


# Active Defense

## Helping Threat Actors Hack Themselves!



OISF Anniversary – July 14, 2018

*Matt Scheurer*

 @c3rkah

Slides:

<https://www.slideshare.net/cerkah>



# About Me

```
root@0ISF:~# whoami
```

**Matt Scheurer**

Systems Security Engineer in the Financial Services Industry

Chair for the CiNPA Security SIG

Speaker at: DerbyCon 5.0, DerbyCon 7.0, the 10<sup>th</sup> Annual NKU Cyber Security Symposium, BSides Indianapolis 2018, BSides Columbus 5.0, BSides Cincinnati 2018, the 11<sup>th</sup> Annual Central Ohio InfoSec Summit, Circle City Con 5.0, and BSides Cleveland 2018

Certifications: CompTIA Security+, MCP, MCPS, MCTS, MCSA, MCITP, and next is CCNA Cyber Ops!

Yes, I have a day job. However...

Opinions expressed  
are solely my own and  
do not express the  
views or opinions of  
my employer.



# Legal Disclaimer



The material presented is made available for informational and educational purposes only. Use of these tools and techniques is **at your own risk!** The presenter hereby disclaims any and all liability to any party for any direct, indirect, implied, punitive, special, incidental or other consequential damages arising directly or indirectly from any use of these materials, which are provided as is, and without warranties.

# What is Active Defense?

Active defense can refer to a defensive strategy in the military or cybersecurity arena. The Department of Defense defines active defense as: "The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy." In the cybersecurity arena, active defense may mean "asymmetric defenses," namely defenses that increase costs to cyber-adversaries by reducing costs to cyber-defenders.

- Source: [https://en.wikipedia.org/wiki/Active\\_Defense](https://en.wikipedia.org/wiki/Active_Defense)

# Why Active Defense?

1. Because “Hacking Back” is illegal!
2. Active Defense is the next level beyond honeypots, honeyfiles, and honeynets

# Our Objectives

1. Shield and protect legitimate users at all times!
  - Be diligent about protecting innocent site visitors...
2. Frustrate malicious threat actors attempting to steal and ex-filtrate data through unauthorized access
  - Preferably by unwittingly hacking themselves...
3. See Objective #1!

# Presentation Focus

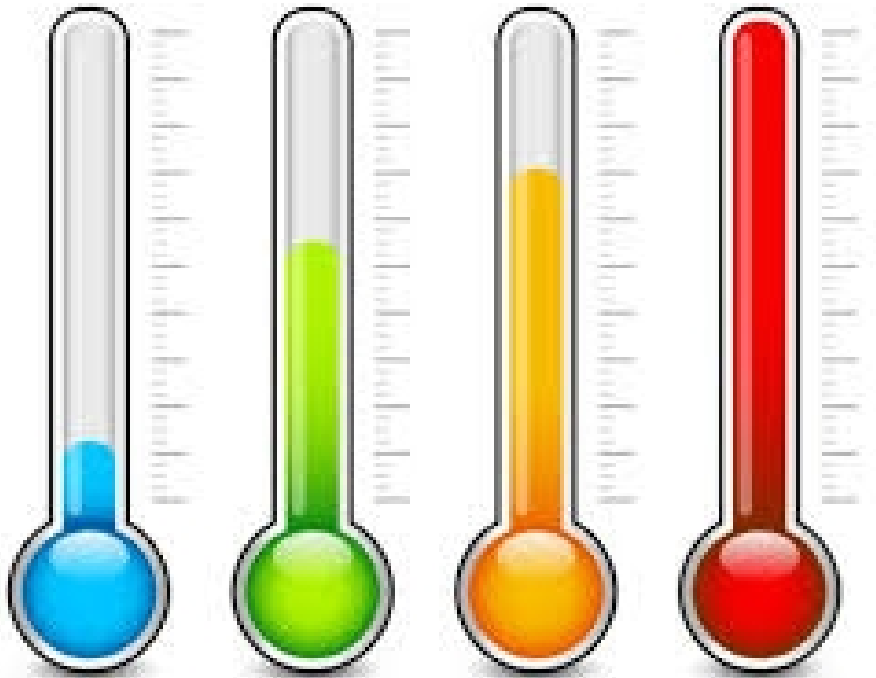
- Active Defense for a website
- Baiting and setting traps for script kiddies and other cyber criminals



