Securing Your Own Internet of Things

Best Practices To Protect Your Organization & Your Data

Justin Hall
Director, Security Services

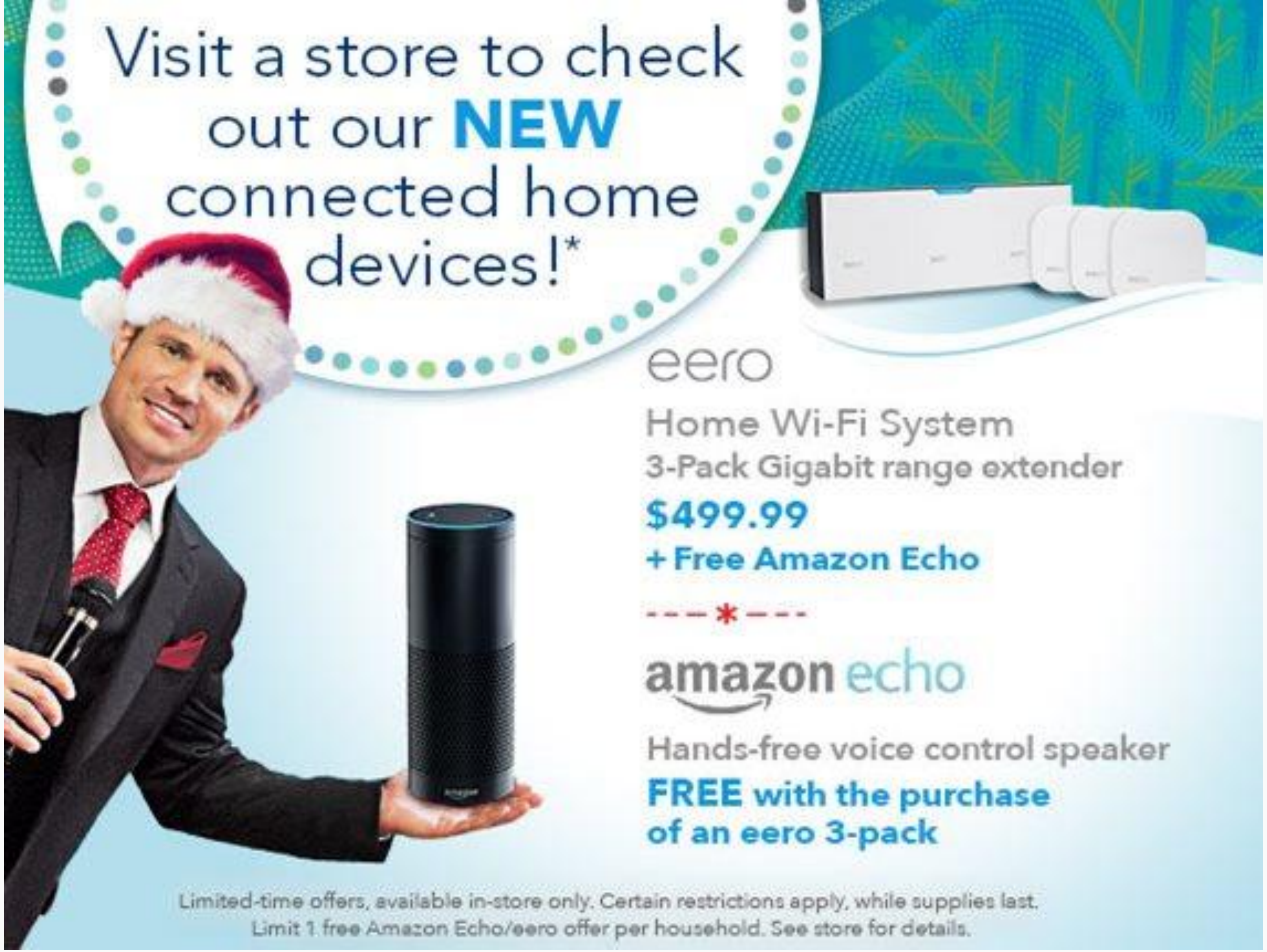
CBTS

/usr/bin/whoami

Twelve years with CBTS as security consultant to shops small (5 person) and large (Fortune 5)

