FIRST DRAFT OF 25 For 25

25 Things to Know/Try for a Better 2025

January 15, 2024

By Aaron Grothe
NEbraskaCERT

Introduction

25 for 25?

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 - Bindiff.

Bindiff is a very nice diff tool for showing the differences between disassembled code

It is being used by a lot of people along with Ghidra and/or IDA pro to reverse engineer patches that come out from Vendors

Used by VxSig to automatically generate AV byte signatures from similar binaries

Tip - Diffoscope.

Diffoscope is a tool that can tell you the differences between two things.

Potential use cases

- Want to know what changed in a ISO image between builds
- Differences between two folders of PDFs
- DIfferences between your incremental backups

Used by reproducible builds project

Tip - Reproducible Builds.

Reproducible builds are simply that you can compile a program and I can compile a program and get the same checksum.

The Debian, NixOS and Arch Linux projects are all working on this.

Reproducible builds will help make sure that nothing has changed in a program from what was generated by your vendor.

This is a big part of efforts to secure the Software Build of Materials (SBoM)

Tip - Safe C++.

Memory Safety for C++???

Safe C++ is a working group going through C++ to work at creating a Memory Safe C++ variant.

Lot of production code is in C++ and if they can come up with a migration path. It might really help them out.

Groups such as the NSA have suggested migrating away from C++ to memory safe languages such as Rust.

Tip - arcX Cyber Threat Intelligence.

Cyber Threat Intelligence 101 Course is currently available for Free.

Is a good little certification you can get done in an afternoon.

Has a nice title and the training is pretty good.

Tip - Bython.

- Almost everybody loves python
- Not everybody loves whitespace

Solution

Python with braces

```
def print_message(num_of_times) {
    for i in range(num_of_times) {
        print("Bython is interesting!");
    }
}
```

Tip - OneFileLinux.

OneFileLinux is a one file linux distribution that fits inside 20mb

Most UEFIs have 100mb of space and are usually half filled

You install this distribution into the EFI system partition and boot

- Doesn't appear in your filesystem
- Since the EFI partition isn't encrypted can theoretically be installed on systems with disk encryption turned on

Will leave the potential to install a covert operating system up to the user.

Tip - Cosmopolitan.

Cosmopolitan makes C a build-once run-anywhere language

Cosmopolitan - modifies the GCC and CLANG compilers to generate a single executable.

This executable will run natively on Linux, Mac, Windows, FreeBSD, OpenBSD, NetBSD, and BIOS for AMD64, and ARM64

Does quite a bit of trickery with the executable to have each represent it.

Tip - Llamafile.

This takes Cosmopolitan and combines it with an LLM into a single executable.

Great way to try out a LLM or create a pocketable AI demo

They have a handful of models ready to go.

Tip - Molmo.

Smaller than most of the commercial models.

Using human annotations to augment the dataset

Multi-modal - text, graphics

MIT license

Interesting to see how it will compare to other models such as Mistral and Llama3.x

Tip - Mandiant - North Korea Hackers.

Hackers from North Korea are applying for and getting IT remote working jobs in the US and England.

Sometimes they have an agent in the country who will host the laptop and help them appear to be in the US.

Goals for the North Koreans

- Hard currency
- Chance to infiltrate systems and put in long term backdoors

Tip - NIST - Post Quantum Standards.

Quantum computing is happening anytime between the next 5 and 50 years

There are reports that the Chinese and others are saving off large amounts of data for later decryption

NIST has approved three post encryption quantum standards

Tip - The Moon is a Harsh Mistress.

A classic book.

- Its description of AI was one of the first.
  - It is a benevolent AI that helps with the revolution
- Popularized TANSTAAFL ("There Ain't No Such Thing As A Free Lunch")
- Also had the concept of Rational Anarchy
- If you haven't read it highly recommend it
- Robert Heinlein was bit right leaning, and it is a book of its time

Tip - PyPi Revival

How this one works

- Someone removes a package from the PyPi repository
  - Maintainer may have retired
  - Maintainer may have changed project name, etc.
- A hacker creates a new project with the same name
- People start downloading and getting hacked
- JFrog is reserving these packages to prevent that from happening

Tip - Bookmark Knocking.