# Inspirations

- **Aikido**
  - Using an opponents energy / force against them
- **My Father**
  - Junk mail counter-strikes
- **Nature**
  - Animal Defenses
- **Nostalgia**
  - Everything old is new again...
- **Security Minded**
  - Yet a prankster at heart <3
- **Vigilante Nature**
  - Love seeing the bad guys getting what they deserve!

# Conventions Used



## Hot Water Index:

- Escalating thermometer temperature indicates the greater potential of getting reported for hosting malicious content

# Protecting Legitimate Users

- Create a “robots.txt” file
- Create a Sitemap XML file
- Do not link to Active Defense Content
  - Use a link / hyperlink checker to verify
- Disable directory indexing on legitimate content
- Potentially protecting yourself by making use of authorized user only messages

# “robots.txt” files

Reference: <http://www.robotstxt.org/>

## **Example**

Sitemap: <https://cybernnati.com/sitemap.xml>

User-agent: \*

Disallow: /cgi-bin/

Disallow: /complex/ # Company Confidential Information

Disallow: /docs/ # Company Confidential Information

Disallow: /org/ # Company Confidential Information

Disallow: /protected/ # Company Confidential Information

Disallow: /webmaster/ # Company Confidential Information

Disallow: /wp-admin/ # WordPress Administration Files

Disallow: /wp-content/ # WordPress CMS Files

Disallow: /wp-includes/ # WordPress CMS Files

# Sitemap XML files

Reference: <https://www.sitemaps.org/protocol.html>

## Example

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<urlset xmlns="http://www.sitemaps.org/schemas/sitemap/0.9"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:schemaLocation="http://www.sitemaps.org/schemas/sitemap/0.  
9 http://www.sitemaps.org/schemas/sitemap/0.9/sitemap.xsd">
```

