19 For 19
19 Things to Know/Try for a Better 2019

by Aaron Grothe
Security+/CISSP/NSA
IAM/NSA IEM/CySA+/PenTest+

Introduction

19 for 19?

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.

Next year's 20 for 20 will probably be a recap of 20 of the all time best from the last 8 years :-)

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.

Kaggle Datasets

This is one of the first places to go looking for a dataset. They have thousands of them. People just drop various datasets they want to make available to the public:

Couple of examples

- Google Play Store Apps - lot of information about the top apps downloaded. Correlate with security notices and you've got yourself a really nice paper
- Compromised password list - list of passwords submitted to an open honeypot. Probably don't want to use

Kaggle Datasets.

Note: The license of the datasets can vary so please keep that in mind.

A lot of information and well worth a visit also really nice if you're looking for some data to upload into your Elasticsearch to play around with Kibana

AWS Artifacts

Amazon Web Services (AWS) Artifacts provides on demand downloads of compliance documents. E.g. AWS ISO Certification, PCI and SCO reports.

Quite simply this allows you to access documentation from Amazon to help you make sure you are in compliance with things such as HIPPA and PCI.

Have not used this yet. It however sounds massively interesting.

AWS Artifacts

E.g. You are going to be processing HIPPA information in AWS. You can enter into a Business Associate Addendum (BAA). You accept the BAA and designate an account for the access. AWS holds the relevant documentation and is used for the processing.

AWS artifacts can be used to review the terms and obligations of the agreement. It can also be used to handle the termination of the agreement if the need for it goes away at some future time.

AWS Artifacts.

Using AWS Artifacts does not remove the need for care

You may have to enter into an NDA with Amazon and be restricted in how you share the information.

However having the ability to point auditors to a portal and say go ahead and have fun sounds remarkably cool :-)

Also keep in mind only a matter of time until other cloud vendors will probably offer similar service.

Azure Sphere IoT

This one is very interesting because it is a Linux distribution from Microsoft for doing the Internet of Things.

Microsoft is releasing a reference platform for IoT devices that runs a custom version of Linux. Development boards are currently starting to trickle out.

Runs on a multi-core system reserves one core for running Security Monitor software on to maintain security/health of system.

Azure Sphere IoT

Why this matters?

The security reference monitor is mentioned often in computer security classes but is rarely implemented in a semi-independent manner like this.

It is Microsoft and Linux

It is getting the regular quality of documentation and tools that comes from Microsoft

Azure Sphere IoT.

Why this matters?

It is not fully Open Sourced. That being said there is a lot of documentation for the project and hopefully Microsoft will Open Source the rest of it.

Hopefully will be a bigger hit than the Zune/Windows RT/Windows ME/Microsoft TV/Spot Watches and of course Microsoft Bob

NITTF Training.

The National Insider Threat Task Force (NITTF) has made their Insider Threat Training course available over the internet

Why this is interesting

Gives you an idea of what some of the internal training inside our country currently looks like
Has some good information to consider including inside your own training programs
You might learn a few things
Also get a printable certificate when you finish

CLIP-OS

CLIP-OS is a Linux distribution being developed with support from the ANSSI (National Cybersecurity Agency of France)

It is being designed to a Multi-Level secure system. It restricts System Call access and a custom Linux Security Module to enforce the separation of different domains.

Will be able to run different security levels on the same machine. Compartmented Mode Workstation style or be able to have Unclassified and Secret in separate windows on same machine ideally.

CLIP-OS

What makes it interesting:

Similar in many ways to the idea of QUBES-OS except it isn't using virtualization for this task and is instead working on enhancing the Linux stack directly

It is French and that makes things interesting. They're taking different approaches in some areas to the ones we're accustomed to. Has been in development for over 10 years. New release is Phase 5.

CLIP-OS.

What also makes it interesting:

Is based on Gentoo :-)

It is Open Source so you can see what is going on :-)
Technically it has always been, but not widely distributed before.

DropBox VDP.

Dropbox has made all the text in their Vulnerability Disclosure Program (VDP) Freely Copyable.

Dropbox uses HackerOne to handle their Bug Bounty program. Still having the text for a VDP freely available (especially one vetted by a company the size of DropBox is nice).

Is very interesting ready to white/gray/black hat hackers as it has a lot of info in it. Such as what they might sue you for.

Biscuit - OS Kernel Written in Go

There have been several operating system kernels written in higher level languages

Microsoft has written Cosmos an O/S written in C#

Biscuit is a Posix compatible kernel written in the Go programming language

What makes this interesting is that it runs real programs such as ngnix, redis and others to be able to compare/contrast with the Linux and BSD kernels

Biscuit - OS Kernel Written in Go.

