Cybersecurity Tips, Tools and Techniques Updated for 2020

Ron Woerner, CISSP, CISM
Professor, Bellevue University
President, Cyber-AAA, LLC
@ronw123
See it on the RSAC App
Who Am I – 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
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
First Some Basics

THANKS...

CAPTAIN OBVIOUS
First Some Basics

- Free is not always “free”
- Do your homework
- Test, test, test
If you only remember 1 slide...

https://staysafeonline.org/

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

https://www.stopthinkconnect.org/

https://www.cisa.gov/
#1 Technical Hacking Tool

https://www.google.com/advanced_search

https://lmgtfy.com/
Lists of Tools, Tips & Tricks

- SecTools
- Peerlyst List of Security Tools
- OlderGeeks
- HowToGeek.com,  Geek School
Lists of Hacker Tools


- Art of Hacking: https://github.com/The-Art-of-Hacking/h4cker
Lists of Hacker Tools


- 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
- 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**
  - Publications: [http://csrc.nist.gov/publications/PubsSPs.html](http://csrc.nist.gov/publications/PubsSPs.html)

- **Center for Internet Security**
  - Controls: [https://www.cisecurity.org/controls/](https://www.cisecurity.org/controls/)
  - Benchmarks: [https://www.cisecurity.org/cis-benchmarks/](https://www.cisecurity.org/cis-benchmarks/)
  - CIS Controls Self-Assessment Tool, or CIS CSAT

- **DoD Cyber Exchange (Public)** - [https://public.cyber.mil/](https://public.cyber.mil/)
  DISA IASE Security Technical Implementation Guides (STIGs) - [https://public.cyber.mil/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

- 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
- 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
- privacypolicies.io – encryption against global mass surveillance
Security Awareness Training

- TreeTop Cybersecurity Awareness – https://www.treetopsecurity.com/slides
- Wizer – https://wizer-training.com/
- SANS – https://www.sans.org/security-awareness-training/resources
Finding Products

https://www.capterra.com/
## MITRE ATT&CK™

### Enterprise Framework

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Exfiltration</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive-by Compromise</td>
<td>AppleScript</td>
<td>bash_profile and <code>bashrc</code></td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>AppleScript</td>
<td>Audio Capture</td>
<td>Commonly Used Port</td>
<td>Automated Exfiltration</td>
<td>Data Destruction</td>
<td></td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>CMSTP</td>
<td>Accessibility Features</td>
<td>Binary Pedding</td>
<td>Bash History</td>
<td>Application Windows Discovery</td>
<td>Application Deployment Software</td>
<td>Distributed Component Object Model</td>
<td>Remote File Copy</td>
<td>Remote File Copy</td>
<td>Data Compressed</td>
<td></td>
</tr>
<tr>
<td>External Remote Services</td>
<td>Command-Line Interface</td>
<td>Account Manipulation</td>
<td>BITS Jobs</td>
<td>Brute Force</td>
<td>Browser Bookmark Discovery</td>
<td>Clipboard Data</td>
<td>Connection Proxy</td>
<td>Data Encrypted for Impact</td>
<td>Data Compressed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Control Panel Items</td>
<td>AppCert DLLs</td>
<td>Application Shimming</td>
<td>Clear Command History</td>
<td>Credentials in Files</td>
<td>File and Directory Discovery</td>
<td>Logon Scripts</td>
<td>Data from Local System</td>
<td>Data Encoding</td>
<td>Data Compressed</td>
<td></td>
</tr>
<tr>
<td>Spear phishing Link</td>
<td>Execution through API</td>
<td>Authentication Package</td>
<td>DLL Search Order Hijacking</td>
<td>Code Signing</td>
<td>Exploitation for Credential Access</td>
<td>Network Share Discovery</td>
<td>Pass the Ticket</td>
<td>Data from Network Shared Drive</td>
<td>Exfiltration Over Command and Control Channel</td>
<td>Data Encrypted for Impact</td>
<td></td>
</tr>
<tr>
<td>Spear phishing via Service</td>
<td>Execution through Module Load</td>
<td>BITS Jobs</td>
<td>Dylib Hijacking</td>
<td>Compile After Delivery</td>
<td>Forced Authentication</td>
<td>Network Sniffing</td>
<td>Remote Desktop Protocol</td>
<td>Data Staged</td>
<td>Domain Fronting</td>
<td>Endpoint Denial of Service</td>
<td></td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td>Exploitation for Client Execution</td>
<td>Bootkit</td>
<td>Exploitation for Privilege Escalation</td>
<td>Compiled HTML File</td>
<td>Hooking</td>
<td>Password Policy Discovery</td>
<td>Remote File Copy</td>
<td>Email Collection</td>
<td>Domains Generation Algorithms</td>
<td>Data Staged</td>
<td></td>
</tr>
<tr>
<td>Trusted Relationship</td>
<td>Graphical User Interface</td>
<td>Browser Extensions</td>
<td>Extra Window Memory Injection</td>
<td>Component Firmware</td>
<td>Input Capture</td>
<td>Peripheral Device Discovery</td>
<td>Remote Services</td>
<td>Input Capture</td>
<td>Feedback Channels</td>
<td>File Accessorption</td>
<td></td>
</tr>
<tr>
<td>Valid Accounts</td>
<td>InstallUI</td>
<td>Change Default File Association</td>
<td>File System Permissions Weakness</td>
<td>Component Object Model Hijacking</td>
<td>Input Prompt</td>
<td>Permission Groups Discovery</td>
<td>Replication Through Removable Media</td>
<td>Man In The Browser</td>
<td>Multi-hop Proxy</td>
<td>Exfiltration Over Other Network Layer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Launch!</td>
<td>Component Firmware</td>
<td>Hacking</td>
<td>Control Panel Items</td>
<td>Kerbeasting</td>
<td>Process Discovery</td>
<td>Shared Webroot</td>
<td>Screen Capture</td>
<td>Multi-Phase Channels</td>
<td>Exfiltration Over Physical Medium</td>
<td></td>
</tr>
<tr>
<td>Local Job Scheduling</td>
<td>Component Object Model Hijacking</td>
<td>Image File Execution Option Injection</td>
<td>DClShadow</td>
<td>Keychain</td>
<td>Query Registry</td>
<td>SIS Hijacking</td>
<td>Video Capture</td>
<td>Multiband Communication</td>
<td>Exfiltration Over Physical Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LSASS Driver</td>
<td>Create Account</td>
<td>Launch Daemon</td>
<td>Decode/Decapsulate/Decode Files or Information</td>
<td>LLMMI/NSTWS</td>
<td>Poisoning and Relay</td>
<td>Remote System Discovery</td>
<td>Taunt Shared Content</td>
<td>Mix Master Encryption</td>
<td>Service Stop</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[https://attack.mitre.org/](https://attack.mitre.org/)
Personal Labs – Virtual Environments