```
<url>
```

```
<loc>http://www.cybernnati.com/</loc>
```

```
</url>
```

```
</urlset>
```

# Directory Indexes

As a matter of good web security, disable directory Indexing on all legitimate web content!

- The lone exception for this is with our Active Defense content
  - This will help ensure that those purposely ignoring the borders and confines defined in our robots.txt and sitemap.xml files find our Active Defense content

# Authorized Users Only

## Example (README.txt or README.html):

-----

W A R N I N G

-----

THIS IS A PRIVATE AREA OF THIS WEBSITE.

This website including all related data and information are provided only for authorized use.

All connections and activity may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security.

Monitoring includes active attacks by authorized personnel and their entities to test or verify the security of the system. During monitoring, information may be examined, recorded, copied and used for authorized purposes.

All information including personal information, placed on or sent over this system may be monitored. Uses of this system, authorized or unauthorized, constitutes consent to monitoring of this system.

Unauthorized use is prohibited! Unauthorized use may subject you to criminal prosecution. Evidence of any such unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

# The Roundtrip Roundkick



- Create a bunch of unused DNS sub-domain host records pointing back to 127.0.0.1
- The harder the attackers try to hit you at these sub-domains, the harder they are actually hitting themselves



# Subdomain Examples

- api
- app
- bbs
- blog
- cloud
- dev
- email
- forum
- ftp
- host
- m
- mail
- mailserver
- mx
- ns
- ns1
- ns2
- owa
- pop
- portal
- remote
- secure
- server
- shop
- smtp
- support
- test
- vpn
- web
- webmail
- autodiscover
- wordpress

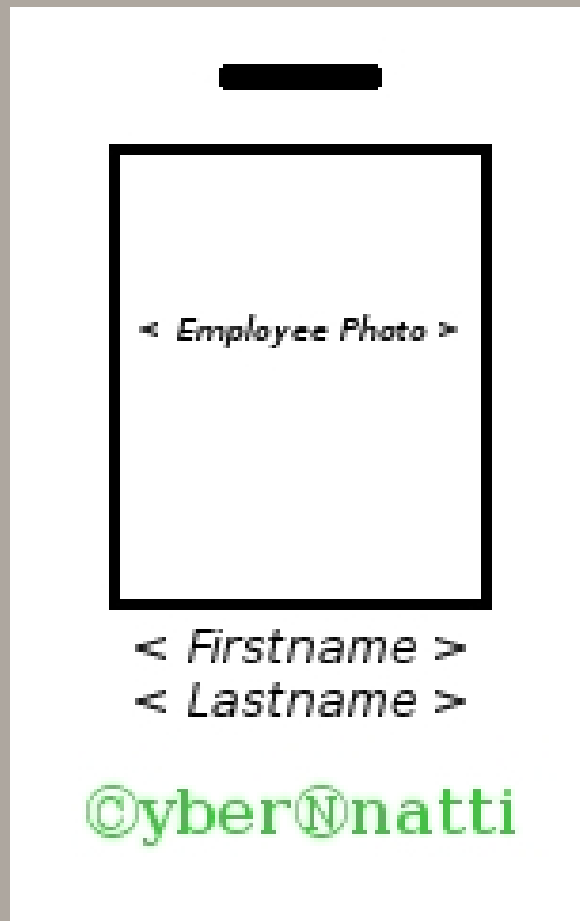
# Stomachvivor / Gross Out



- Stage an unreferenced folder with a fake door badge ID template
  - **NOTE:** Not too similar to one's you actually use!
- Place “gross-out” pictures of choice disguised as staff photo headshots

# Phony Photo IDs

/complex/buildings/access/  
Door\_Badge\_ID\_Template.jpg



/complex/buildings/access/2017\_headshots/  
Guthrie\_Ricky.jpeg



# Reflector Madness



- Create an easy to crack password protected folder
- What's waiting inside is not something threat actors will expect...

# Can you guess my credentials?

.htaccess file:

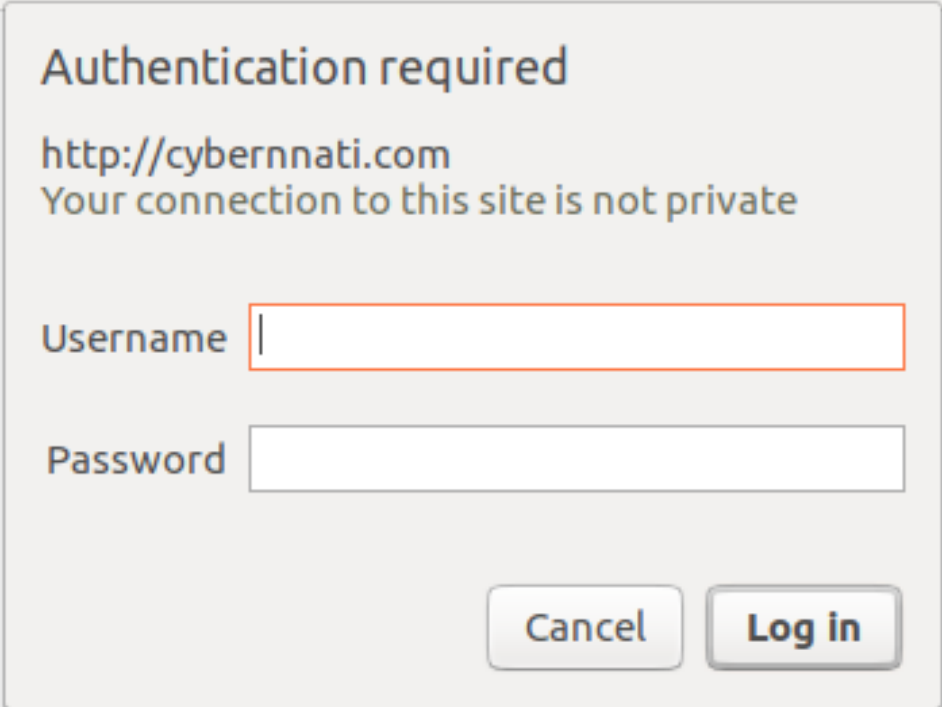
AuthType Basic

AuthName "protected"

AuthUserFile

"/home2/<SNIP>/.htpasswd/public\_html/protected/passwd"

require valid-user



Authentication required

http://cybernnati.com  
Your connection to this site is not private

Username

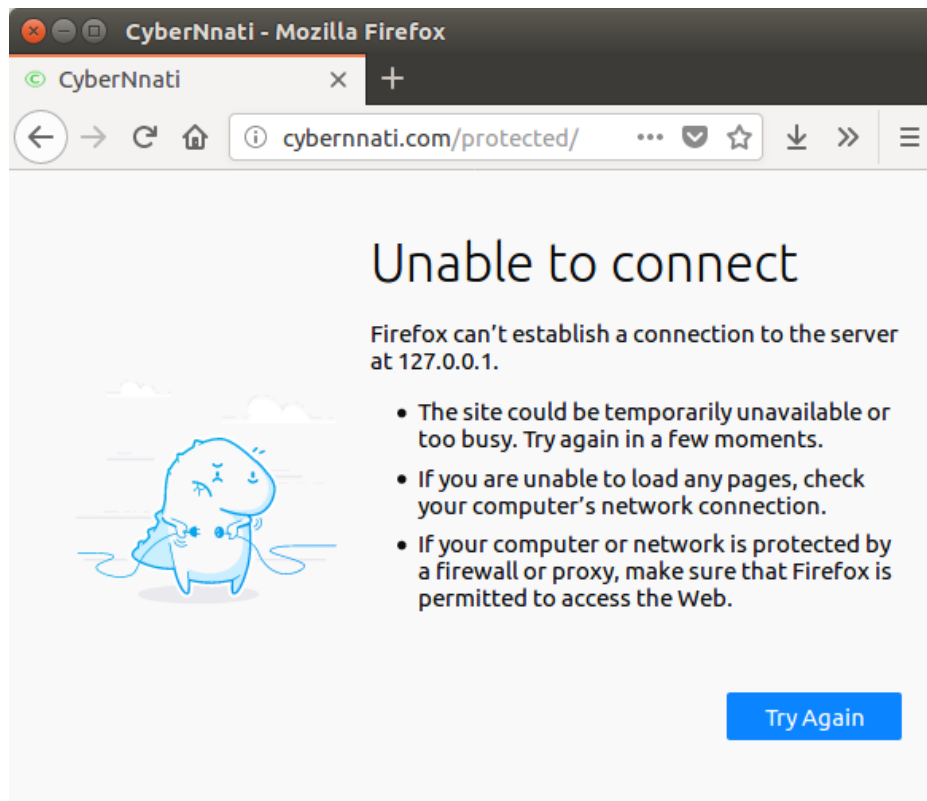
Password

Cancel Log in

- **HINT:** It's possibly one of the worst username and password combinations you could have on a network device

# Reward for cracking the login is?

- Probably this...



- But maybe this!



# Inside the source code

- A no borders iFrame pointing back to the loopback address...
  - If an attacker is running a web server locally on their system then they may potentially attack themselves