GIAC Certified Penetration Tester, Incident Handler, Forensic Analyst

BSidesCincinnati cofounder



Visit a store to check out our **NEW** connected home devices!*

eero

Home Wi-Fi System

3-Pack Gigabit range extender

$499.99

+ Free Amazon Echo

amazon echo

Hands-free voice control speaker

FREE with the purchase of an eero 3-pack

Limited-time offers, available in-store only. Certain restrictions apply, while supplies last.
Limit 1 free Amazon Echo/eero offer per household. See store for details.

*Note: From our own advertisements!

1. Botnet compromised smart devices on campus network

2. Compromised devices begin to hammer DNS server with bogus lookups

3. College students lose internet connection, weep bitter tears

1. Attackers install malware on connected key management system
2. Attackers demand ransom, threatening to keep all doors locked
3. Hotel pays up, finances additional cybercrime

“Hotel ransomed by hackers” - Central European News, Koen Berghuis

Internet of…
What things?

At work!

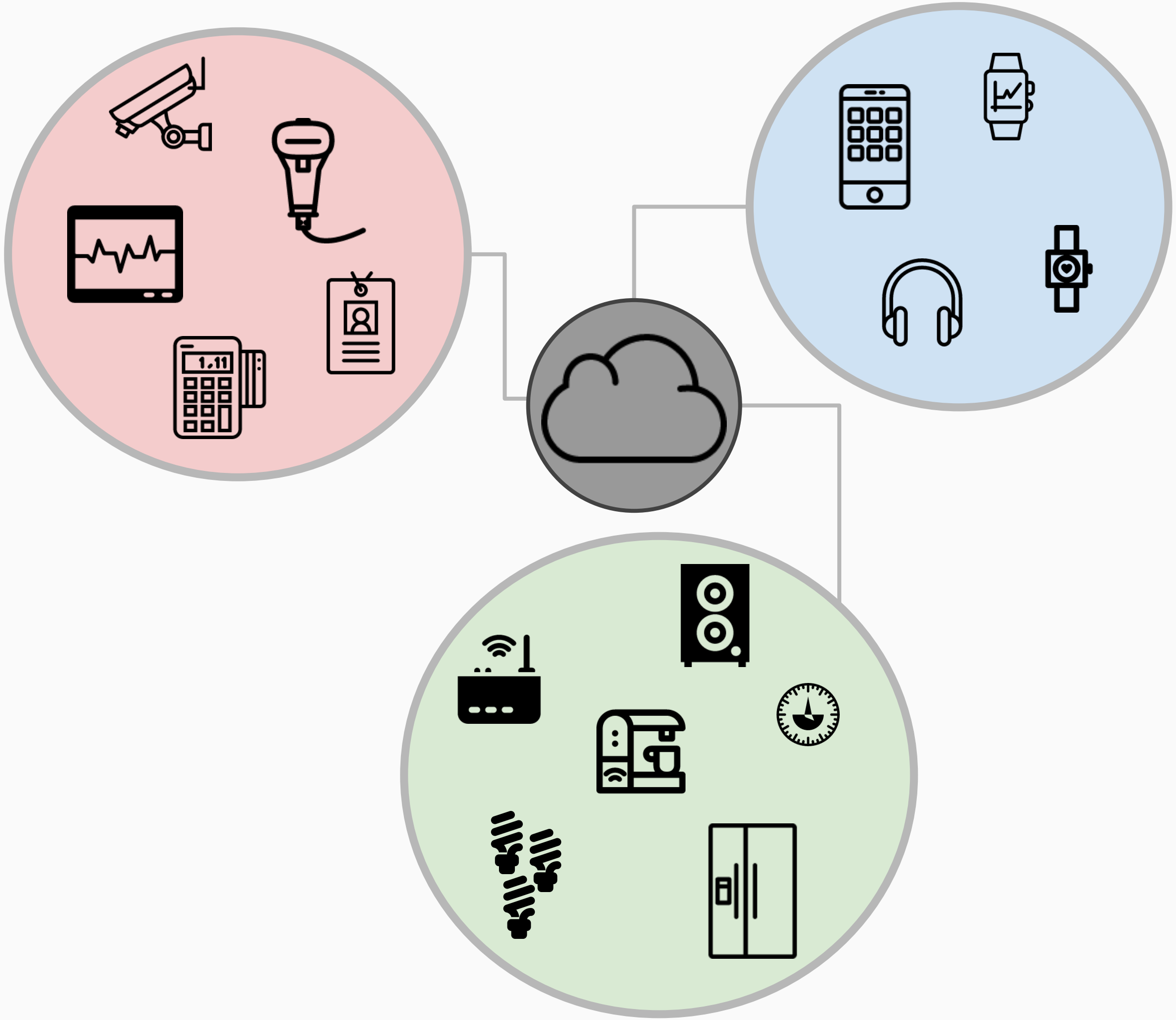
- CCTV cameras
- Barcode scanners
- Medical devices
- Credit card terminals
- Badge readers

