24 For 24
24 Things to Know/Try for a Better 2024

January 17, 2024

By Aaron Grothe
NEbraskaCERT

Introduction

24 for 24?

I did a 12 for 12 talk in 2012 and have just kept going from there. Used to say I was in a rut now describe it as a groove.

Links are at the end of the talk
Slides are posted at the NEbraskaCERT website
http://www.nebraskacert.org/csf

Introduction (Continued)

If you have questions/comments please feel free to ask them anytime. You don't have to hold them until the end of the talk.

If there are other resources similar to these that you think might be useful to people please let the group know.

Hopefully this will be an interactive and productive session.

Tip - BlackCat Ransomware

BlackCat Ransomware Criminal decides to extort ransomware victim's customers

BlackCat has managed to exfiltrate 265GB of data from the accounting software company Tipalti

Since Tipalti's cyberinsurance doesn't cover extortion the BlackCat ransomware group has announced they will be directly contacting Tipalti's customers to attempt to get payment

Tip - BlackCat Ransomware.

Why this matters:

This is a new attack vector from Ransomware people. Not really, that successful apparently.

BlackCat have attempted to go after customers including Roblox and Twitch.

Roblox and Twitch have both said they haven't had any infiltration.

Tip - Medicat - USB.

Medicat is a toolkit with a bunch of tools for computer diagnostics and recovery tools

Uses Ventoy to combine a lot of Windows live images into an easy to use system

E.g. Anti-virus, Password recovery, and so on

Uses about 32gb of storage

Legality of the toolkit might be an issue

Tip - Wazuh

Wazuh - Free/Open Source XDR, SIEM Solution

What is Wazuh? Wazuh takes the OSSEC project and adds an OpenSearch backend to it.

Wazuh has agents for Windows/Mac OS X and Linux.

Has profiles for things like HIPPA/PCI and others.

Very nice little SIEM, highly recommend giving it a spin.

Tip - Wazuh.

Project I'm thinking about working on with it is as follows:

1. Create a Wazuh server in a VPS system (Linode/Vultr/Digital Ocean) - hopefully for the $5/month size
2. Install agent on my parent's Windows 10 PC
3. Be able to verify that their PC is up to date with patches and so on

Might also consider going with the original OSSEC project for this as well

Tip - Microsoft Security Copilot

Microsoft Security Copilot is a ChatGPT AI Large Language Model

This is still in the Early Access Program and you have to be invited into the program

It uses components such as Microsoft Sentinel/Defender/Intune and other tools to ingest data into the system.

Te goal here is to be able to have a conversation about an attack and have it provide feedback.

Tip - Microsoft Security Copilot.

Potential conversation along the lines of the following:

User: We're seeing unusual traffic against our webserver from the following IPs - (list of ips). What should be our first steps to respond?

Copilot: You may want to block these IP addresses. Here is how you would do that.

Example of commands to block relevant IP addresses.

Tip - OpenSnitch

OpenSnitch

OpenSnitch is a linux program that monitors all outbound network connections and allows you to approve/disapprove them.

Example use: You've installed a new application on your linux box and you want to monitor what it attempts to communicate with.

OpenSnitch will monitor these activity and allow you to allow/not allow connections.

Tip - OpenSnitch.

OpenSnitch can be quite interactive. A lot of programs can open a lot of connections

There is a Mac OS X program named LittleSnitch that predates OpenSnitch. For Microsoft Windows there are similar programs named - netlimiter and Comonodo

OpenSnitch and the others can be helpful when trying to figure out the behaviour of a program

Tip - Movies for Hackers.

If there is anything Hackers really like it is a watch party for a horrible computer movie. Phrases that are part of my vocab:

"Hack the Planet"
"I'm Sorry I can't do that Dave"

And so on

This site lists most of the movies I know and is broken into Thrillers/Drama, Action/SF, Documentaires and so on

Also has a section for TV Shows

Tip - False Claims Act

Aerojet Rocketdyne agrees to pay $9 million to resolve false claims act allegations

Aeroject Rocketdyne suit alleged the they made false claims about their cybersecurity status by not disclosing the full extent of Aerojet's noncompliance with the DFARS and NASA FARS clauses

Disclosures to DoD agencies "softened," the state of Aerojet's noncompliance or were cherrypicked, which resulted in omissions of information that the government would want to know to make assessment about the safety of its information

Tip - False Claims Act.

