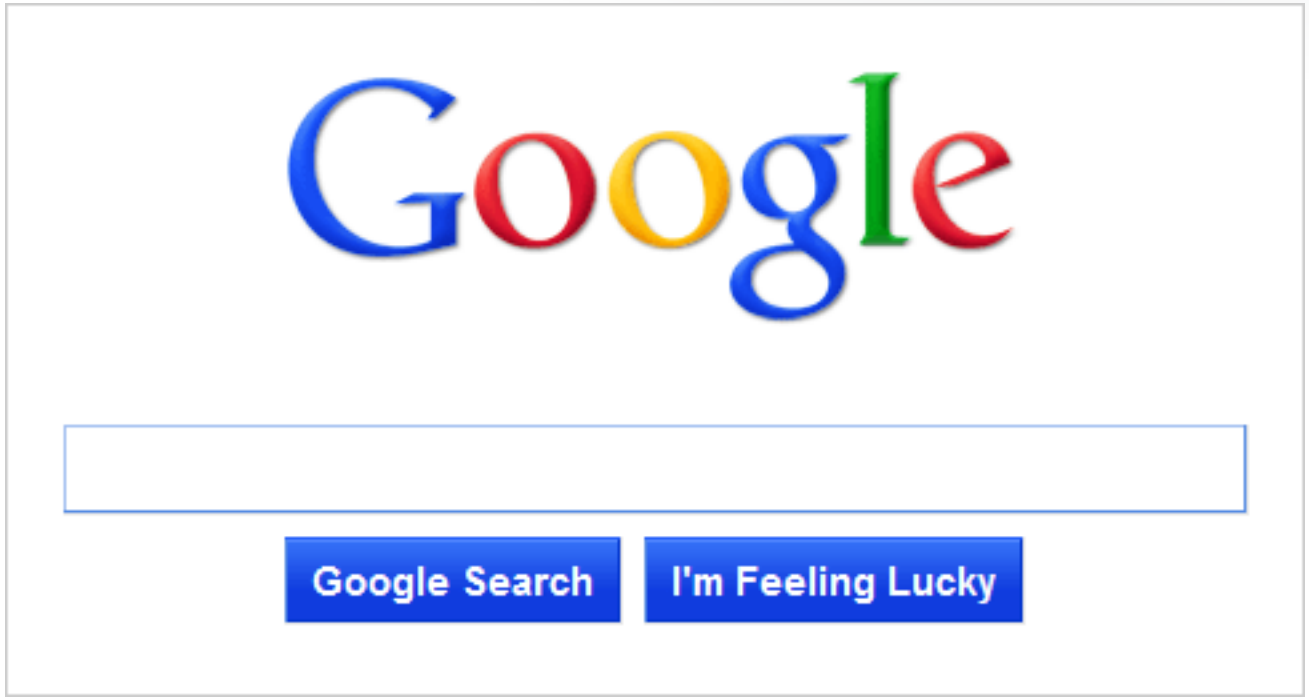
if you SEE | SAY something | something™

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/

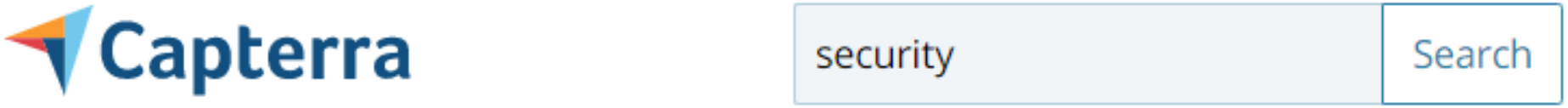
General Cybersecurity Resources

- 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/

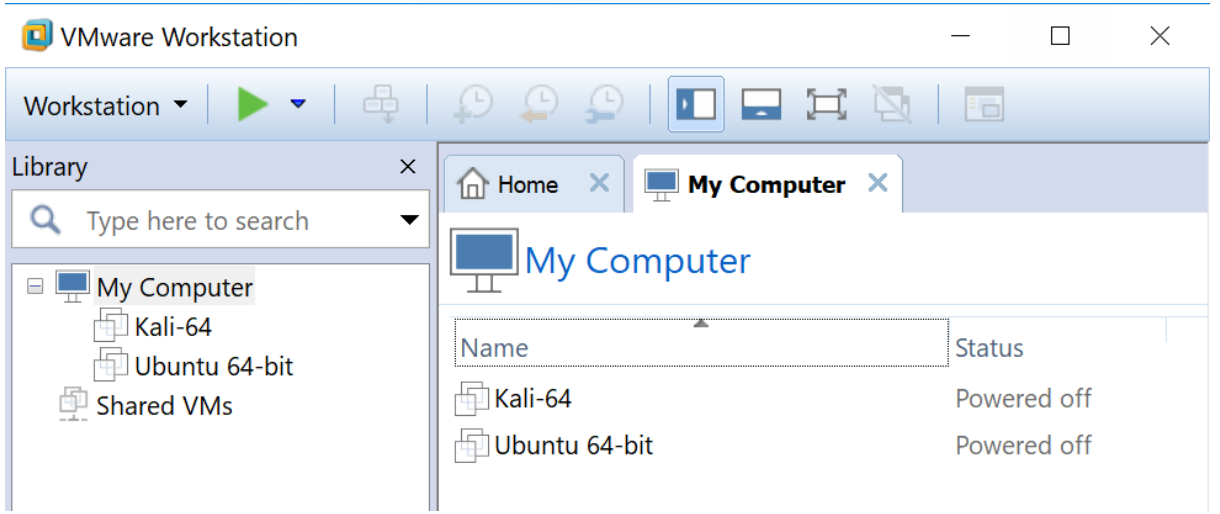
MITRE ATT&CK™ Enterprise Framework

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		

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