```
<!DOCTYPE html>
```

```
<html dir="ltr" lang="en-us">
```

```
<head>
```

```
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
```

```
<title>CyberNnati</title>
```

```
</head>
```

```
<body style="margin: 0px; padding: 0px; overflow: hidden">
```

```
<div>
```

```
<iframe src="http://127.0.0.1/" style="position: absolute; width: 100%; height: 100%; border: none">
```

```
</iframe>
```

```
</div>
```

```
</body>
```

```
</html>
```

# Going Nowhere Fast!

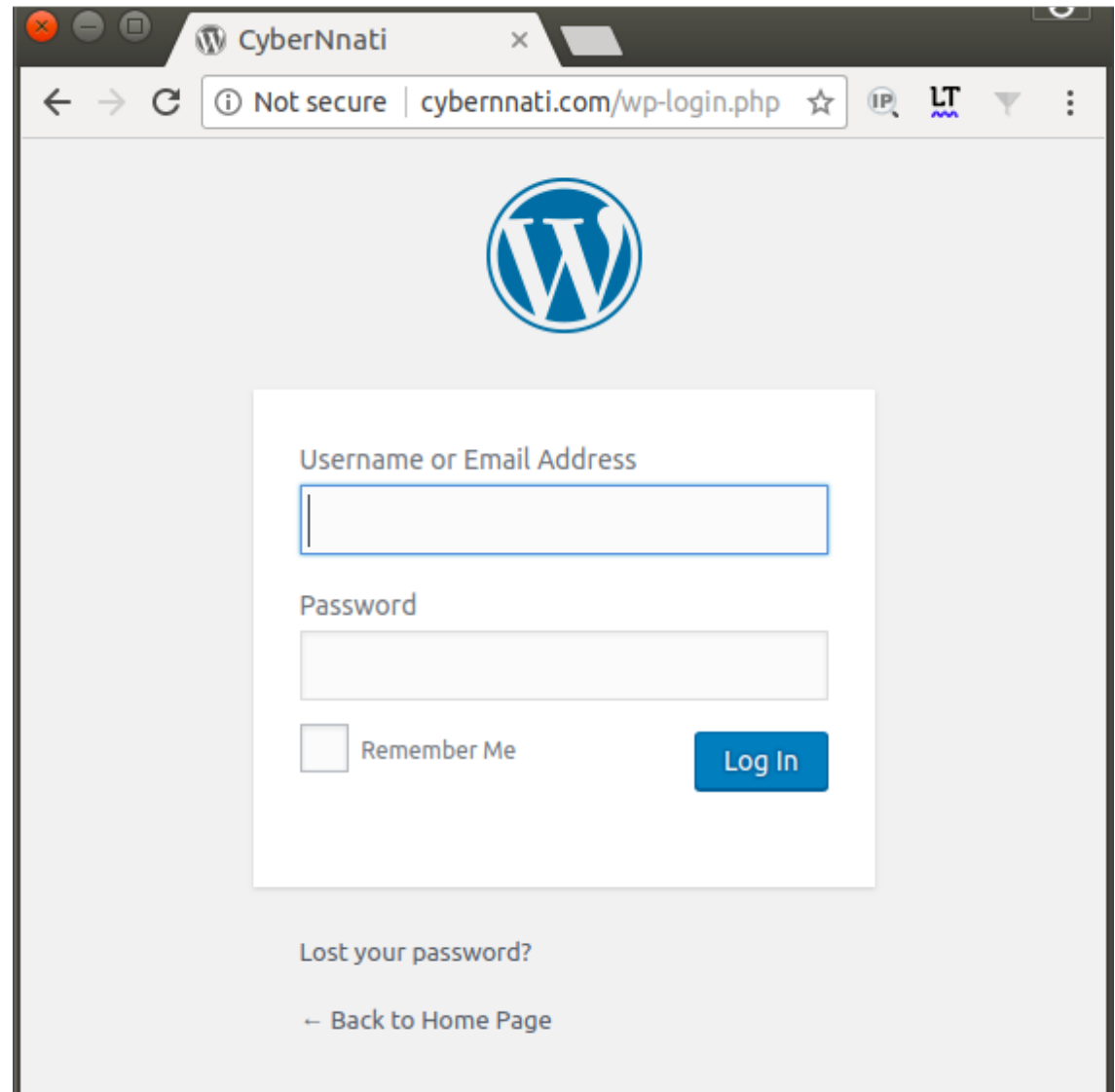


- WordPress is by far the most deployed CMS in the World powering countless web sites
- Consequently the WordPress login page is one the most targeted for brute force attacks by malicious threat actors



# Try Guessing my Credentials Now?

This is a live  
“wp-login.php”  
page:

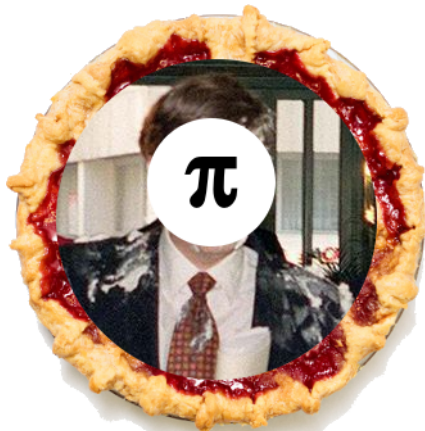


# What went wrong?

The web page you just saw was a completely fabricated WordPress login page. And there is absolutely no real username or password. The goal is to have brute force attackers spin their wheels thus wasting their time, energy, and resources!

This is further sold by planting the appropriate folder structure and default files that give away a site as a WordPress site.

# Pi to the Face



- There is quite a bit to unpack for this Active Defense strategy...
