22 For 22
22 Things to Know/Try for a Better 2022

January 19, 2022

By Aaron Grothe
NEbraskaCERT

Introduction

22 for 22?

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 will be 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 - Missouri Governor accuses newspaper of hacking

Newspaper journalists found a simple data disclosure on a department of education website. It was retrieving full Social Security Numbers, but only displaying the last 4 digits.

The journalists discovered this by accessing the html source code for the website

The journalists notified the correct authorities and the flaw was soon remediated..

After the flaw was fixed they reported on it

Tip - Missouri Governor accuses newspaper of hacking.

The Governor has announced that they will be prosecuting the journalists for participating in a multi-stage process to access and download at least 3 educators information.

"They had no authorization to convert and decode the code."

If F12 is criminalized only criminals will have F12

Tip - Hospital sued after baby dies during Ransomware attack

During a ransomware attack a hospital was unable to use their networked computers and were forced to use paper forms.

Because of this it appears the correct people were not notified which they would have been had the network system been up.

Because of this a child in ICU died.

Tip - Hospital sued after baby dies during Ransomware attack.

Child's mother says she would not have admitted her child to the hospital if they knew they were having computer issues.

From a screenshot submitted during the lawsuit:

"I need u to help me understand why I was not notified,"

Tip - Security through obsolescence

Interesting story of Pen Testers trying to hack the Inflight Entertainment (IFE) system.

Most modern attack vectors and pen testing tools were unavailable. RDP didn't exist for NT4 :-) other tools such as cscript are also unavailable

Ended up using CVE-1999-1011 and old MDAC (Microsoft Data Access Components) exploit

Tip - Security through obsolescence.

Got access through metasploit tftp server and cracked admin password.

This brings up an interesting question is there a point where having an obsolete system is worth it.

Many years ago when NEbraskaCERT actually held PCI information we ran a custom Linux on a Dec Alpha. The goal to make people work for it :-)

Tip - Rig - random identity generator.

Random Identity Generator - simple utility to generate an identity for signing up for stuff online

grothe@project:~/debian/tmobile$ rig

Addie Sargent
237 Shalton Dr
Dallas, TX 75260
(214) xxx-xxxx

Can use -f/-m flag for gender of generated identity, -n will give you the number of addresses.

Tip - AWS CUR - AWS Cost and Usage Report.

If you're using AWS make sure you have this enabled.

You setup an s3 bucket and you enable this service.

It provides a lot more detail about how you're using AWS.

Helps if you have decent tags on your information.

Can integrate with Amazon Athena, Amazon Redshift, or Amazon QuickSight to be able to do queries on your system.

If you've got AWS ask to see one for your department's assets.

Tip - Double free example How to exploit a double free.

Very nice example of how to exploit a double free attack.

Author titles it "Use-After-Free for dummies"

A great writeup. Their example uses a raspberry pi, but can be adapted to x86 pretty easily.

If you ever wanted to know more about this or be able to do a demo, highly recommend this one.

Tip - Github awesome "topic".

Thanks to Chad Homan for this one.

Simply google "github awesome <topic>" and you'll probably find a good page of links/information about almost any topic.

E.g. "github awesome waf", "github awesome honeynet", "github awesome docker", etc.

Quality of the github pages varies a biit, but is a great place to get more information about a topic.

Tip - LANtenna - Side Channel through ethernet cable

Interesting paper talking about using the ethernet cables that a device is connected through to create a covert channel.

Last year talked about project to switch internet speeds as a covert channel.

Used two methods of generation

Network speed toggling
UDP packet transmissions

Tip - LANtenna - Side Channel through ethernet cable.

The bandwidth of this attack is pretty low but the possibility is interesting.

There are options to work around this as well.

- Detection of network speed toggling/udp packet transmission
- Signal monitoring/Jamming
- Shielding ethernet cables - secure routing trays

Tip - Close but not quite - Apache 2.4.50/Apple Finder Fix

Making patches is hard. Here are two examples

Apache 2.4.50 “fixed” a critical path transversal and remote code execution in 2.4.49

Turns out it didn’t handle all the cases and permutations and Apache had to issue another update 2.4.51 shortly thereafter because of aliases

Tip - Close but not quite - Apache 2.4.50/Apple Finder Fix.

Once a patch is released hackers will be reverse engineering the patch to look for edge cases.

David Litchfield has made quite a career of submitting an Oracle bug, waiting for Oracle to release a fix then submitting a very similar Oracle bug and repeat.

Creating a bug fix that has fixes the bug and doesn't break anything can be quite challenging.

Tip - Microsoft Agent - No, No, you do the patching

When you deploy a Linux Azure VM and enable some Azure functionality Microsoft automatically installs their OMI agent without the user being aware.