At home!

- Appliances
- Light bulbs
- Media devices
- Routers, APs, ISP Modems

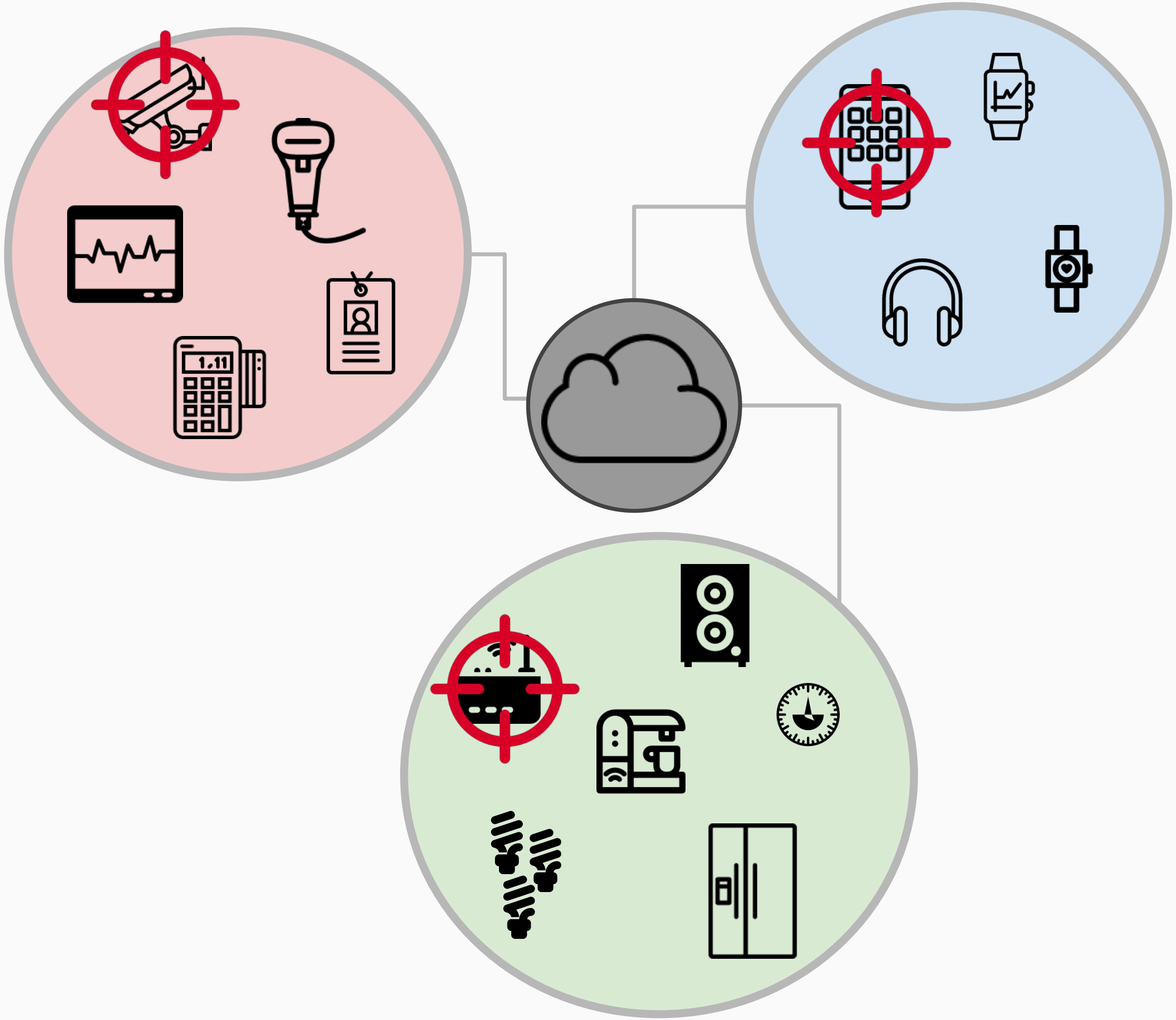
On us!