Why this matters?

The fact that FCA is going to be used in the Cybersecurity space for punishing vendors who make false claims is an interesting change.

Out of this might come standards for how do you figure out what is a false picked or cherry-picked claims.

One thing to keep in mind is Aerojet Rocketdyne didn't admit guilt.

Tip - Executive Order for Cybersecurity

Executive Order for Cybersecurity 2023

Main points:

- Create an "energy star" type of system the public can see to see if software was developed securely
- Create baseline of security standards for developing software sold to the government
- Improve communication between the government and industry on security matters

Tip - Executive Order for Cybersecurity.

Why this matters?

- An “energy star” type of rating system might make it easier for end users to evaluate software
- The devil is in the details, executive orders have limited enforcement

Tip - Minimum Hospital Cybersecurity

Health & Human Services is supposed to be releasing draft rules in the next few weeks for Healthcare providers

- Will establish new enforcable standards for health care providers
- Establish basic network defenses
- Will create common/basic standard for healthcare providers

Tip - Minimum Hospital Cybersecurity.

Why this matters?

- Ransomware is getting nastier as the Blackcat item proves
- Any system that accepts Medicaid might have to work at complying with this
- Is removing funding from Healthcare providers the best solution

Tip - Chinese Loongon Chip.

Chinese's latest homegrown chip the Loongon chip is roughly equivalent to Intel's 10th gen 4-core processor

Currently high end chips from the AMD/Intel are classified and munitions have restrictions on sales to China

If China can create an equivalent chip it will be interesting to see if it possibly gets adopted by vendors for devices like Smart TV, Cars, and networking equipment

Can backdoors be built into the system. E.g. something like the Intel Management Engine?

Tip - MGM/Caesar Attack Analysis

The MGM Attack is having some analysis of how it happened being released.

Extreme simplification

- Social engineering attack, used LinkedIn to identify user
- Took about 10 minutes to get password reset and administrator access to Azure and Okta domains
- Suffered nearly a week of outages, $100milion of losses

Given the scope, this will be one to continue to follow

Tip - MGM/Caesar Attack Analysis

Few details of the Caesar Attack have been released

Extreme simplification

- Social engineering attack was done by the same group that did MGM attack
- Believed to have happened in a similar way
- Caesar paid the ransomware demands after negotiating the payment from $30 to $15 million
- Minimal disruption to business

Tip - MGM/Caesar Attack Analysis.

So do you pay Ransomware?

Will be interesting if more information comes out about the MGM and Caesar attacks

Tip - Thorium.

Want a version of Chromimum that goes up to 40% faster.

- Thorium is a customized version of Google's open source Chromium browser. It has a lot of optimizations in it.
- Claims to be the "fastest browser on earth"
- Lot of compiler optimizations in it and some other changes
- Proves that there is still a lot of room for speeding up browsers

Tip - Pentest Book.

Very nice freely available Pentest book

Covers all the major sections of typical pentest: Recon, Enumeration, Exploitation, Post Exploitation

Also has good info on Mobile attacks as well

Highly recommend the site. Whatever your level you'll probably learn something

Tip - Rawsec's CyberSecurity Inventory.

Rawsec's Cybersecurity Inventory has a lot of Cybersecurity tools listed on it

Including

Cryptography, Red Teaming, Reverse Engineering, CTF Platforms, Web Application Exploitation, Wireless, Digital Forensics, Code Analysis

Lot of information on the site

Tip - NSA Top Director Approved

Timothy Haugh's promotion to director of the NSA and U.S. Cyber Command was approved December 19th.

Why this matters

This promotion was being held up Senator Ron Wyden until the nominee answered several questions about NSA data collection policies

Main question: Does the NSA purchase publicly available information on U.S. citizens?

Tip - NSA Top Director Approved.