There were 4 Remote Code Exploits against the OMI - ranging from 7.0 to 9.8 (ouchie)

Microsoft did not automatically patch these systems for the users at first. The user was responsible for patching these systems instead,

Tip - Microsoft Agent - No, No, you do the patching.

Even worse the images still had the bad version of OMI in them initially. So any user deploying a new Linux VM that had OMI was vulnerable.

Even worser. You had to add the MS repos to your system if they weren't already there and update the system.

Microsoft has resolved this, but still it goes to show you that the cloud is in some ways still a wild place where the shared responsibility model is being evolved.

Tip - Windows Subsystem for Linux 2.0

Microsoft has made some interesting changes to WSL in the 2.0 version

- Have moved from being a windows feature to being installed through Microsoft store, so hopefully faster updates
- Able to run gui linux applications on a windows box without needing to install an X11 server
- Runs a linux kernel internally instead of just mapping calls to Windows so much more compatible

Tip - Windows Subsystem for Linux 2.0.

Brings its Linux compatibility pretty well up to spec. Linux distros such as Debian, Kalii, and SUSE and others are available through the Microsoft Store

One caveat, currently you can't run Windows 11, WSL and VirtualBox together. Hope this is resolved soon,

Tip - Ubuntu Micro Cloud.

Ubuntu Micro Cloud combines LXD, MAAS, Ceph, and Kubernetes to create the capability of deploying small clouds in remote areas.

Some examples of this are multiple hardened machines being deploy to factory floors, sensors, and so on.

Combining the above technologies together make for an interesting tech stalk.

Can be deployed on Raspberry PIs, other SBCs and also x86/x64 machines.

Tip - Microsoft release CBL mariner linux

Microsoft has created their own Linux distribution to be used in Azure.

Microsoft has also released their build tools and images so anyone can build the distro from scratch or run it locally.

Uses RPM for its package format

Interesting to see that Microsoft has go so far as to release their own distro. Granted it is made more for servers and containers, but is still a big step from Microsoft.

Tip - Razer Mouse hack.

When you plug in a Razer mouse or keyboard it automatically downloads and installs the Razer Synapse software.

If you intercepted the installation it would allow you to pick a folder from where to run the executable. Easy Peasy admin privileges.

Goes back to a question about the driver model that ships with Windows 10/11.

Other systems probably have same issue e.g. usb printers.

Tip - Xclicker - automate mouse clicking under Linux.

Sometimes you want to automate something without figuring out selenium or another macro recording/replay tool.

Xclicker lets you automatically click a location a number of times without user interaction.

Xclicker is distributed as an app image. Is based around x/y coordinates so you may need to run your apps full screen to work consistently.

Tip - Firefox relay - easy forwarding email accounts.

Firefox relay gives you 5 email forwarded accounts at any one time.

You can create/delete and stop accounts from forwarding email to.

Emails addresses will be in the form sds@relay.firefox.com

Note: doesn't work with all services.

Other options that are also useful are things like 10 minute email and so on.

Tip - SHElib - Homomorphic encryption Library/HELib

Homomorphic encryption allows you to modify entry in a file without knowing what the value is.

E.g. You have bank information from a user. You can update information like current balance by adding $200.00 to an account without knowing the actual value.

Provides the capability to share data with 3rd parties, they are able to modify it but they don't know the actual data.

Tip - SHElib - Homomorphic encryption Library/HELib.

The overhead of doing Homomorphic encryption along with concerns about its security have slowed its adoption.

SHElib is a library that simplifies experimenting with Homomorphic encryption making it is easier to use.

Tip - Goodbye Alice & Bob.

If you've ever done Public key cryptography you've probably seen examples using the terms Alice, Bob & Carol and a cast of others,

The University of Edinburgh is considering using new terms because of a desire to "decolonize" their Informatics curriculum

Still in early discussions, but is something people are discussing.

Tip - Bookmark knocking.

This one is just cool and potentially could save lives

You can hit a set of bookmark links in an order and it will hit a hidden bookmark.

The way it hides data at the end of the bookmarked URL is pretty interesting.

Tip - Bookmark knocking.

This can be useful if you're in a situation e.g. an abusive relationship and you need to hide information about a bookmark entry talking about services that deal with abuse.

It is similar to portknocking except it is for bookmarks.

Could probably use a bit more research on it to make sure it is safe, but a very cool idea.

Tip - Secure Software Development Fundamentals Courses.

The Open Source Security Foundation (OpenSSF) has made their secure development course available for free.

You can also pay to get the certification upon the completion of the course as well.

Is expected to take 5 months assuming you spend 1-2 hours a week on the coursework.

Looking through the curriculum looks to be pretty good with a lot of information about threat models.

Tip - Monitoring github configurations for security

Allstar is a github app that monitors the settings of your github repo to make sure that your settings are secure.