- Phones
- Smart watches
- Fitness trackers
- Audio devices



Smart Devices Become Targets

- Default vendor-assigned passwords
- Missing patches & out of date firmware
- Open ports & listening management services



What are they after?

Bandwidth

ROOT:#

Access

CONFIDENTIAL
TOP SECRET
DO NOT SHARE
SERIOUSLY
THAT'D BE REAL BAD
TLP DARK RED

Sensitive Data

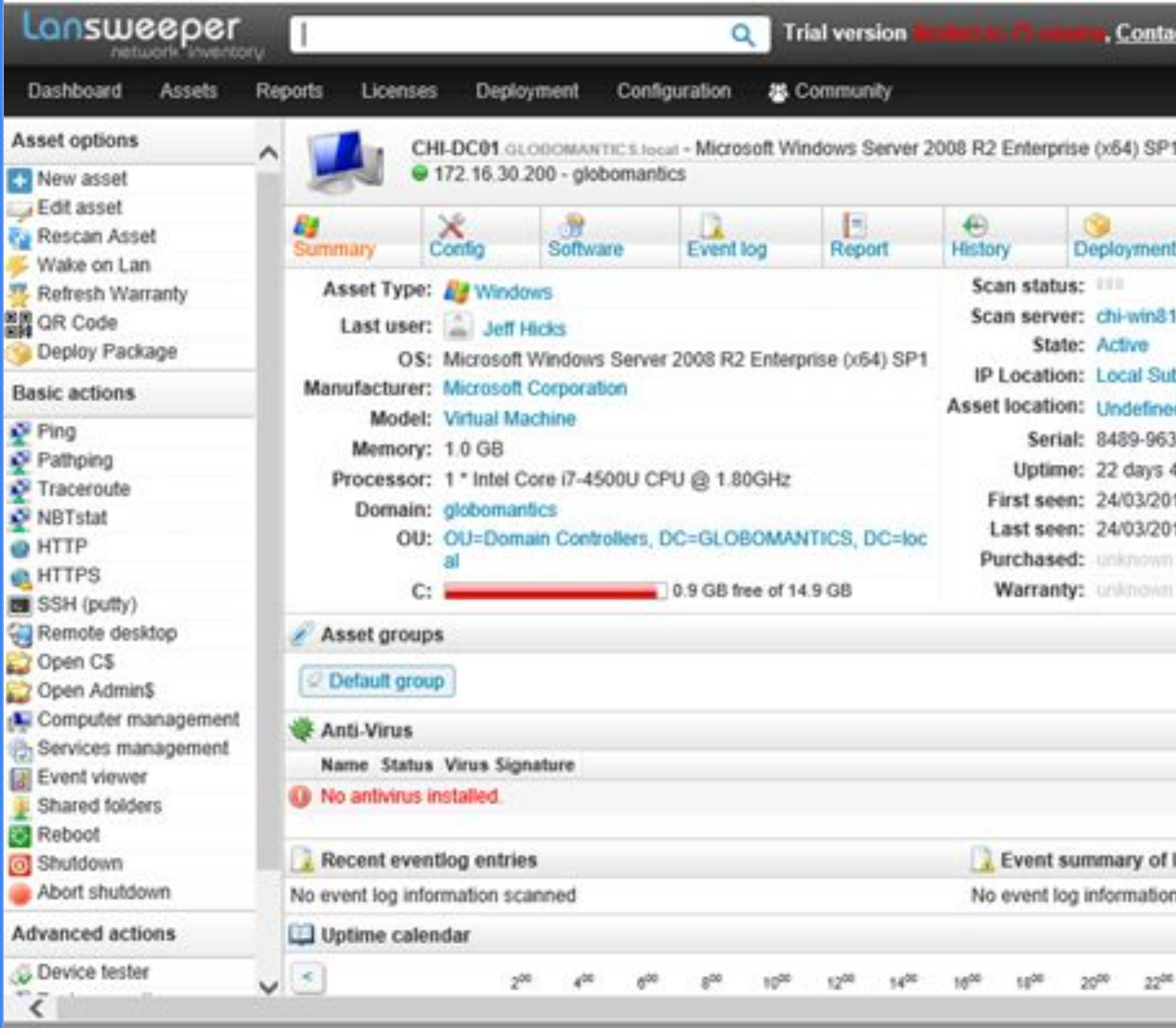
1 Know what’s in your environment

1. Know what's in your environment

Complete asset inventory, including servers, workstations, network devices, mobile devices, smart devices

Periodic portscans - what ports should be/are open on assets?

Vulnerability scans - what needs to be patched & fixed?



CHI-DC01 GLOBOMANTICS.local - Microsoft Windows Server 2008 R2 Enterprise (x64) SP1
172.16.30.200 - globomantics

Asset Type: Windows
Last user: Jeff Hicks
OS: Microsoft Windows Server 2008 R2 Enterprise (x64) SP1
Manufacturer: Microsoft Corporation
Model: Virtual Machine
Memory: 1.0 GB
Processor: 1 * Intel Core i7-4500U CPU @ 1.80GHz
Domain: globomantics
OU: OU=Domain Controllers, DC=GLOBOMANTICS, DC=local
C: 0.9 GB free of 14.9 GB

Scan status:
Scan server: chi-win81
State: Active
IP Location: Local Sub
Asset location: Undefine
Serial: 8489-963
Uptime: 22 days
First seen: 24/03/20
Last seen: 24/03/20
Purchased: unknown
Warranty: unknown