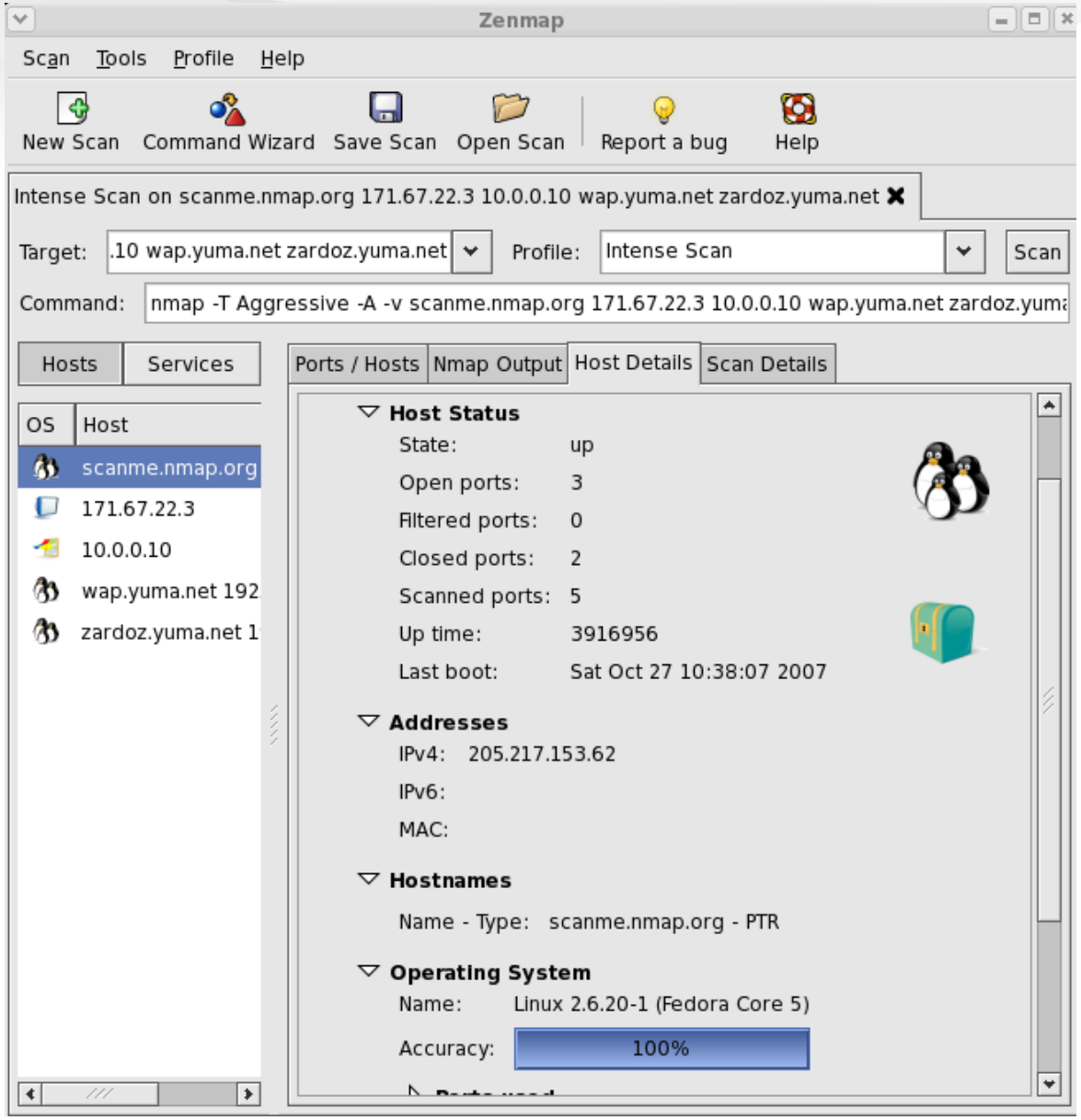
Linux Distros

Linux Distros

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

Network Mapping

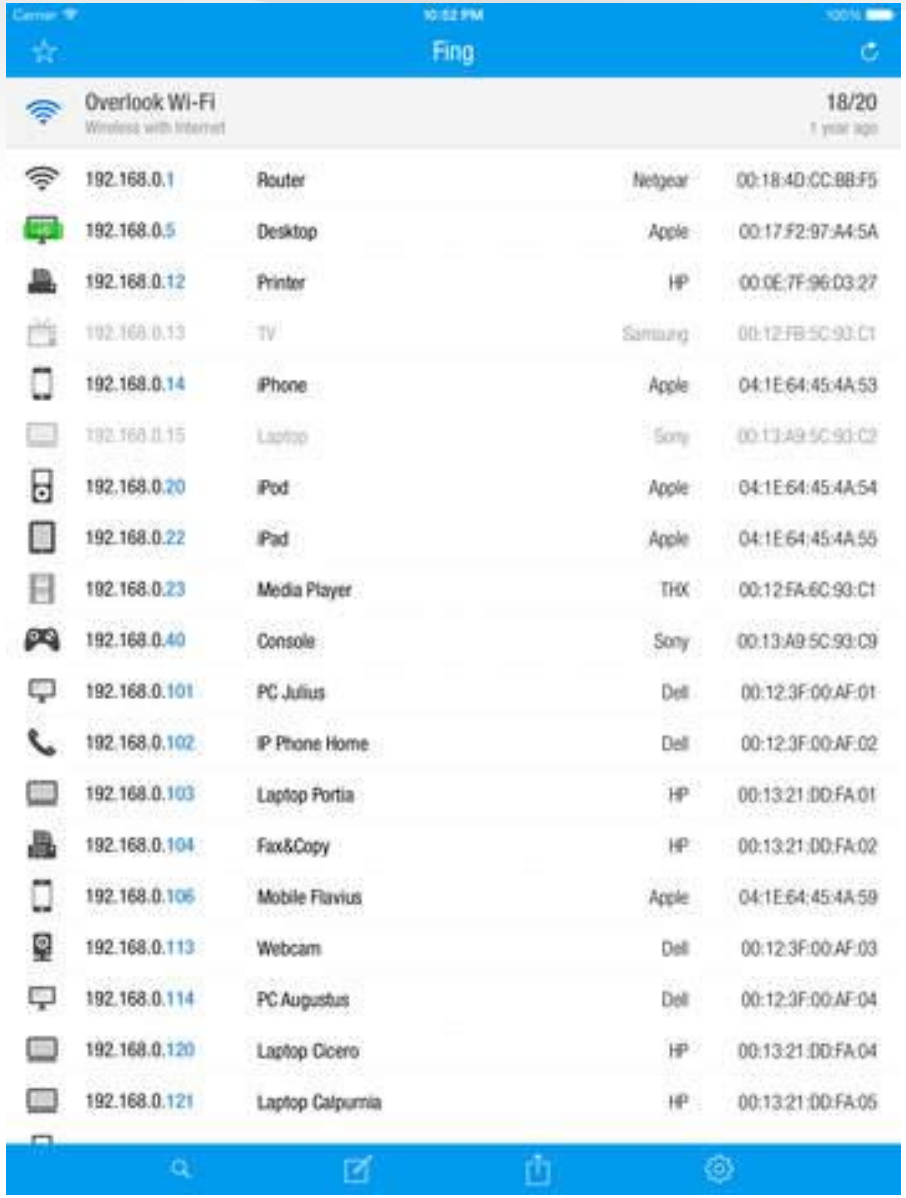
Nmap / ZenMap



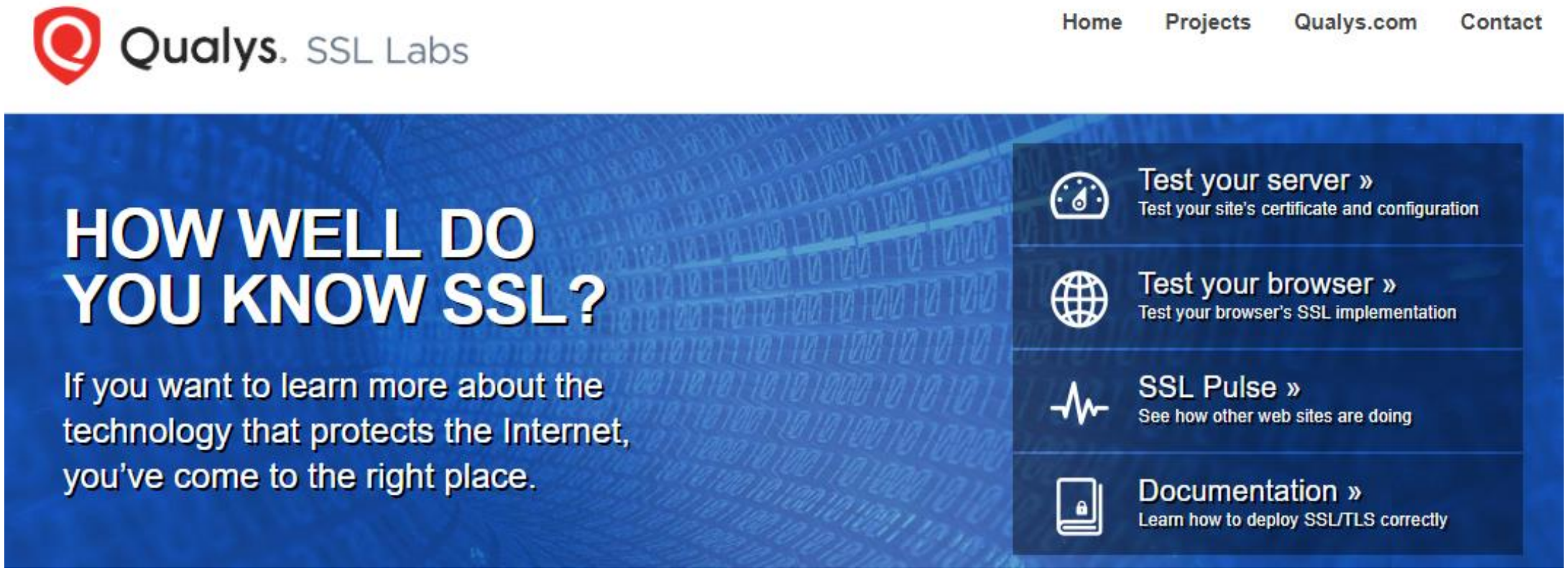
Network Mapping

[Fing]

(iOS & Android)



Network Vulnerability Detection



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, VMMap, VolumeID, Whois, 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