Interesting project that allows you to create bookmarks that you can hit in a specific order to open a "hidden" bookmark.

Shows what can be done with Javascript and bookmarks. Potentially useful for people who need to hit an emergency site.

How it works

- Select a couple of URLs
- Save them to your browser
- Click them in order to hit hidden "site"

Tip - Pollyfill.io

Polyfill.io was a library that allowed older web browsers to emulate newer features.

Polyfill.io sold their website and github assets to China-based company Funnull

They then began to serve malware from it

For a brief period of time over 250,000 websites were linking to Pollyfill.

Tip - Project Naptime.

Google's Project Zero is an LLM to do basic Vulnerability research.

- Generates Python code for simple exploits
- Early days, but will keep getting better

It is going to get to the point where it can be a force multiplier for security researchers looking simple exploits

Tip - Traceshark.

Traceeshark is a tool that allows you to perform system traces dump them into a file and then use wireshark to analyze them.

One of the biggest issues with doing system traces is analyzing the data. Wireshark excels at this. So it is a very cool design.

If you're doing malware analysis this tool could be worth it.

Tip - AWS Kill Switch.

AWS Kill Switch is a project that can allow you to quickly lock down your AWS environment

Can lock down AWS Account and IAM roles during a security incident

E.g. you believe improper data has been uploaded to an S3 bucket. AWS Kill Switch, can pull all S3 access across your account while you figure things out.

Tip - Logging Made Easy

Logging Made Easy (LME) is a tool from CISA for Windows boxes that provides a simple log management system.

It isn't a SIEM. Could be quite useful for a SOHO environment

If you don't have a SOC, SIEM or another monitoring solution. LME can help provide you a basic level of auditing.

Tip - Logging Made Easy.

From their github page

- Show where administrative commands are being run on enrolled devices
- See who is using which machine
- In conjunction with threat reports, it is possible to query for the presence of an attacker in the form of Tactics, Techniques and Procedures (TTPs)

Still very early in development

Tip - NetAlertX.

Tool that can detect when new or unknown wifi devices pop onto your network and can alert you to that via telegram, email and other methods.

Know when your home network or soho has new things popping onto your network

Can give you a heads up when things start to get interesting.

Think running ndiff on your network regularly is probably better, but this has a nice gui

Tip - Sshamble.

Can identify misconfigurations in ssh settings.

Can also do some cool auditing things.

Scenario. Bill leaves the company

- Go through all the machines and see if there are any public keys that Bill could use to get back into a machine
- Can also be used to figure out other misconfigurations as well

Tip - LLMs hallucinating .

Large Language Models tend to hallucinate package names when you ask them to generate code for example.

E.g. it can tell you to import packages that don't exist

These names are generated in a semi-predictable way

Given that attackers can create these packages, insert malware and people will download them.

Largely an NPM/PyPi issue

Tip - Mystery Linux 9.9 CVE - its Cups.

The week of September 23rd there was an announcement

A 9.9 CVE that is remotely exploitiable and is in nearly every version of Linux will be receiving a patch

Given the overall description it sounded like the apocalypse. Assumptions ran wild. Would it be over something to do with SSH? Would it be related to some other utility that is accessible to most Linux systems connected to the internet.

Tip - Mystery Linux 9.9 CVE - its Cups.

Once it came out. The issue was with CUPs the printing system for Linux.

Most people don't have CUPs exposed to the internet so not quite the issue that it was described as.

That being said it was a 9.9 and if you had CUPS on your local network, most people do it was a heck of an attack vector.

Summary

Time to revisit my predictions for 2024.