Asset groups

Default group

Anti-Virus

Name	Status	Virus Signature

No antivirus installed

Recent eventlog entries

No event log information scanned

Event summary of l

No event log information

Uptime calendar

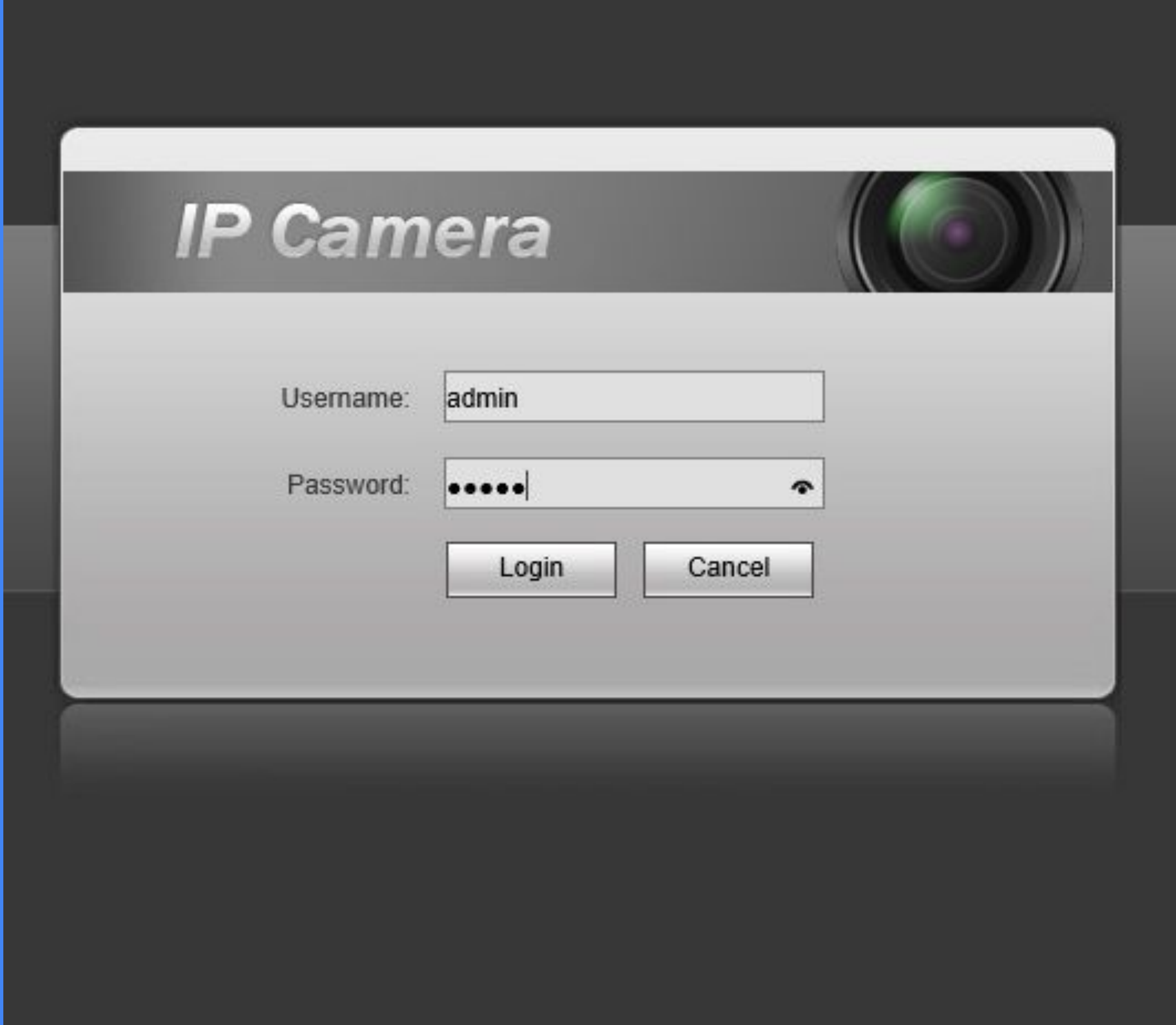
2 Harden authorized smart devices

2. Harden authorized devices

Patch vulnerabilities

Change default passwords & SNMP strings

Disable unnecessary services (file transfer, management, shell, etc)



Username: admin

Password: ●●●●●

3 Remove unauthorized devices

3. Remove unauthorized devices

Rogue wireless access points

IP cameras

Appliances

Audio/video streaming systems

Personal tablets, phones, laptops

4 Stay watchful

4. Stay watchful

Monitor your logs and network traffic for suspicious activity

Scan the environment monthly & use passive “scanning”