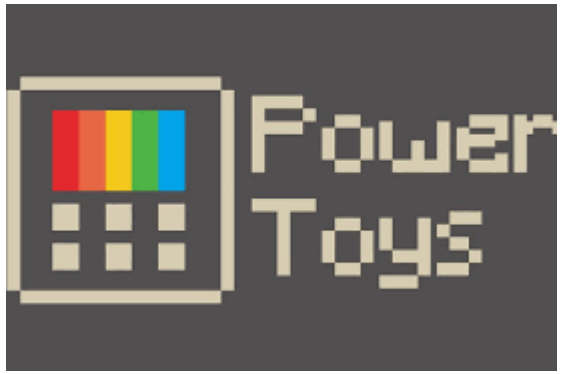
Windows Administration

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



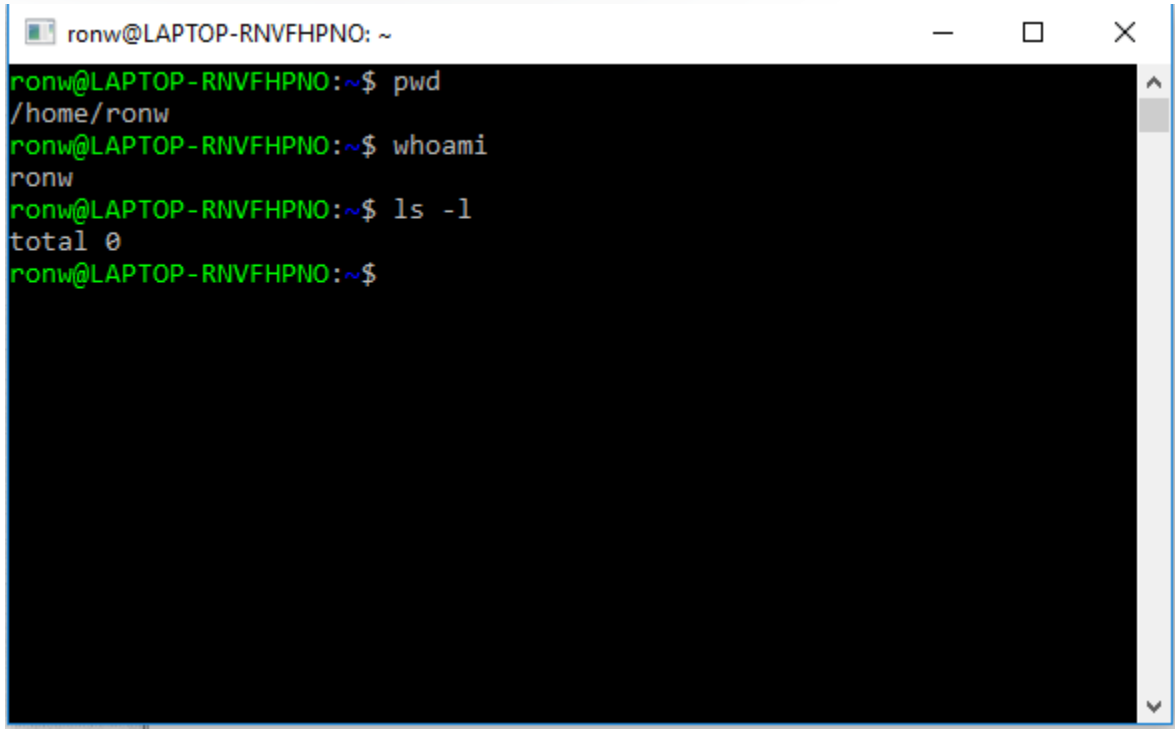
Linux on Windows

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/

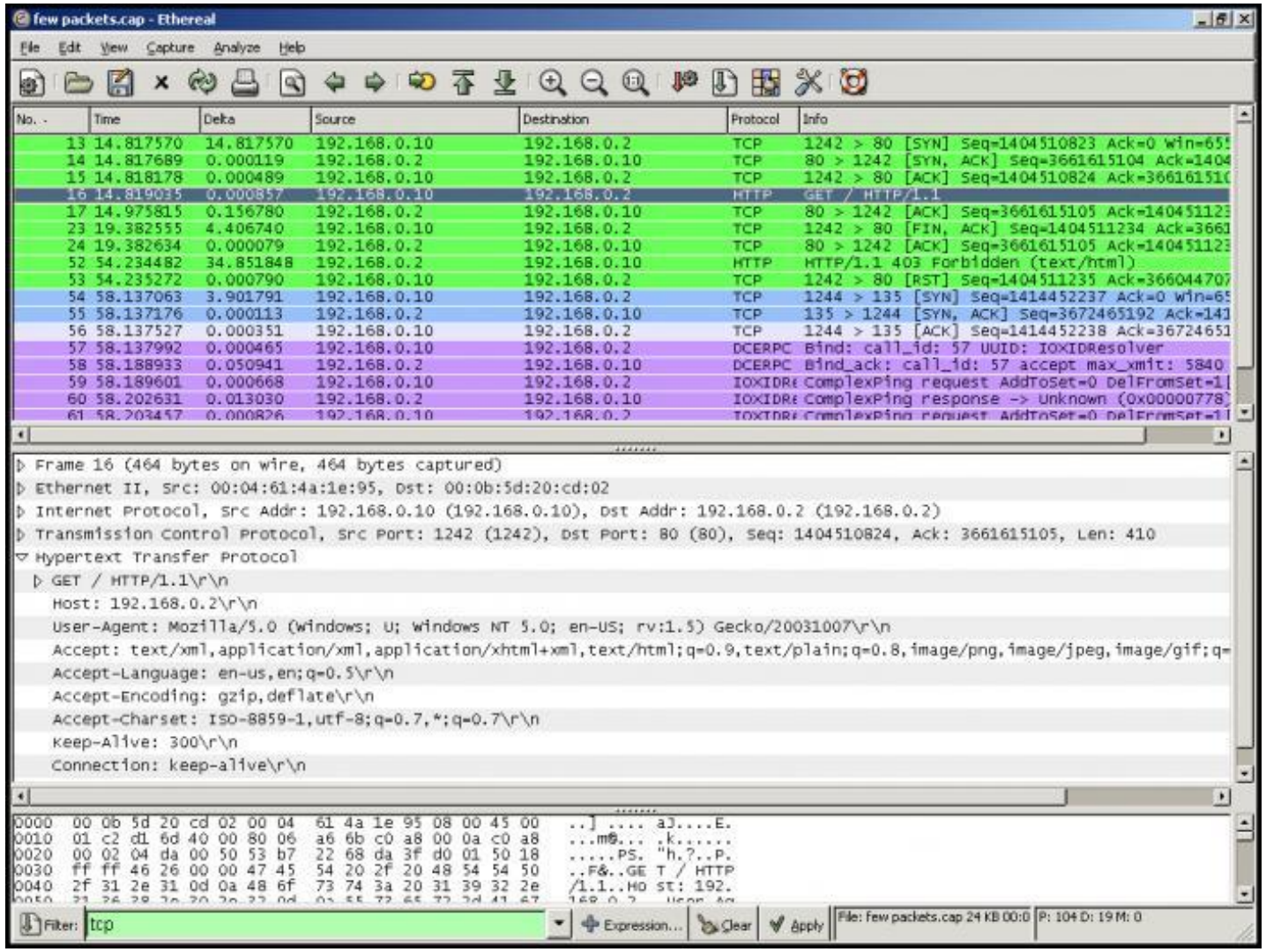


Network Evaluation / Troubleshooting

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.

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

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

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

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

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

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

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:

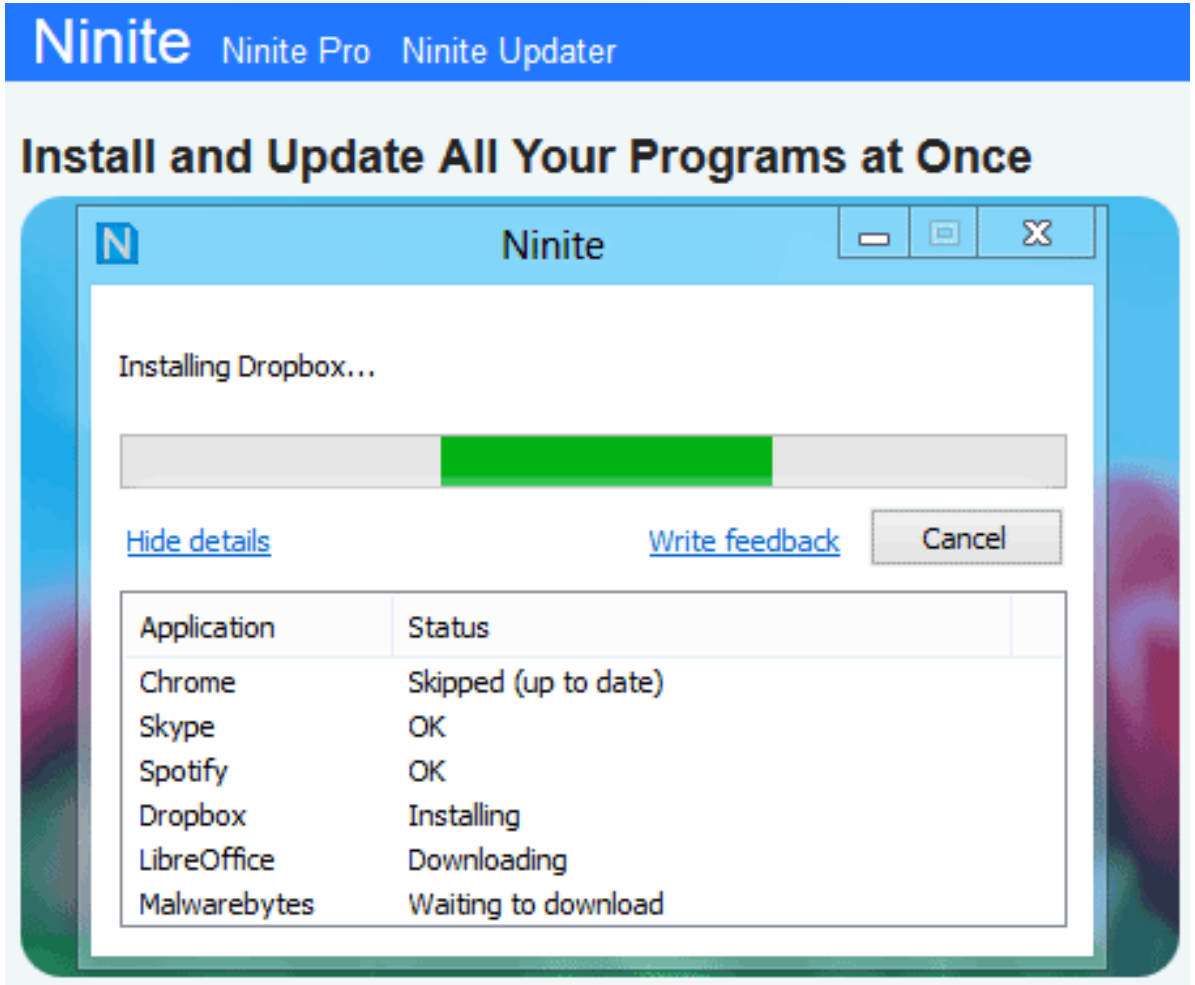
- Suricata
- Elasticsearch
- Logstash
- Kibana
- Scirius Community Edition
- EveBox

