



Attacker Cryptonite, How To Threat Model Your Way To A Good Night's Sleep

Lockdown 2017

Why This Talk

Story

Extraordinary Security Comes From Within

Allows For Security Enablement

I Want You To Sleep

Problem Statement

Your work prioritization is almost always determined by forces outside of your control

Vulnerabilities

Have Become FUD

Lead To Poor Security Practices

Hurt Business Relationships

Money Makers

Verizon 11:20 PM 21%

< Tweet +

 **egyp7**
@egyp7

This. Stop worrying about one exploit for one vuln delivering one ransomware payload. Make it harder for **every** exploit and **every** payload

strandjs @strandjs
Good architectures should be resilient to 0-days. App white listing, endpoint firewalls and egress white listing are the new min

6/27/17, 1:57 PM

51 Retweets 110 Likes

Vulnerabilities (Continued)

They Are Not Org Specific

Attempts To Score Vulnerabilities For Severity Are Disconnected From The Reality of Exploiting Them

The screenshot displays the Nessus interface for a vulnerability scan. The main table lists the following vulnerabilities:

Severity	Plugin Name	Plugin Family	Count
CRITICAL	CentOS 6 / 7 : openssl (CE...	CentOS Local Security Checks	1
CRITICAL	CentOS 7 : glibc (CESA-201...	CentOS Local Security Checks	1
HIGH	CentOS 7 : graphite2 (CESA...	CentOS Local Security Checks	1
HIGH	CentOS 7 : kernel (CESA-20...	CentOS Local Security Checks	1
HIGH	CentOS 7 : mariadb (CESA-...	CentOS Local Security Checks	1
MEDIUM	CentOS 5 / 6 / 7 : bind (CES...	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : ipa / libidb / ll...	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : libssh2 (CES...	CentOS Local Security Checks	1

Host Details:

- IP: 192.168.56.102
- DNS: st91.l
- MAC: 08:00:27:db:3e:a2
- OS: Linux Kernel 3.10.0-327.4.5.el7.x86_64 on CentOS Linux release 7.2.1511 (Core)
- Start: May 11 at 10:34 PM
- End: May 11 at 10:39 PM
- Elapsed: 6 minutes
- KB: [Download](#)

Vulnerabilities Legend:

- Critical (Red)
- High (Orange)

What Do You Look At?

“When you Change The Way You Look At Things,
what You Look At Changes”

-Wayne Dyer

Threat Modeling Step 1

Document, don't create
Network Topology?

Threat Modeling Step 2

Clearly Define All of Your Security Controls Across Your Organization

Don't Forget things like AD and External MSSPs

Threat Modeling Step 3

Map Your Network Topology To Your Security Controls
and Identify Easy Gaps

Adopt A Framework

“If Someone Is Earning 25k a year it is not because they want to it is because they are not aware of how to earn 50k” – Bob Proctor

Attackers Do Why Don't Defenders?

MITRE ATT&CK Framework

Lets Do Some Math

Network Topology + Security
Controls + Framework +
Central Logging = Success

Blue Team Ethos

Complete
Ownership

This is YOUR
Environment Not
the Attackers

It's Not About
Good Security It's
About Having
Frustrating Security



**KEEP
CALM
AND BELIEVE THAT
BLUE TEAM
ROCKS**

Contact Info

Eric Groce

@IA_Every_Day