The U.S. Government has very strict rules on collecting information on citizens.

There however there is no restriction on the purchasing publicly available information about our citizens.

Potential sources: Google/Apple location information, any information shared with an app, etc.

Tip - SSH Keys Stolen

Passive SSH key recovery

In 2023 for the first time the private portion of SSH keys have been able to be recovered

Several important parts of this

- Closed source ssh implementations used didn't include openssh mitigations
- IPsec based
- RSA-keys only

Tip - SSH Keys Stolen.

Being able to recover SSH private keys is a big deal

While this is a very specific set of circumstances. What typically happens is that these attacks usually are generalized over time

Tip - Iranian Terrorists vs US Water.

Iranian Terrorist group CyberAv3ngers have attacked Israel designed programmable logic controllers (PLCs) used in multiple water systems in facilities across the US.

Major factors

- PLCs were accessible via the internet
- PLCs had the default password

Even in 2023, we're still hooking up devices to the internet with the default passwords :-(

Tip - Amazon Sidewalk Network.

If you've got an Amazon Echo or Ring device you might already be a part of this network.

- The network in 900mhz Lora, and bluetooth
- Is a mesh network

Is being mostly designed for environmental and physical security currently, but what are the limits?

Tip - 7 Minute Security Podcast.

Seven Minute Security Podcast is a 7 minute podcast about computer security.

Is a good fast security podcast

Some of the recent topics

- How to build an intentionally vulnerable SQL server
- Tales of Pentest Pwnage (ongoing series, up to #52)
- Monitoring your tailscale network with uptime Kuma

Tip - OpenELA - Enterprise Linux.

Redhat has redone CentOS so it is no longer a no-cost, no-support equivalent to Redhat Enterprise OS.

They have also started enforcing their contracts to prevent people with RHEL licenses from sharing their code.

OpenELA is a group formed by Oracle, Suse and CIQ to help make sure that the source code of an enterprise distribution remains available.

Other groups: Rocky, AlmaLinux and others are doing other things to try and keep in sync with RHEL.

Tip - Post Open Source?

Register interview with Bruce Perens about what comes next for Open Source.

2023 was a rough year for Open source

- Redhat enforcing additional contractual requirements for RHEL
- Hashicorp migrating to Business Source License
- Sentry moving to the Functional Source License

Perens talks about trying to create an equitable way to pay for Open Source licenses

Tip - Open Source Licenses?

Going to close out with Four "Open Source Licenses" that are on the Rise.

1. Business Source License
2. AGPL with CLA
3. Functional Source License
4. Elastic License

About 25 years ago there were a lot of semi-open source licenses before it turned into the main ones we use today: GPL, AGPL, BSD, MIT, Apache 2.0 License

Tip - Business Source License (BSL)

Business Source License

Created by (David Axmark and Michael Widenius) of MariaDB

- Provides access to the product code for modification, distribution, etc.
- Requires a commercial license by anyone making production use of their software

Other companies have begun to adopt this license such as Hashicorp

Tip - AGPL with CLA

The Affero General Public License (AGPL) with Contributor License Agreement (CLA).

The AGPL is designed to address the Application Service Providers (ASP) loophole. E.g. Cloud vendor can use a piece of software without sharing any of the modified source code.

The AGPL requires vendors to make these code changes available.

Tip - Functional Source License.

Some of the interesting features

- After two years the license for the software switches to either Apache 2.0 or MIT
- Question of how you deal with vulnerabilities
- Created by Sentry application monitoring software

Tip - Elastic License

Used by Elastic to license their Elastic Search software

Interesting points

- Prevents use of software in a hosted or managed service, where the user is provided access to any "substantial set of the features or functionalities of the software"
- You can't bypass any license key functionality in the software

AWS forked the last version of Elasticsearch into a new project named Opensearch

Summary

So that is 24 for 24. Have a couple of themes this year

- Cybersecurity is getting a higher profile in the government
  - Energy star system might be interesting
  - False Claims Act
- We're still using default passwords, and accounts in 2023/2024
- Licensing is going to be getting a lot more interesting in 2024
  - Companies are working to deal with hosting companies using their software
  - Companies are trying to make money on their software
- 2024 is going to be an interesting year