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/

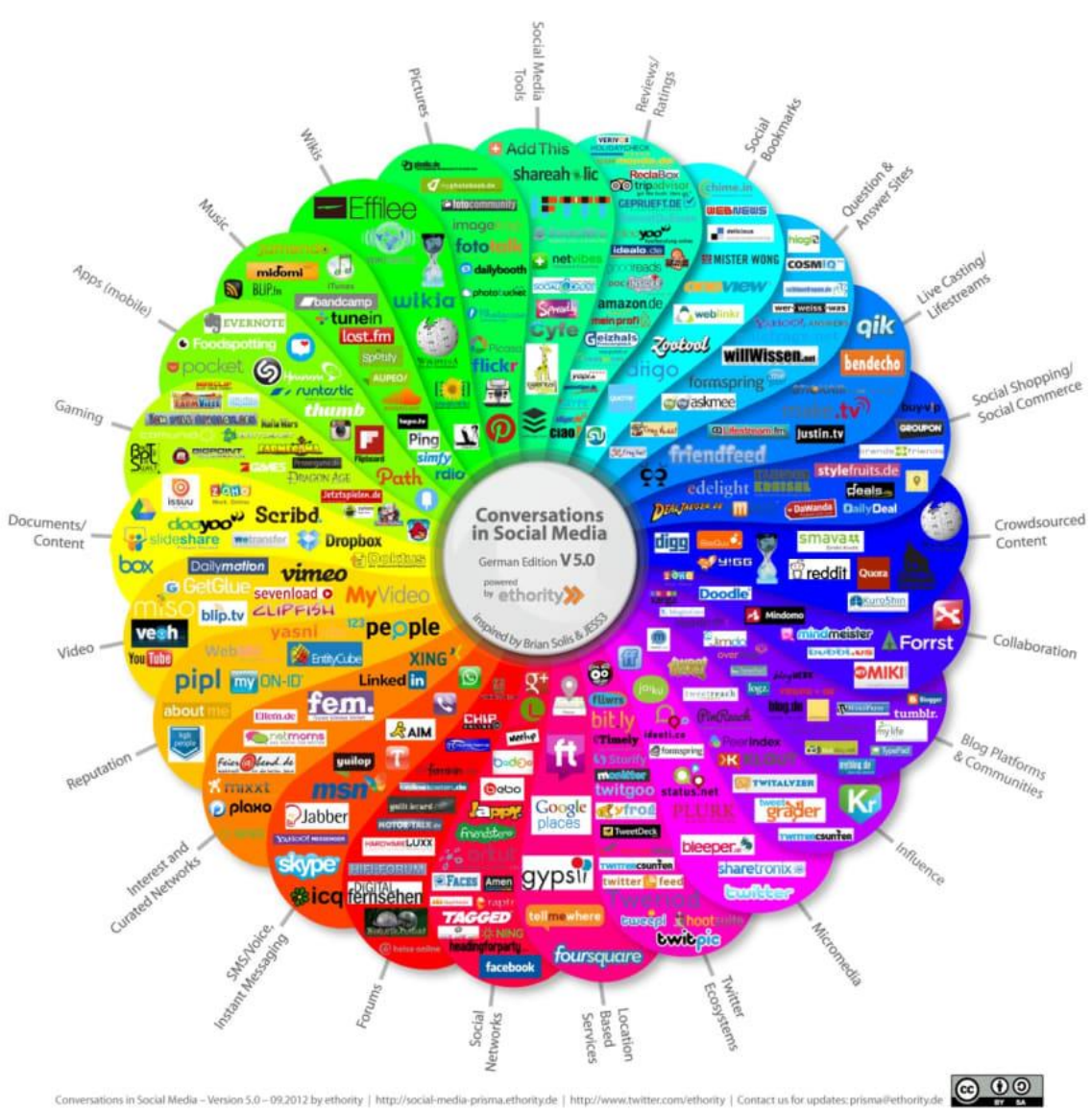
BatchPatch*

https://batchpatch.com/

*Trial versions

Open Source Intelligence

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

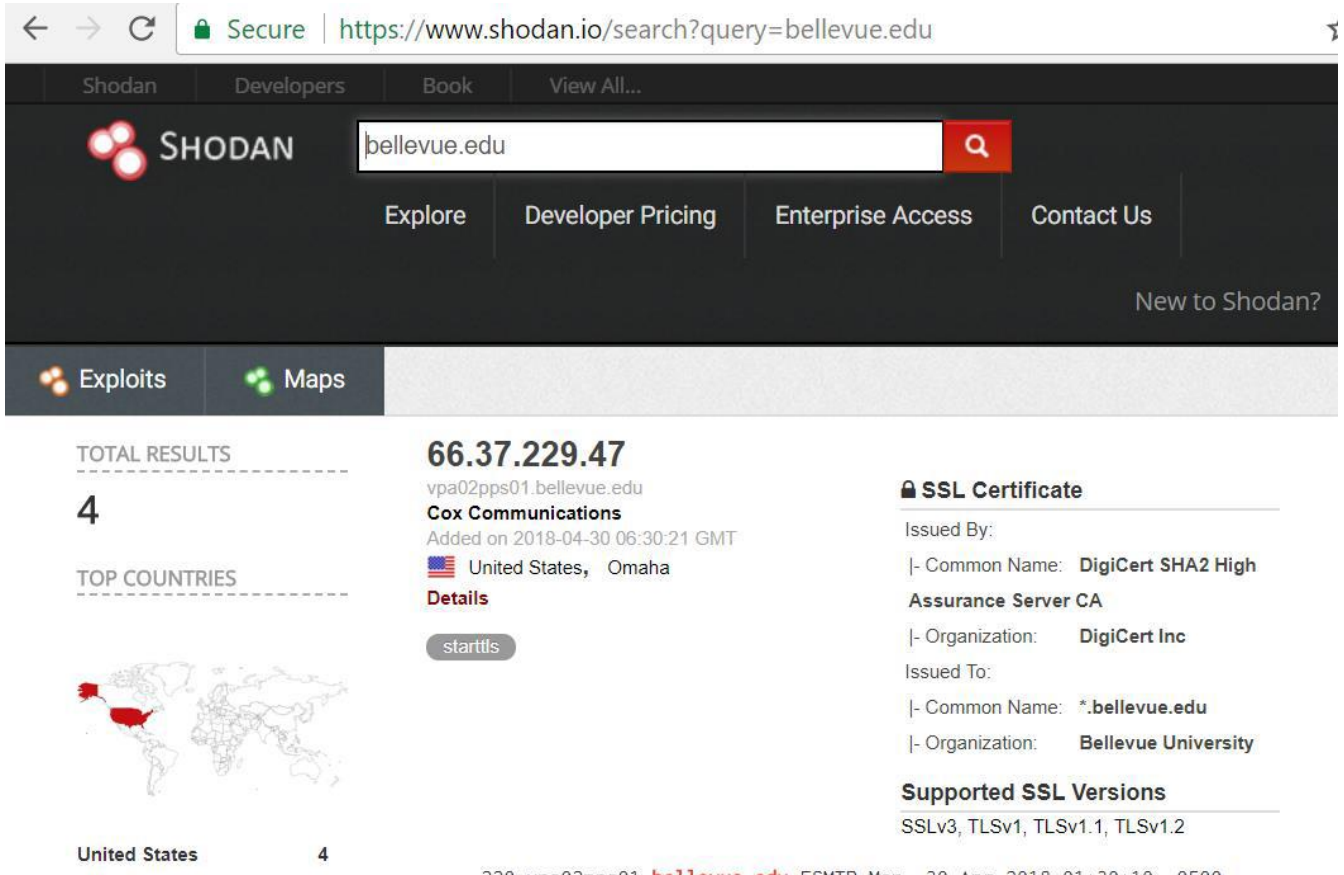


Social Engineering - OSInt

- 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.peekyou.com

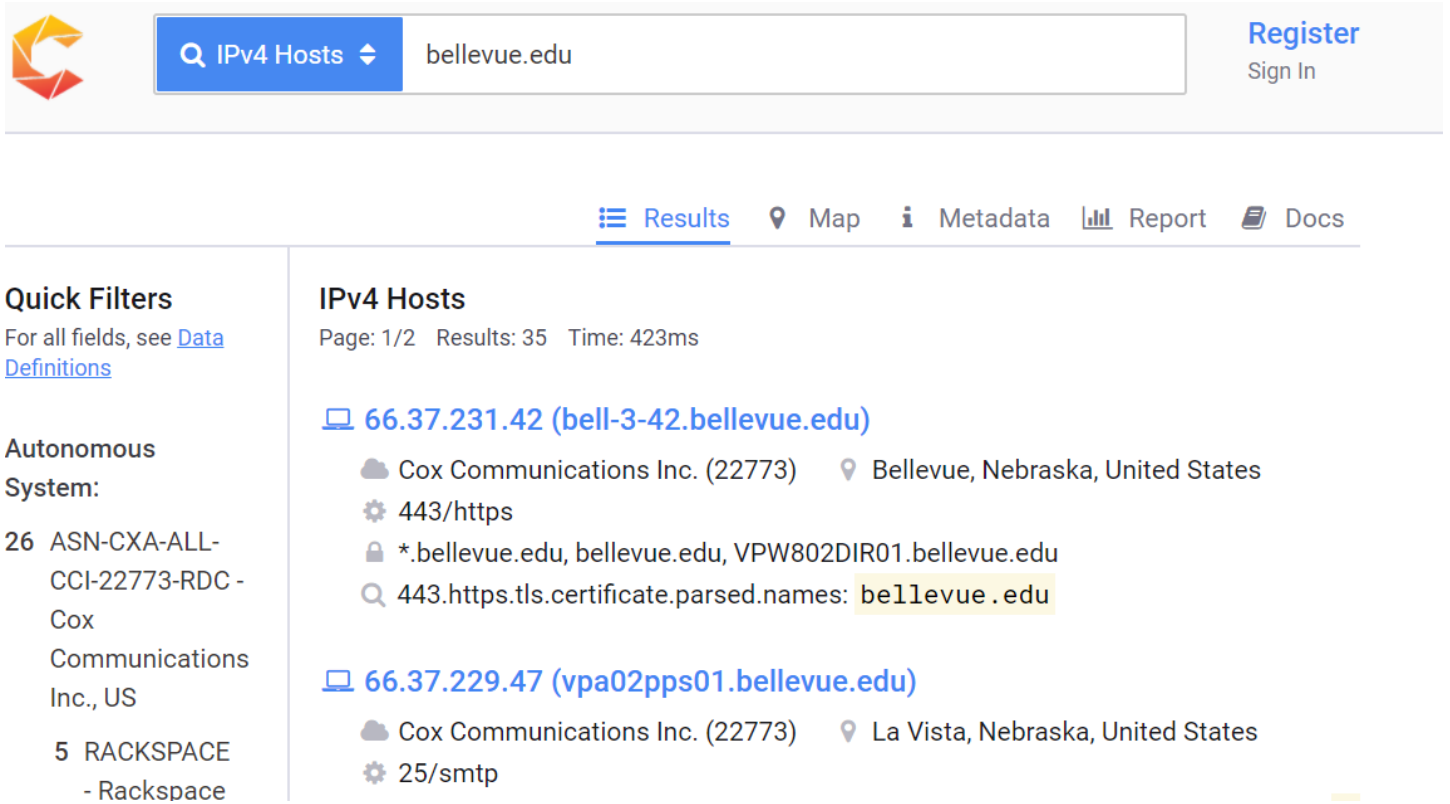
Social Engineering - OSInt

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