  - From disinformation, to wasting attackers time, to potentially getting them banned from larger service providers, to burning their CPU cycles and draining batteries
- We start by using the enterprising cyber criminals own CryptoJacking techniques against them...

# The Setup...

- Have a “webmaster” folder containing a fictitious “bookmarks.html” file
- Stage non-existent login account links for popular sites and services an attacker might waste time attempting to brute force
  - Hopefully they trip whatever alert thresholds these service providers may have in place resulting in a ban or being reported to a threat intelligence feed!
- Behind the scenes we are computationally calculating Pi hundreds of thousands of times
  - Wash, rinse, repeat!

# Inside “bookmarks.html”

**Facebook:**

<https://www.facebook.com/login.php?email=webmaster@cybernnati.com>

**Google:**

<https://mail.google.com/mail/u/?authuser=webmaster@cybernnati.com>

**LinkedIn:**

<https://www.linkedin.com/uas/login?email=webmaster@cybernnati.com>

**Microsoft LiveID:**

<https://login.live.com/login.srf?email=webmaster@cybernnati.com>

**Twitter:**

[https://twitter.com/login?username\\_or\\_email=webmaster@cybernnati.com](https://twitter.com/login?username_or_email=webmaster@cybernnati.com)

**Yahoo:**

<https://login.yahoo.com/config/login?username=webmaster@cybernnati.com>

# Source Code

## bookmarks.html

Inside the <head> and </head> tags:

```
<meta http-equiv="refresh"
content="3.14">
```

Right before the </body> and </html> tags:

```
<script
src="./scripts/includes.js"></scri
pt>
```

```
<script
src="./scripts/pinapall.js"></scri
pt>
```

## includes.js / pinapall.js

```
var pinapall=0;
var zzz=1;
var
enumeration=314159265;
for (i=0;i<=enumeration;i++)
{
    pinapall=pinapall+(4/zzz)-
(4/(zzz+2))
    zzz=zzz+4
}
```

# CPU Impacts to Attackers

- On a low powered system or dual-core VM this can spike the CPU up to 100%
- On a moderately powered system this may spike the CPU up to 50%
  - If they are already running a heavy CPU load then this will effectively spike the CPU all the way
  - Not uncommon with Java based tools like Burp
- Heavy CPU loads will drain batteries on mobile devices, including laptops, at a notably accelerated rate

# The Wrong Answer



- Ever have to recover a system with a 100% full disk drive?
- Stage a file with an enticing name inside of an unreferenced folder such as:  
**/docs/hr/employee\_salary\_history.xlsx.zip**
- Which is really just a renamed version of the infamous “42.zip” file!

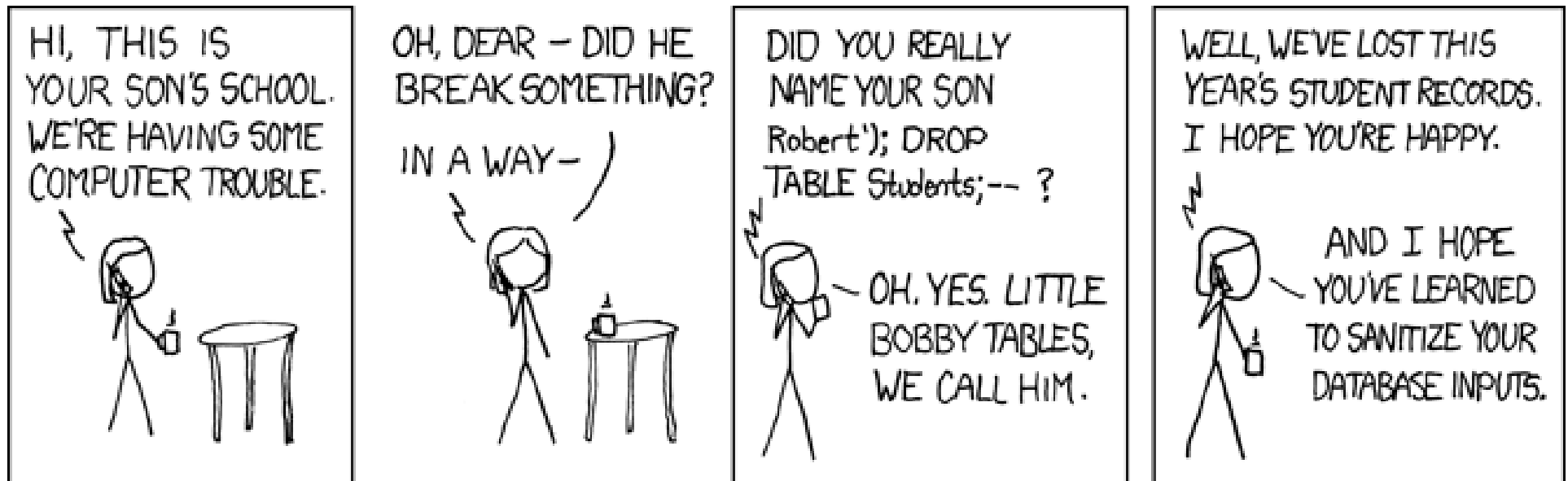


# What is “42.zip”?

42.zip is an approximately 42kb compressed zip file. Fully uncompressed the extracted files expand out to upwards of 4.2 Petabytes of data!

- Most data thieving cyber criminals won't have a hard drive that large... :)

# Bobby Dropkick



Cartoon From:

<https://xkcd.com/327/>

Titled: "Exploits of a Mom"



# The Setup

- Stage a fake employee database dump file inside of an unreferenced folder:

i.e., /org/departments/human\_resources/

- Give the file an enticing name such as:

2017-12-05\_hris\_employee\_mysql\_db\_backup.zip

- OR -

2017-12-05\_hris\_employee\_mysql\_db\_backup.sql

# What Else is Inside?

Just a little SQL code to permanently wipe out the MySQL internal databases...

```
DROP DATABASE mysql;
```

```
DROP DATABASE sys;
```

```
DROP DATABASE performance_schema;
```

```
DROP DATABASE information_schema;
```

If you thought recovering from a full disk situation was a hassle... :)

# Alternative Active Defense Options



<https://www.blackhillinfosec.com/projects/adhd/>



SEC550: Active Defense, Offensive Countermeasures and Cyber Deception

<https://www.sans.org/course/active-defense-offensive-countermeasures-and-cyber-deception>

# Criticisms, I've received a few...

- You should make the “Reflector Madness” login harder to crack
  - You're in control...
  - Make it as simple or difficult to defeat as you like!
- This would make a legitimate penetration test more difficult
  - Have good documentation prepared in advance for white box or gray box engagements
  - An advance explanation of your robots.txt and sitemap should provide guidance

# Other expressed concerns...

- “We’re not going to implement this, it might really tick off some skilled attackers and vindictive types!”
  - Malicious threat actors are mostly undeterred today
    - They do not fear retribution for their actions
    - That is why they keep compromising vulnerable systems
  - The fact that Brian Krebs is still alive today is a testament to not living in fear of what might happen
    - Krebs adversaries ultimately respect him more for continuing his work
- Still not convinced in implementing Active Defense strategies?
  - Then simply don’t implement them!

# Questions

**Who ...**

**What ...**

**When ...**

**Where ...**

**Why ...**

**How ...**






# Thank you for attending!



OISF Anniversary – July 14, 2018

*Matt Scheurer*

 @c3rkah

Slides:

<https://www.slideshare.net/cerkah>