Links

Tip - BlackCat Ransomware

- https://gridinsoft.com/blogs/tipalti-roblox-twitch-hacked/
- https://www.theregister.com/2023/12/05/alphvblackcat_shakes_up_tactics_again/

Tip - Medicat - USB

- https://medicatusb.com/

Links

Tip - Wazuh

- https://www.wazuh.com
- https://www.grothe.us/presentations/olug-202311-wazuh.pdf

Tip - Microsoft Security CoPilot

- https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-security-copilot
- https://www.theregister.com/2023/03/28/microsoft_security_copilot/

Links

Tip - OpenSnith

- https://github.com/evilsocket/opensnitch
- https://www.obdev.at/products/littlesnitch/index.html
- https://www.comodo.com/
- http://www.netlimiter.com/

Tip - Movies for Hackers

- https://github.com/k4m4/movies-for-hackers

Links

Tip - False Claims Act

- https://www.theregister.com/2022/11/01/openssl_downgrades_bugs/

Links

Tip - Executive Order for Cybersecurity

- https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-improving-nations-cybersecurity#:~:text=The%20EO%20will%20improve%20the,making%20security%20data%20publicly%20available.
- https://www.cisa.gov/sites/default/files/2023-02/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks-508c.pdf

Links

Tip - Hospital Minimum Cybersecurity

- https://www.theregister.com/2024/01/10/us_hospitals_security_rules/
- https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf

Links

Tip - Chinese Loongon Chip.

- https://www.tomshardware.com/news/loongson-unveils-32-core-cpu
- https://technode.com/2023/11/29/loongson-3a6000-cpu-allegedly-equivalent-to-intels-10th-gen-4-core-processor/

Links

Tip - MGM/Caesar Attack Analysis

- https://westoahu.hawaii.edu/cyber/global-weekly-exec-summary/alphv-hackers-reveal-details-of-mgm-cyber-attack/#:~:text=Executive%20Summary&text=The%20hacker%20groups%20used%20social,%2C%20slot%20machines%2C%20and%20websites.
- https://thenewstack.io/mgm-hack-analysis-security-still-a-test-of-your-weakest-link/
- https://www.theregister.com/2023/12/28/casino_ransomware_attacks/

Links

Tip - Thorium

- https://www.thorium.rocks

Pentest Book

- https://pentestbook.six2dez.com/

Links

Tip - Rawsec's CyberSecurity Inventory

- https://inventory.raw.pm/tools.html

Tip - NSA Top Chiefs position held up over Government buying personal data

- https://www.theregister.com/2023/12/02/nsa_held_hostage/
- https://www.politico.com/news/2023/11/30/wyden-block-senate-vote-nsa-cyber-command-00129432

Links

Tip - SSH Keys Stolen

- https://arstechnica.com/security/2023/11/hackers-can-steal-ssh-cryptographic-keys-in-new-cutting-edge-attack/

Tip - Iranian Terrorists vs US Water

- https://www.theregister.com/2023/12/04/iran_terrorist_us_water_attacks/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

Links

Tip - Amazon Sidewalk Mesh Network

- https://www.theregister.com/2023/03/28/amazon_sidewalk_mesh_network/

Tip - 7 Minute Security Podcast

- https://7ms.us/

Links

Tip - OpenELA - Enterprise Linux

- https://openela.org/faq/

Tip - Post Open Source

- https://www.theregister.com/2023/12/27/bruce_perens_post_open/

Links

Tip - Business Source License

- https://www.theregister.com/2023/08/11/hashicorp_bsl_licence/
- https://www.theregister.com/2023/10/19/hashicorp_ceo_license_changes/

Tip - AGPL with CLA

- https://en.wikipedia.org/wiki/Affero_General_Public_License

Links

Tip - Functional Source License

- https://blog.sentry.io/introducing-the-functional-source-license-freedom-without-free-riding/

Tip - Elastic License

- https://www.elastic.co/licensing/elastic-license