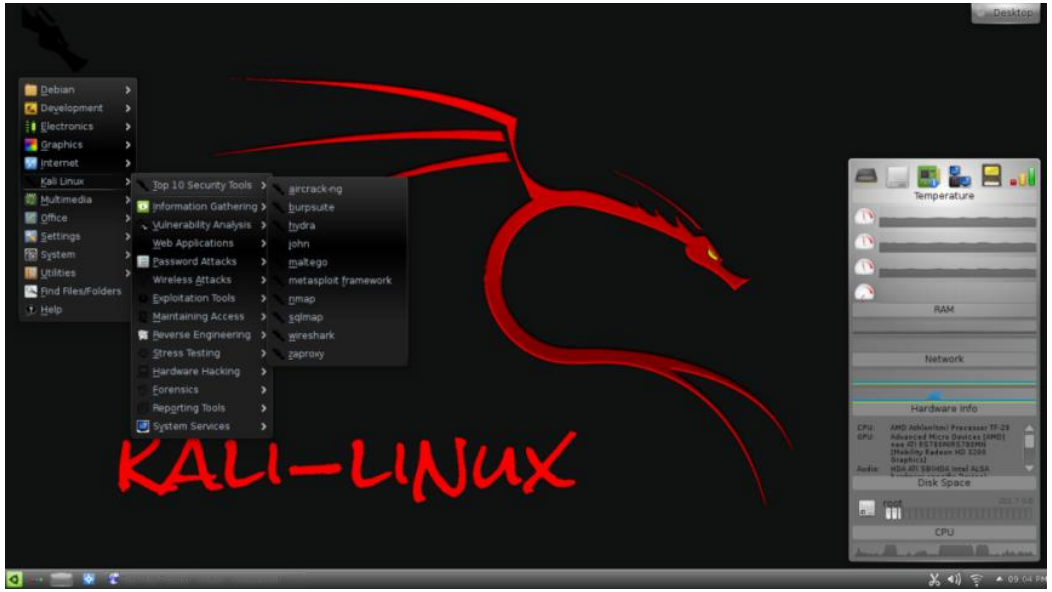
Social Engineering - OSInt

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



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/

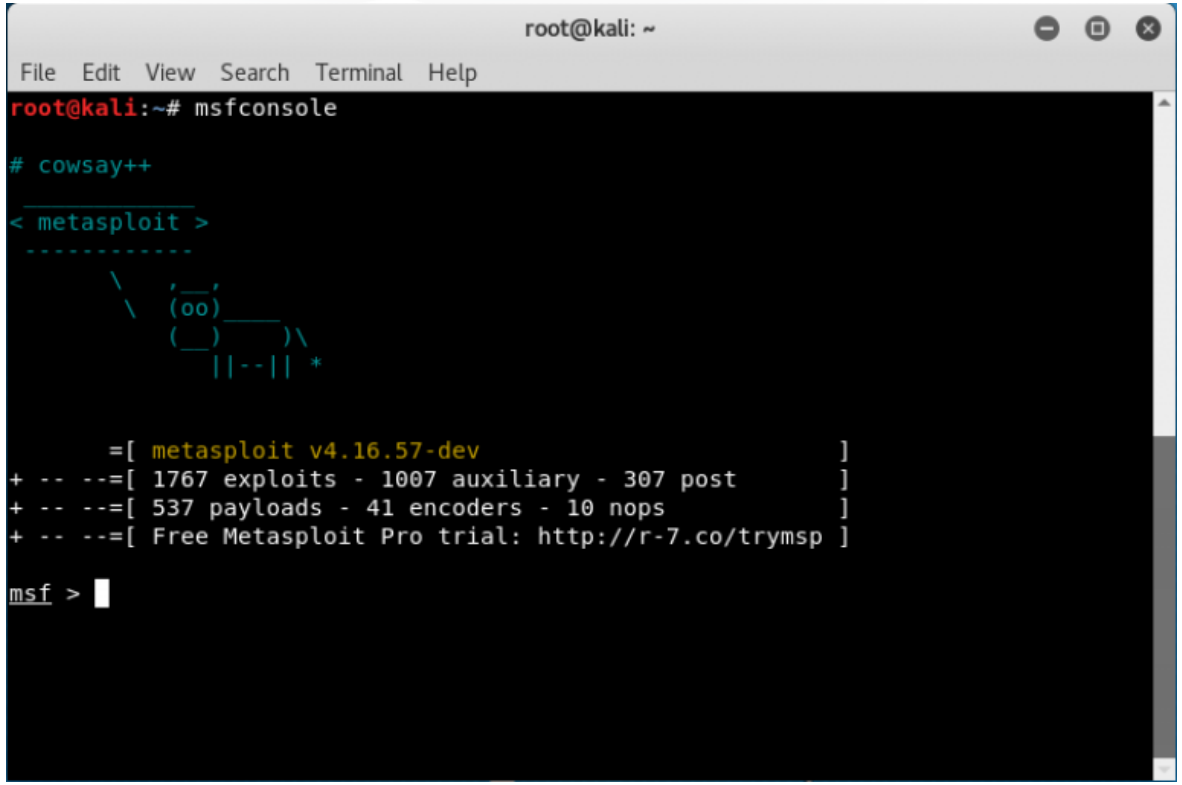
Pen Testing Framework

metasploit®

https://www.metasploit.com/

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

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



Security Testing

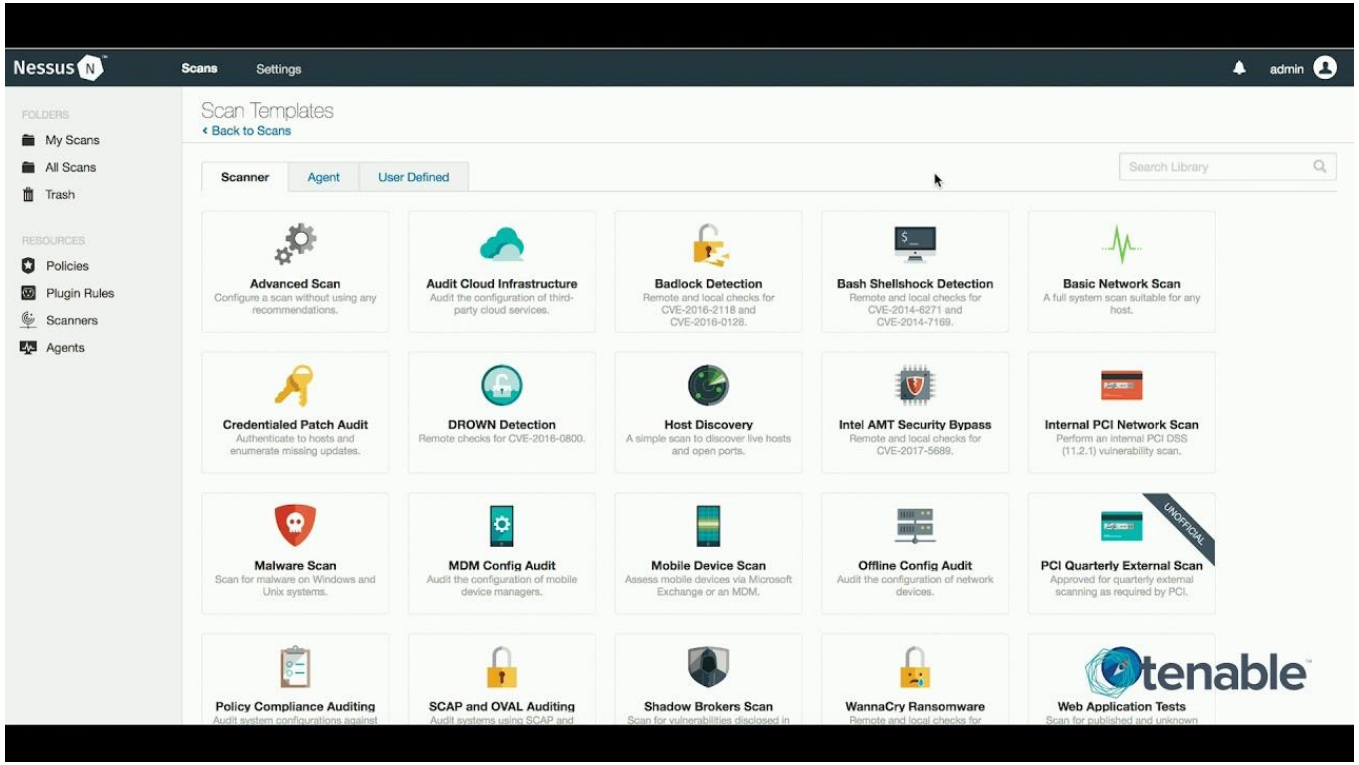