Have a third party perform a security assessment & penetration test

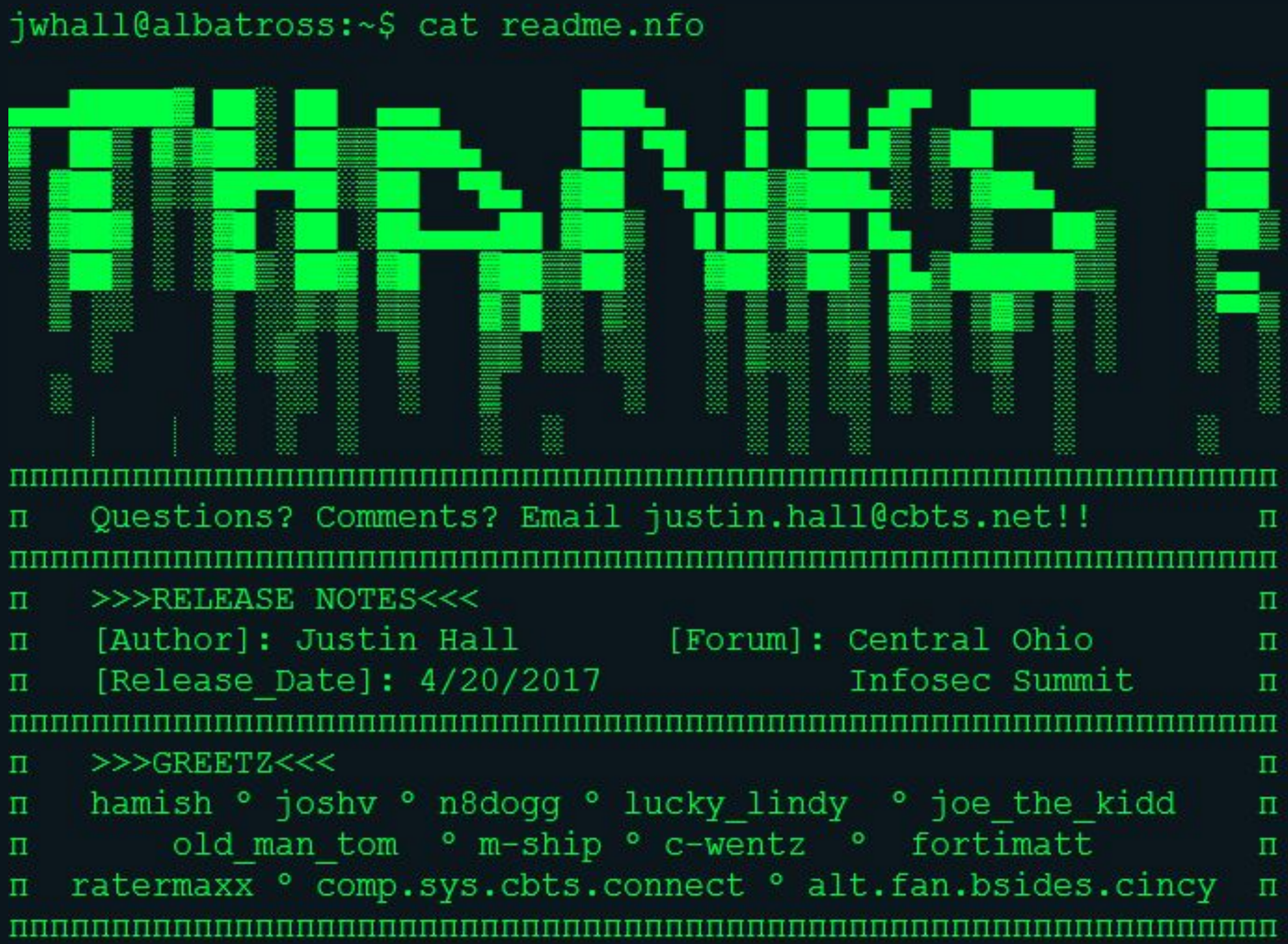
BSidesCincinnati 2017 - May 20
University of Cincinnati

Listen to excellent talks! Network! Learn! Beer! Food! Swag!

@bsidescincy / bsidescincy.org

Q&A

@justinhall
justin.hall@cbts.net



```
jwhall@albatross:~$ cat readme.nfo

пппппппппппппппппппппппппппппппппппппппппппппппппппппппппппппп
п   Questions? Comments? Email justin.hall@cbts.net!!        п
пппппппппппппппппппппппппппппппппппппппппппппппппппппппппппппп
п   >>>RELEASE NOTES<<<                                      п
п   [Author]: Justin Hall          [Forum]: Central Ohio     п
п   [Release_Date]: 4/20/2017               Infosec Summit   п
пппппппппппппппппппппппппппппппппппппппппппппппппппппппппппппп
п   >>>GREETZ<<<                                             п
п   hamish ° joshv ° n8dogg ° lucky_lindy  ° joe_the_kidd    п
п       old_man_tom  ° m-ship ° c-wentz  °  fortimatt        п
п  ratermaxx ° comp.sys.cbts.connect ° alt.fan.bsides.cincy  п
пппппппппппппппппппппппппппппппппппппппппппппппппппппппппппппп
```