When installing it will ask for required permissions.

Allstar may be set to notify, open an issue or in some cases you can have it make changes to the repository or project toe enforce your security settings.

Tip - Monitoring github configurations for security.

E.g. of some of the checks

- Are binary objects present in the repo?
- Does the project have a security policy?
- Is the project maintained?
- Does project have unpatched vulnerabilities? Uses the OSV service for this

Another interesting piece of software from the OpenSSF project.

Tip - OpenSnitch

OpenSnitch is a tool for Linux systems that you can use to whitelist all connections that apps on your system attempts. You can then allow or deny each action.

This can be quite noisy so you can also have it just log the requests and review them later.

Very interesting because it allows you to see how many connections various applications open.

Tip - OpenSnitch.

Be careful if you run this in anything but logging as you'll spend a lot of time clicking accept.

Can also be useful if you're trying to see what apps on your system might be doing something nefarious.

Mac OS X - has a similar tool called Little Snitch that was written before OpenSnitch.

Tip - Cyber Mentor's Youtube Channel.

Cyber Mentor is the gentleman who runs TCM Security Academy. His youtube channel has a lot of good videos on it:

Examples

- Ethical Hacking in 12 Hours
- Learn OSINT in 4.5 Hours
- Become an Ethical Hacker for $0

TCM is the company offering Practical Network Penetration Tester (PNPT) certification as well.

Links

Tip - Missouri Governor accuses newspaper of hacking

https://gizmodo.com/missouri-governor-wants-to-prosecute-journalist-for-war-1847866414

https://www.rollingstone.com/politics/politics-news/missouri-governor-teacher-data-hacking-1242493/

Links

Tip - Hospital sued after baby dies during Ransomware attack

https://www.theregister.com/2021/10/04/in_brief_security/

Tip - Security through obsolescence

https://www.theregister.com/2021/05/21/boeing_747_ife_windows_nt4_shell_access/

Links

Tip - Rig - random identity generator

https://www.networkworld.com/article/3606570/random-identity-generation-in-linux.html

Tip - AWS CUR - AWS Cost and Usage Report

https://docs.aws.amazon.com/cur/latest/userguide/what-is-cur.html

Links

Tip - Double free example How to exploit a double free

https://github.com/stong/how-to-exploit-a-double-free

https://hackaday.com/2021/10/29/this-week-in-securityuse-after-free-for-dummies-wifi-cracking-and-php-fpm/

Tip - Github awesome "topic"

Search github awesome topic .e.g "github awesome docker"

Links

Tip - LANtenna - Side Channel through ethernet cable

https://arxiv.org/pdf/2110.00104.pdf

Tip - Close but not quite - Apache 2.4.50/Apple Finder Fix

https://httpd.apache.org/security/vulnerabilities_24.html?incomplete

https://www.theregister.com/2021/09/22/macos_rce_flaw/

Links

Tip - Microsoft Agent - No, No, you do the patching

https://www.theregister.com/2021/09/17/microsoft_manual_omigod_fixes/

Tip - Windows Subsystem for Linux 2.0

https://docs.microsoft.com/en-us/windows/wsl/about

Links

Tip - Ubuntu Micro Cloud

https://ubuntu.com/engage/micro-clouds

Tip - Microsoft release CBL mariner linux

https://www.computing.co.uk/news/4034680/microsoft-releases-cbl-mariner-linux-distribution-cloud-edge

https://github.com/microsoft/CBL-Mariner

Links

Tip - Razor Mouse hack

https://www.bleepingcomputer.com/news/security/razer-bug-lets-you-become-a-windows-10-admin-by-plugging-in-a-mouse/

Tip - Xclicker - automate mouse clicking under Linux

https://linuxiac.com/xclicker-linux-auto-clicker/

Links

Tip - Firefox relay - easy forwarding email accounts

https://relay.firefox.com/?utm_source=blog.mozilla.org&utm_medium=referral&utm_content=seo

Tip - SHElib - Homomorphic encryption Library/HELib

https://copr.fedorainfracloud.org/coprs/rrelyea/SHELib/

https://github.com/homenc/HElib

Links

Tip - Goodbye Alice & Bob

https://www.theregister.com/2021/10/15/computer_scientist_terminology/

Tip - Bookmark knocking

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

Tip - Secure Software Development Fundamentals Courses

https://openssf.org/training/courses/

Links

Tip - System for monitoring github configurations to make sure it is secure.

https://github.com/ossf/allstar

Links

Tip - OpenSnitch

https://github.com/evilsocket/opensnitch

https://www.obdev.at/products/littlesnitch/index.html

Links

Tip - Cyber Mentor's Youtube Channel

https://www.youtube.com/c/TheCyberMentor/videos

https://academy.tcm-sec.com/

https://www.thecybermentor.com/