- Oracle VM VirtualBox
- VM Ware 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/
Network Mapping

Nmap / ZenMap
#RSAC

## Network Mapping

### Fing

(iOS & Android)

![Network Mapping Diagram](image-url)
Network Vulnerability Detection

Qualys. SSL Labs

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.

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
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
- **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:
Network Security Monitoring

Zeek (fka Bro): [https://www.zeek.org/](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.


A Live ISO dedicated to Suricata

SELKS is both bootable 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 90 sec. The name comes from its major components:

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

HT to [https://www.activecountermeasures.com/free-tools/](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 –
Social Engineering - OSInt

- OSInt Framework – [https://osintframework.com/](https://osintframework.com/)
- Sublist3r, Enumerate website subdomains – [https://github.com/aboul3la/Sublist3r](https://github.com/aboul3la/Sublist3r)
- Spiderfoot – [https://www.spiderfoot.net/](https://www.spiderfoot.net/)
- Maltego – [https://www.paterva.com/](https://www.paterva.com/)
- Peek You - www.peekyou.com
Social Engineering - OSInt

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/](https://www.kali.org/downloads/)

- **Parrot Security OS**

- **Tails**
  [https://tails.boum.org/](https://tails.boum.org/)
Social Engineering Toolkit (SET)

https://www.trustedsec.com/social-engineer-toolkit-set/
Pen Testing Framework

https://www.metaspoit.com/

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

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

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

- 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


*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:  

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

HT to

Pineapple WiFi
Packet Squirrel
Rubber Ducky
Business Continuity Planning

Business Impact Analysis
- Develop questionnaire
- Conduct workshop to instruct business function and process managers how to complete the BIA
- Receive completed BIA questionnaire forms
- Review BIA questionnaires
- Conduct follow-up interviews to validate information and fill any information gaps

Recovery Strategies
- Identify and document resource requirements based on BIAs
- Conduct gap analysis to determine gaps between recovery requirements and current capabilities
- Explore recovery strategy options
- Select recovery strategies with management approval
- Implement strategies

Plan Development
- Develop plan framework
- Organize recovery teams
- Develop Relocation Plans
- Write business continuity and IT disaster recovery procedures
- Document manual workarounds
- Assemble plan; validate; gain management approval

Testing & Exercises
- Develop testing, exercise and maintenance requirements
- Conduct training for business continuity team
- Conduct orientation exercises
- Conduct testing and document test results
- Update BCP to incorporate lessons learned from testing and exercises

DHS – Ready.Gov
Going for Help

- FBI Internet Crimes Complaint Center (IC3): https://www.ic3.gov/default.aspx
- The Cybersecurity and Infrastructure Security Agency (CISA)
- State Patrol and Local Police
- Your bank & insurance
Security Careers / Certifications

https://www.cyberseek.org/
Heat Map &
Career Pathway
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.
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/