Ideally this would make it much harder to have memory access errors that are possible in lower level languages such as C and assembler

Performance overhead of about 15% for most things. Also the dreaded pauses when doing Garbage collection.

There have been a couple of papers and presentations about it. The Code is available at Github. Huge potential for future research in the area.

Joint Report on Publicly Available Hacking Tools

This is a report created by the Five Eyes Alliance (US, UK, Canada, Australia, New Zealand)

Short 20 page report provides a bit of information about commonly used tools

Remote Access Trojans JBiFrost
Web Shells: China Chopper
Credential Stealers: Mimikatz
Later Movement Frameworks: Powershell Empire
C2 obfuscation tools: HTran

Joint Report on Publicly Available Hacking Tools.

Each tool provides the following

Intro (History of tool and so on)
In Use
Capabilities
Examples
Detection and protection

Lot of the information can be applied to other similar tools such as the JBiFrost stuff is useful for a lot of other Remote Access Tools. Keep in mind of many of these tools also have legitimate uses

CloudFlare Registar

CloudFlare has a Domain Registar that is currently in beta.
It does At-cost pricing for domain registration and renewal.

.com - $8.03
.net - $9.95
.org - $10.11
.info - $11.02

Prices are subject to change of course.

CloudFlare Registar.

Right now this is a program you have to request access to and get on a waiting list.

You have to be a CloudFlare customer to be able to use the service. They do have a free tier so anybody should be able to join.

PCI - ASV Program Guide.

The Approved Scanning Vendor (ASV) Program Guide lays out the hows and whys of external vulnerability scans for merchants by vendors

This guide can give you a lot of insight of what an external vulnerability scan must include and gives you a better base language to discuss findings with your external vendors.

The ASV Program Guide v3.0 is about 50 pages so it isn't too bad.

Jigsaw Intra

Intra is an android app that is designed to prevent DNS manipulation.

Intra encrypts DNS queries so they can't be analyzed or manipulated by companies, isps or governments.

Points to Google's Public DNS service by default

Has been tested in Venezuela which does tend to do this type of filtering.

Jigsaw Intra.

Currently only an Android app.

Is Open Source

Also additional DNS traffic will be encrypted in the future by default so useful there as well

Android 9 supports DNS-over-TLS, Intra uses the DNS-over-HTTPS protocol

For fun find a DNS expert and ask him whether he prefers DoH or DoT :-P

Alphabet Outline

Outline is a roll-your-own VPN solution from Google.

Using this and a VPS solution you can roll out your own personal VPN.

Outline isn't the only option in this space.

Ideally was designed for Journalists to make reaching out easy.

Doesn't use OpenVPN protocol so it isn't universal.

Alphabet Outline.

The VPN can be quite a bit slower than commercial VPNs.

Like the Open Source nature and the ease of installing it on a server.

Doesn't currently support Linux, so not going to be my go to choice for a while.

You can learn a lot in the process of setting up an Outline VPN.

Automate the Boring Stuff with Python

Great book on how to get things done with Python. Freely available on their website.

Couple of Examples:

- Website scraping
- Connecting to a database
- Reading/Writing Excel documents
- Modifying a PDF

Automate the Boring Stuff with Python.

Couple of Things:

It is not “best practice” for python. It is not how to write really good python but python that will get the job done.

Got to say I’ve used the book a whole lot.

Public Report on SingHealth Attack

Singapore Health has just published their report on the attack against the Singapore Healthcare system.

Purpose of the attack was to get the health records for the Singaporean Premier Lee Hsien Loong.

Lays out timeline, failures and their recommendations to prevent this from happening again.

Is critical of the communication between groups. Is a good read.

GRC's - SQRL.

GRC's (Gibson Research Center's) - SQRL (Secure Quick Reliable Login)

Steve Gibson of Security Now fame has release SQRL a tool for doing secure website logins. Partially a response to tools such as lastpass and others.

Has a lot of interesting features such as QR-code support, optional phone support and so on.

Still being developed.

OSQuery.

OSQuery is a SQL-like language that you can use to query an OS to get information from. Created initially by Facebook.

You can then push that information into a tool like ElasticSearch Stack via Logstash and track changes over time.

Some of the things you can monitor are mount points, file integrity monitoring and so on.

Google Rapid Response (GRR)

GRR comprises a client and server portion.

It is designed to do remote forensics at scale.

E.g.

