SESSION ID: TECH-R02

CYBERSECURITY TIPS, TOOLS AND TECHNIQUES FOR ALL SECURITY PROFESSIONALS

Ron Woerner
IT Risk and Compliance Consultant
DirectDefense
@ronw123
Poll the Audience

- Session ID: TECH-R02

- Do you have a USB drive on you?
  - Yes
  - No

Poll the Audience

- Session ID: TECH-R02

- When were you last asked to fix someone's computer?
  - < 1 week
  - < 1 month
  - < 3 months

CyberSecurity Consultant / Trusted Advisor for DirectDefense
Adjunct Professor, Bellevue University
25+ years experience in IT / Security
CISSP, CISM, CEH, BS-A
Blogger & writer
Given tons’o presentations on security and Internet safety
Thoughts are my own
Use at your own risk
Apologies in Advance for any broken links

Content as of February 2018
If you only remember 1 slide...

https://www.stopthinkconnect.org/

https://www.lockdownyourlogin.com/

https://www.dhs.gov/see-something-say-something
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.
Security Tools Tips Techniques
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 Art of Human Hacking
Google Hacking

Time Travel

- Google Cache

- Archive.org – Wayback Machine
Lists of tools, tips, & tricks

- OlderGeeks
- SecTools
- HowToGeek.com, Geek School
- The Geek Stuff (mostly Linux)
Security Awareness

- DHS Stop-Think-Connect
- NCSA Stay Safe Online
- Director of National Intelligence: https://www.dni.gov/index.php/resources/protecting-personal-information
Virtual Environments

- VMWare Player / Workstation
- Oracle VM VirtualBox
Cookie & Ad Blockers

- Firefox NoScript
- Ghostery
- Editthiscookie
- EFF Privacy Badger
- Sandboxie
- EFF – Privacy Badger
Forensics

- **OSForensics**
  - Licensed – free for home use

- **WinHex**
SysInternals Suite

- Autoruns
- Process Explorer
- Process Monitor

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, CtrlZCap, DebugView, Desktops, Disk2Vhd, DiskExt, DiskMon, DiskView, Disk Usage (DU), FFSDump, FindLinks, Handle, Hex2dec, Junction, LDMDump, ListDLLs, LiveKd, LoadOrder, LogonSessions, MoveFile, NotMyFault, NTFSInfo, PageDefrag, PendMoves, Pipeline, PortMon, ProcDump, Process Explorer, Process Monitor, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsList, PsLoggedOn, PsLogList, PsPasswd, PsPing, PsService, PsShutdown, PsSuspend, PsTools, RAMMap, RegDeNull, RegHide, RegJump, Registry Usage (RU), SDelete, ShareEnum, ShellRuns, Sigcheck, Streams, Strings, Sync, Sysmon, TCPView, VMMap, VolumeID, Whois, WinObj, ZoomIt

Download Sysinternals Suite (22.6 MB)
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

- **Using Windows PowerShell**
- **PowerShell.exe Command-Line Help**

```powershell
PowerShell[.exe]
    [-EncodedCommand <Base64EncodedCommand>]
    [-ExecutionPolicy <ExecutionPolicy>]
    [-InputFormat [Text | XML]]
    [-Mta]
    [-NoExit]
    [-NoLogo]
    [-NonInteractive]
    [-NoProfile]
    [-OutputFormat {Text | XML}]
    [-PSConsoleFile <FilePath> | -Version <Windows PowerShell version>]
    [-Sta]
    [-WindowStyle <style>]
    [-File <FilePath> [<Args>]]
    [-Command { - | <script-block> [-args <arg-array>]
                 | <string> [[<CommandParameters>]] ] ]

PowerShell[.exe] -Help | -? | /?
```
System Inventory & Automation

**PDQ Inventory & Deploy**
https://www.pdq.com/

**Ansible**
https://www.ansible.com/
Patching & Updating

Ninite (https://ninite.com/)
Patching & Updating

BatchPatch

(https://batchpatch.com/)