nessus Essentials

Personal use

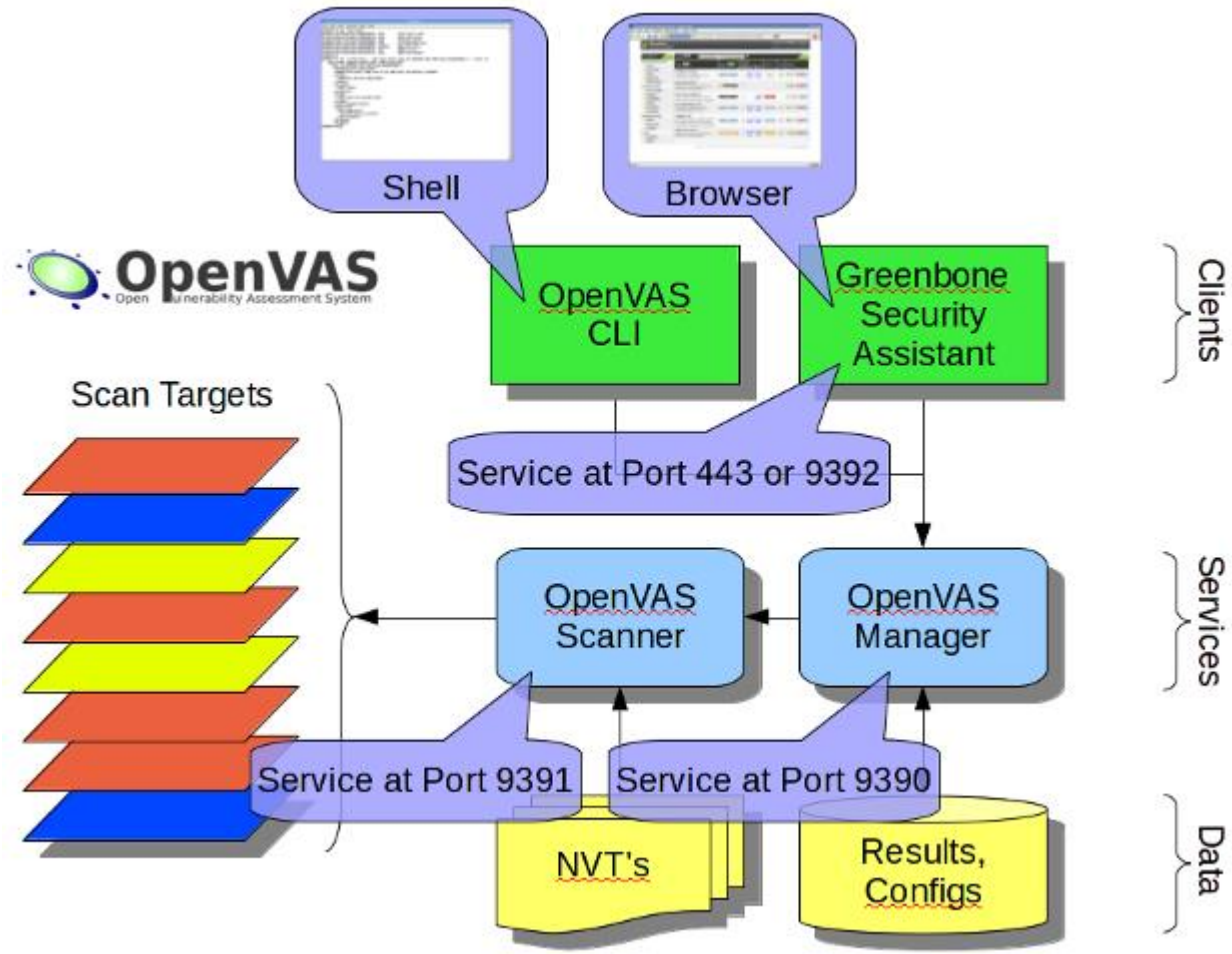
Scan up to 16 IPs

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

Note: Registration required



Security Testing



OpenVAS

Open Vulnerability Assessment Scanner

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

- Zeltsers List – https://zeltser.com/automated-malware-analysis/
- Volatility – https://github.com/volatilityfoundation/volatility
- Cuckoo Sandbox – https://cuckoosandbox.org/