A user reports something weird checkout his machine via GRR even if they're not in the office
Check if a machine is compromised and check the rest of them at the same time
Acquire a subset of machines to try something out on - say 5 linux machines on the network.

Google Rapid Response (GRR)

Client provides components such as YARA memory analysis
Sleuthkit for File system access
Monitoring of CPU, Network and other items

Server provides capabilities to schedule activities
Async scheduling - for when machines become available in the future
Can scan entire network for certain signatures, activities

Google Rapid Response (GRR).

Is almost an Ansible/Salt/Puppet like system except instead of being designed to handle system updates/configuration changes is designed for security.

Don't know anybody who has deployed it, have heard about companies pulling parts of the system into their other config systems such as ansible

Oracle Cloud v2.0 (Star Wars)

Oracle is redesigning the whole of its cloud environment. Part of this is the separation of the control components from the regular hosts being run by customers.

It is also supposed to be working on roving AI and Machine Learning that will go through and monitor the system. Sarah Conner be afraid.

The separation of duties and other capabilities here sound very interesting. Want to see how that competes with other cloud vendors.

Oracle Cloud v2.0 (Star Wars).

How will other vendors (AWS & Azure) respond? Will they do the same separation or will they disregard it.

Also have to admire irony of calling your project Star Wars when the whole empire was brought down by one rebel who know how to kill swamp rats.

Virtualized Enterprise

Italian researchers have put together a white paper laying out how to emulate a network and relevant machines.

Including the following

Public - facing servers
DMZ subnets
Firewalled Internal Networks

OSes include Windows, Ubuntu, MacOS

Virtualized Enterprise.

System can be replicated by someone with around $10-$15k in budget.

Major components include OpenNebula, OpenvSwitch, and GlusterFS platforms.

Is a very nice paper the level of completeness and documentation is very impressive.

Additional work is planned on this project to better simulate user behaviour.

Microsoft Windows Sandbox.

Microsoft Windows is adding Sandbox functionality. This allows running dangerous apps in a safer container.

Available in build 18305 and later. Requires Windows 10 Pro or Enterprise.

Creates a licensed throwaway container.

Another option some people use is sandboxie.

Q & A

Questions???

Links

Tip - Kaggle Datasets

https://www.kaggle.com/datasets

Tip - AWS Artifacts

https://aws.amazon.com/artifact/

Links

Tip - Azure Sphere IoT

https://azure.microsoft.com/en-us/services/azure-sphere/

http://linuxgizmos.com/how-azure-sphere-ensures-iot-security-within-a-4mb-linux-stack/

Links

Tip - NITTF Training

Register Article on the NITTF Training Couse

https://www.theregister.co.uk/2018/09/13/nittf_insider_threat_self_analysis/

Link to Course

https://www.dni.gov/ncsc/Insider-Threat/

Links

Tip - CLIP-OS

https://clip-os.org/en/clipos5/

Github Repo for Clip-OS

https://github.com/clipos

Links

Tip - Biscuit - OS Kernel written in GO

Github repo

https://github.com/mit-pdos/biscuit.git

Paper describing OS

https://www.usenix.org/system/files/osdi18-cutler.pdf

Links

Tip - Joint Report on Publicly Available Hacking Tools

https://www.ncsc.gov.uk/joint-report

https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

Links

Tip - Cloudflare Registrar

https://www.cloudflare.com/products/registrar/

PCI ASV Guide v3.0

https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.0.pdf

Links

Tip - Jigsaw Intra

Google Play Store Entry for Intra

https://play.google.com/store/apps/details?id=app.intra

Article describing Jigsaw Intra

https://www.helpnetsecurity.com/2018/10/04/intra/

Links

Tip - Alphabet Outline

https://getoutline.org/en/home

Tip - Automate the Boring Stuff with Python

https://automatetheboringstuff.com/

Links

Tip - Singhealth Attack

https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2019/1/public-report-of-the-coi

Tip - GRC's - SQRL

https://www.grc.com/sqrl/sqrl.htm

Tip - OSQuery

https://osquery.io/

Links

Tip - Google Rapid Response (GRR)

https://github.com/google/grr

Tip - Oracle Cloud v2 (Star Wars)

https://www.theregister.co.uk/2018/10/23/oracle_openworld_ellison_keynote/

Links

Tip - Build Your Own Virtual Enterprise

https://www.theregister.co.uk/2018/10/26/infosec_holodeck_network/
https://arxiv.org/pdf/1810.09752.pdf

Tip - Microsoft Windows Sandbox

https://www.theregister.co.uk/2018/12/19/microsoft_windows_sandbox/
https://www.sandboxie.com/