- 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

Summary

So that is 25 for 25. Time for my 2025 Predictions

- Cybersecurity positions will be augmented by AI more than ever before
  - Security Copilot from Microsoft is pretty interesting
  - AI LLMs are getting more and more powerful and cheaper for companies to implement their own private AI
- There will be a Cyber Attack / Ransomware attack that will have some loss of life (not one I'm thrilled with)
- 2024 is going to be an interesting year

Links

Tip - Bindiff

- https://www.helpnetsecurity.com/2023/09/25/bindiff-open-source-comparison-tool-for-binary-files/
- https://github.com/google/bindiff

Links

Tip - Diffoscope

- https://diffoscope.org/

Links

Tip - Reproducible Builds

- https://reproducible-builds.org/
- https://en.wikipedia.org/wiki/Reproducible_builds

Links

Tip - Safe C++

- https://www.theregister.com/2024/09/16/safe_c_plusplus/
- https://safecpp.org/P3390R0.html

Links

Tip - arcX Cyber Threat Intelligence

- https://arcx.io/courses/cyber-threat-intelligence-101

Links

Tip - Bython

- https://github.com/mathialo/bython
- https://news.ycombinator.com/item?id=39665905

Links

Tip - OneFileLinux

- https://github.com/zhovner/OneFileLinux
- https://www.theregister.com/2024/09/09/onefilelinux_esp_distro/

Links

Tip - Cosmopolitan

- https://github.com/jart/cosmopolitan

Links

Tip - Llamafile

- https://github.com/Mozilla-Ocho/llamafile
- https://future.mozilla.org/builders/news_insights/introducing-llamafile/

Links

Tip - Molmo

- https://molmo.org/
- https://www.wired.com/story/molmo-open-source-multimodal-ai-model-allen-institute-agents/

Links

Tip - Mandiant - North Korea Hackers

- https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat/
- https://www.theregister.com/2024/09/24/mandiant_north_korea_workers/

Links

Tip - NIST - approves post quantum encryption standards

- https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

Links

Tip - PyPi Revival

- https://jfrog.com/blog/revival-hijack-pypi-hijack-technique-exploited-22k-packages-at-risk/

Links

Tip - Bookmark Knocking

- https://jstrieb.github.io/projects/hidden-bookmarks/

Links

Tip - Polyfill

- https://arstechnica.com/security/2024/07/384000-sites-link-to-code-library-caught-performing-supply-chain-attack/
- https://sansec.io/research/polyfill-supply-chain-attack

Links

Tip - Naptime

- https://googleprojectzero.blogspot.com/2024/06/project-naptime.html

Links

Tip - Traceeshark

- https://github.com/aquasecurity/tracee
- https://github.com/aquasecurity/traceeshark

Links

Tip - AWS Kill Switch

- https://www.helpnetsecurity.com/2023/11/27/aws-kill-switch-open-source-incident-response-tool/
- https://github.com/secengjeff/awskillswitch

Links

Tip - Logging Made Easy

- https://www.helpnetsecurity.com/2023/10/30/logging-made-easy-lme-free-log-management/
- https://github.com/cisagov/LME

Links

Tip - NetAlertX

- https://www.helpnetsecurity.com/2024/09/25/netalertx-open-source-wi-fi-intruder-detector/
- https://github.com/jokob-sk/NetAlertX

Links

Tip - Sshamble

- https://www.helpnetsecurity.com/2024/08/08/sshamble-test-ssh-services/
- https://github.com/runZeroInc/sshamble
- https://www.runzero.com/sshamble/

Links

Tip - LLMs hallucinating Package names

- https://www.theregister.com/2024/09/30/ai_code_helpers_invent_packages/
- https://www.theregister.com/2024/03/28/ai_bots_hallucinate_software_packages/
- https://arxiv.org/abs/2406.10279

Links

Tip - Mystery Linux 9.9 CVE - its Cups

- https://www.theregister.com/2024/09/26/cups_linux_rce_disclosed/
- https://securityintelligence.com/news/fysa-critical-rce-flaw-in-gnu-linux-systems/