AntiVirus

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

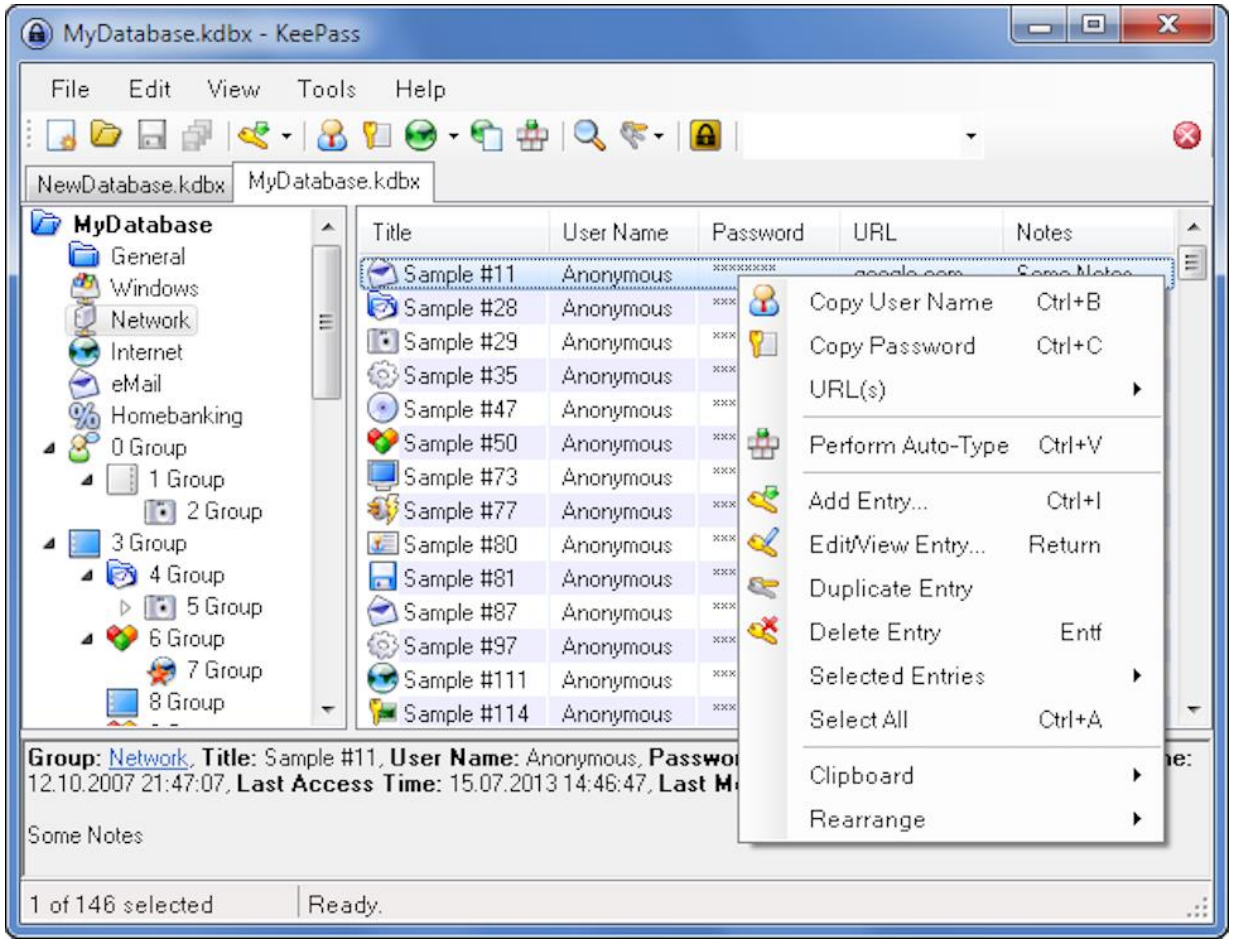
Free AV Products*

- *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)