Chocolatey

(https://chocolatey.org/)
Network Evaluation

Introduction video

- TcpDump
Network Evaluation

Nmap / ZenMap
Network Evaluation

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Device</th>
<th>Mac Address 1</th>
<th>Mac Address 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.1</td>
<td>Router</td>
<td>Netgear</td>
<td>00:18:4D:CC:BB:F5</td>
</tr>
<tr>
<td>192.168.0.5</td>
<td>Desktop</td>
<td>Apple</td>
<td>00:17:F2:97:4A:5A</td>
</tr>
<tr>
<td>192.168.0.12</td>
<td>Printer</td>
<td>HP</td>
<td>00:0E:7F:96:03:27</td>
</tr>
<tr>
<td>192.168.0.13</td>
<td>TV</td>
<td>Samsung</td>
<td>00:12:FB:5C:93:C1</td>
</tr>
<tr>
<td>192.168.0.14</td>
<td>iPHONE</td>
<td>Apple</td>
<td>04:1E:64:45:4A:53</td>
</tr>
<tr>
<td>192.168.0.15</td>
<td>Laptop</td>
<td>Sony</td>
<td>00:13:A9:5C:93:C2</td>
</tr>
<tr>
<td>192.168.0.20</td>
<td>iPod</td>
<td>Apple</td>
<td>04:1E:64:45:4A:54</td>
</tr>
<tr>
<td>192.168.0.22</td>
<td>iPad</td>
<td>Apple</td>
<td>04:1E:64:45:4A:55</td>
</tr>
<tr>
<td>192.168.0.23</td>
<td>Media Player</td>
<td>TiKV</td>
<td>00:12:FA:6C:90:C1</td>
</tr>
<tr>
<td>192.168.0.40</td>
<td>Console</td>
<td>Sony</td>
<td>00:13:A9:5C:93:C0</td>
</tr>
<tr>
<td>192.168.101</td>
<td>PC Julius</td>
<td>Dell</td>
<td>00:12:3F:00:AF:01</td>
</tr>
<tr>
<td>192.168.102</td>
<td>IP Phone Home</td>
<td>Dell</td>
<td>00:12:3F:00:AF:02</td>
</tr>
<tr>
<td>192.168.103</td>
<td>Laptop Porta</td>
<td>HP</td>
<td>00:13:21:0D:FA:01</td>
</tr>
<tr>
<td>192.168.104</td>
<td>Fax&amp;Copy</td>
<td>HP</td>
<td>00:13:21:0D:FA:02</td>
</tr>
<tr>
<td>192.168.106</td>
<td>Mobile Flavius</td>
<td>Apple</td>
<td>04:1E:64:45:4A:59</td>
</tr>
<tr>
<td>192.168.113</td>
<td>Webcam</td>
<td>Dell</td>
<td>00:12:3F:00:AF:03</td>
</tr>
<tr>
<td>192.168.114</td>
<td>PC Augustus</td>
<td>Dell</td>
<td>00:12:3F:00:AF:04</td>
</tr>
<tr>
<td>192.168.120</td>
<td>Laptop Cicero</td>
<td>HP</td>
<td>00:13:21:0D:FA:04</td>
</tr>
<tr>
<td>192.168.121</td>
<td>Laptop Calpurnia</td>
<td>HP</td>
<td>00:13:21:0D:FA:05</td>
</tr>
</tbody>
</table>
Encryption

- **7-Zip**
- **AES Crypt**
- **Office 365**
Password Vaults

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

Tails

https://tails.boum.org/

Tor

DuckDuckGo
Proxy Resources

- **Anonymouse**: This service allows you to surf the web without revealing any personal information.
- **250 Working Proxies**: the biggest list I've ever seen of anonymous proxies.
Security Testing

- OWASP Zed Attack Proxy *(ZAP)*
- Portswigger Burp Suite
- GuardiCore Infection Monkey
- Metasploit
Kali Linux

- Kali Linux is a Debian-derived Linux distribution, designed for digital forensics and penetration testing.
- Kali Linux is preinstalled with numerous penetration-testing programs.
- Kali Linux can be run from a hard disk, live CD, or live USB. It is a supported platform of the Metasploit Project's Metasploit Framework, a tool for developing and executing security exploits.
"the quieter you become, the more you are able to hear"
Social Engineering Toolkit (SET)

There is a new version of SET available.
Your version: 7.3.12
Current version: 7.3.16

Please update SET to the latest before submitting any git issues.

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

99) Return back to the main menu.
Cheat Sheets


Finding People

- Google
- LinkedIn
- Peek You - www.peekyou.com
More Lists

- Sectools.org
- Tools Watch— Top Security Tools
- SANS Twenty Critical Security Controls
- Lifehacker
- HowToGeek
- Eric Ligman Collection of FREE Microsoft eBooks
  - 2014, 2015, 2016, 2017
Checklists

- **NIST**
  - Publications: [http://csrc.nist.gov/publications/PubsSPs.html](http://csrc.nist.gov/publications/PubsSPs.html)
  - Baldrige Cybersecurity Excellence Builder

- **U.S. Cyber Consequences Unit (US-CCU)** Cyber Security Matrix
What else?
“Apply” Slide

Immediate
- Pick 1 or 2 tools
- Play / Try it out / Experiment

Next 3 mos.
- Review this slide deck
- Pick more tools (3-5)
- Experiment with tools in a virtual environment
- Review the awareness websites

Share!
Questions???
I have no special talents. I am only passionately curious.

- Albert Einstein

HOMEWORK
Get out and play
Ron Woerner, CISSP, CISM
rwoerner @ directdefense.com
Twitter: @ronw123

By working together and helping each other, we all become stronger