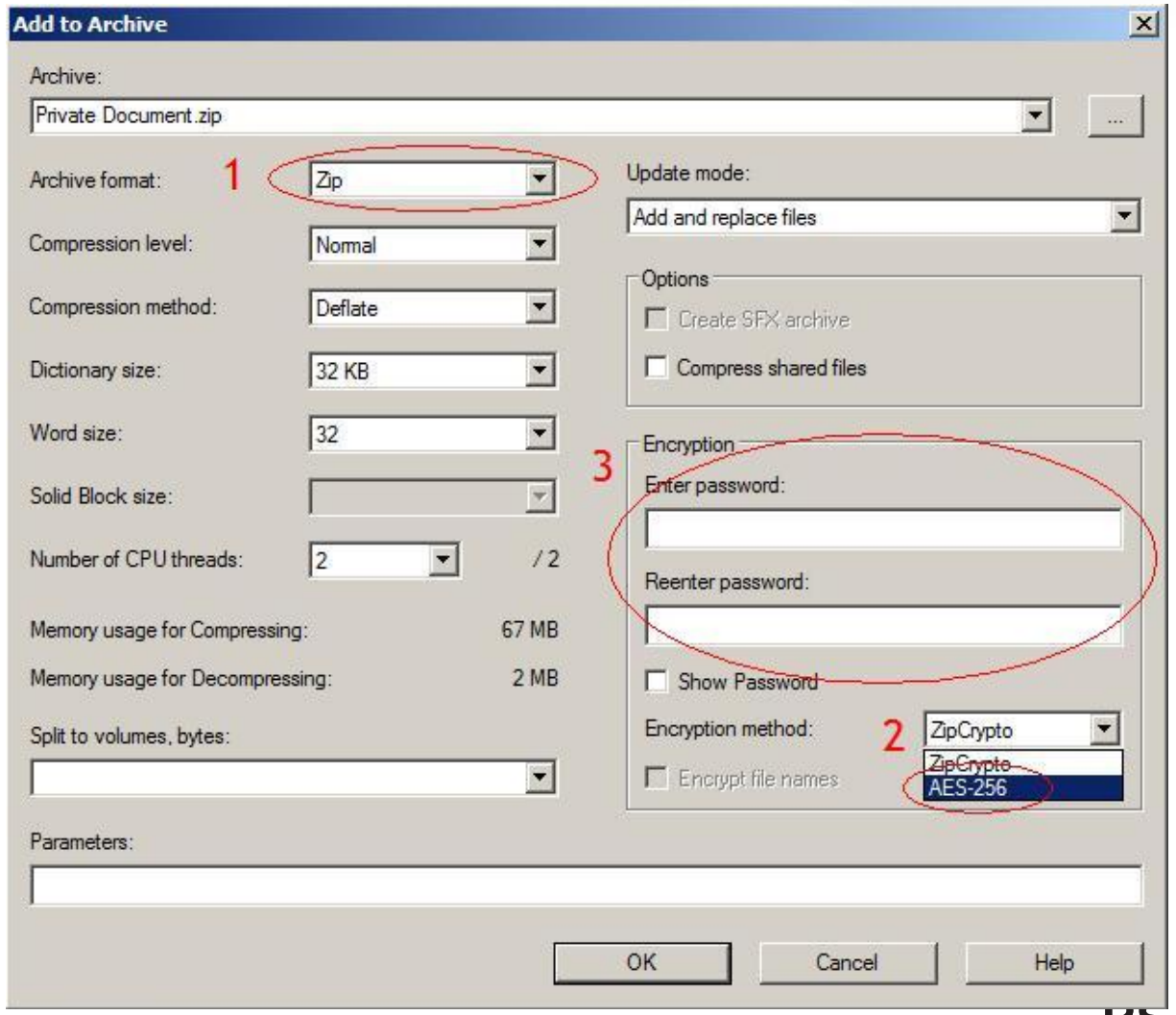
Personal Security – Password Vaults

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



Personal Security – Encryption

- 7-Zip
- AES Crypt
- Veracrypt



Hardware

Raspberry Pi:
https://www.raspberrypi.org/

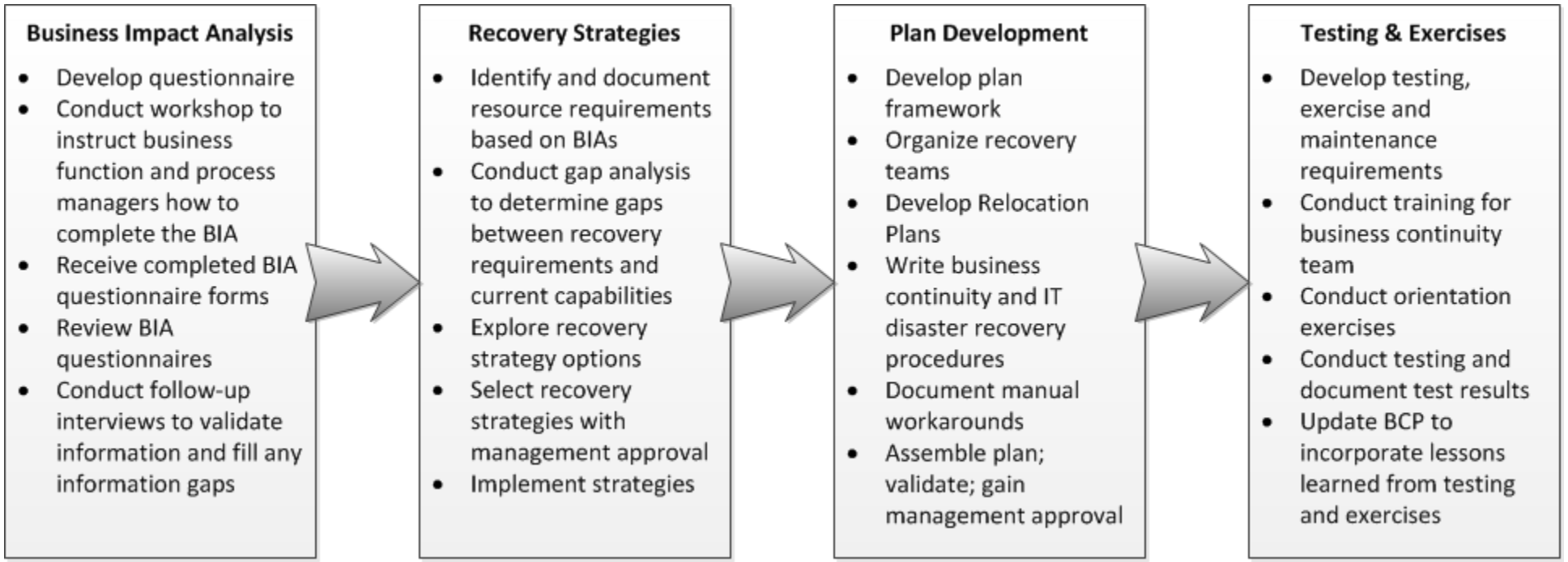
Hak5: https://shop.hak5.org/

Pineapple WiFi

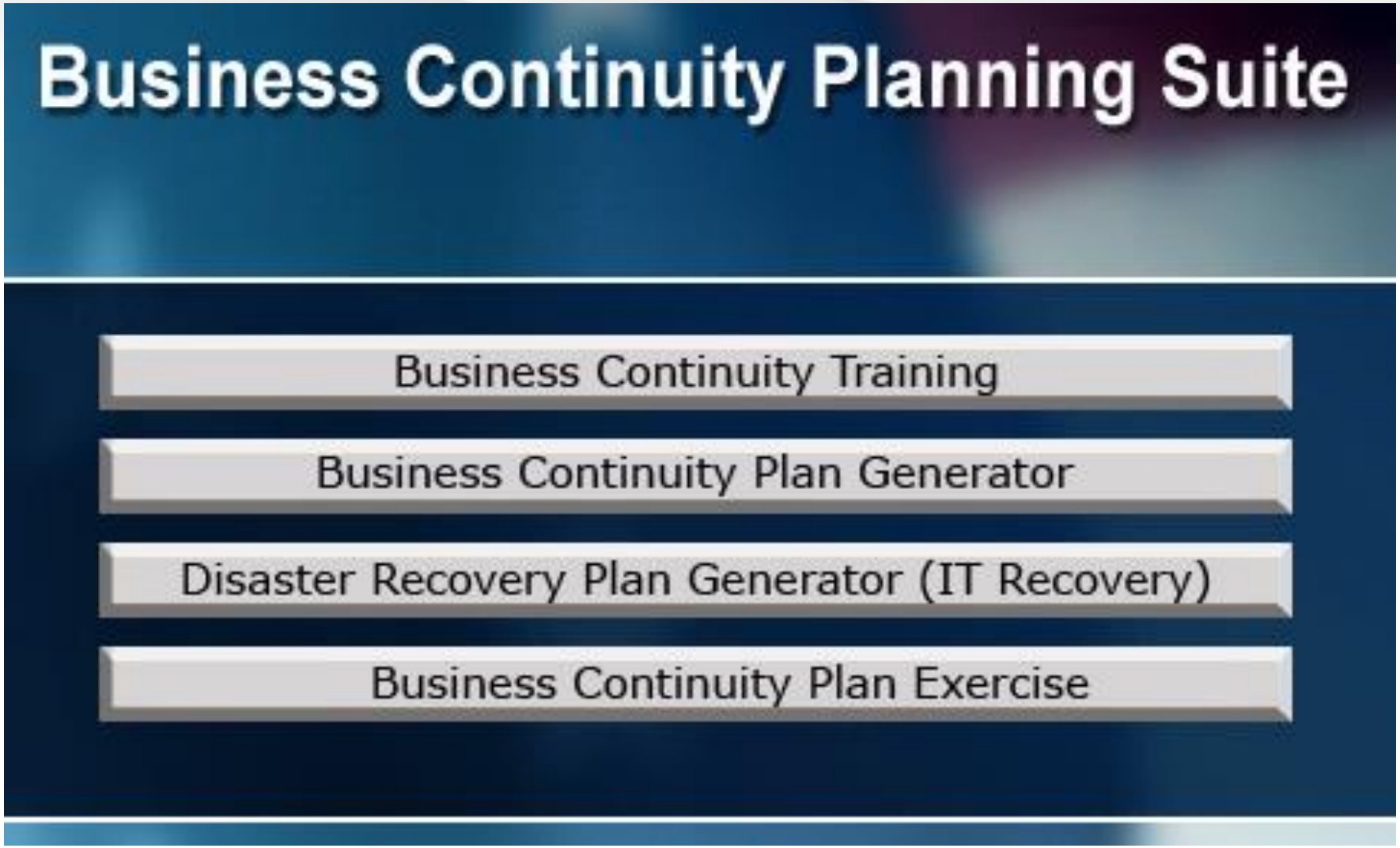
Packet Squirrel

Rubber Ducky

Business Continuity Planning



DHS – [Ready.Gov]



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

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

CyberSeek™

https://www.cyberseek.org/

Heat Map &
Career Pathway

CompTIA

LinkedIn LEARNING

(ISC)²

CYBRARY

Security Books

CYBERSECURITY CANON

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"

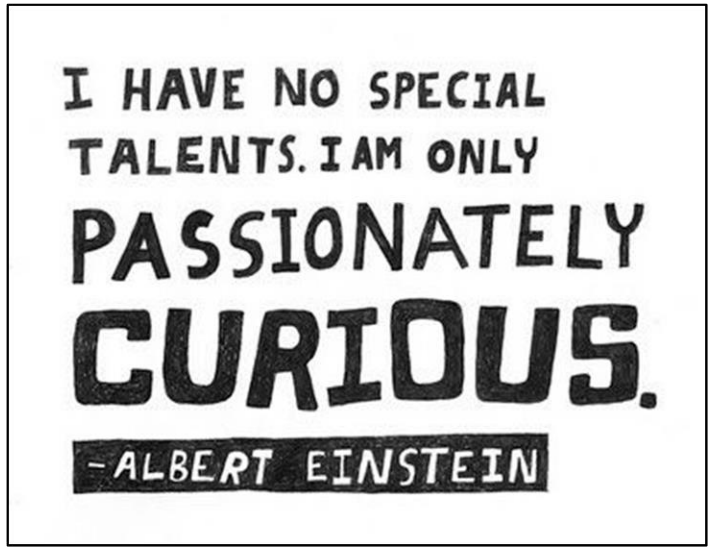
- Immediate:
  - Pick 1 or 2 tools / techniques
  - Play / Try it out / Experiment
- Next 4-6 Weeks (rinse and repeat in 3 & 6 mos):
  - Review this slide deck
  - Pick more tools (3-5)
  - Experiment with tools in a virtual environment
  - Review the awareness websites

Cybersecurity Tips, Tools, & Techniques

Ron Woerner, CISSP, CISM

ron.woerner @ rwxsecurity.com

Cyber-AAA.com

Twitter: @ronw123

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