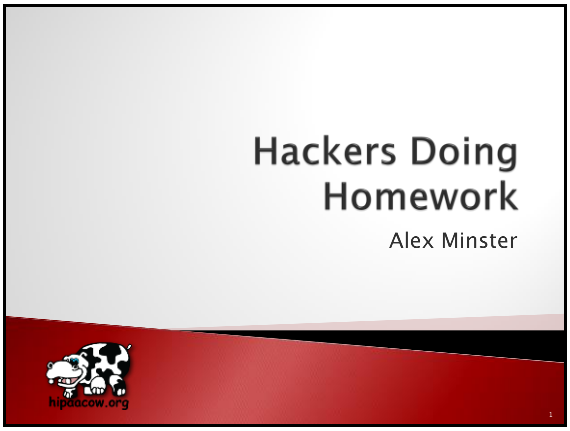
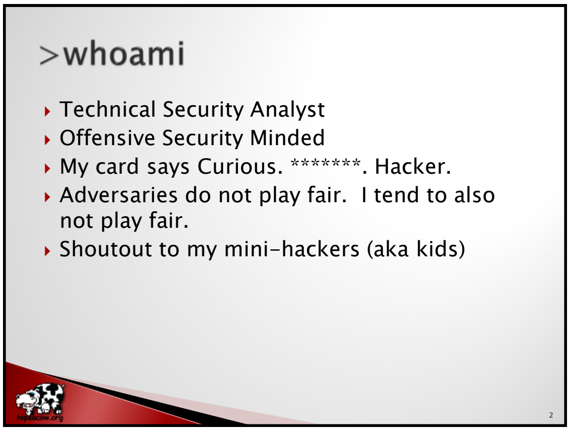


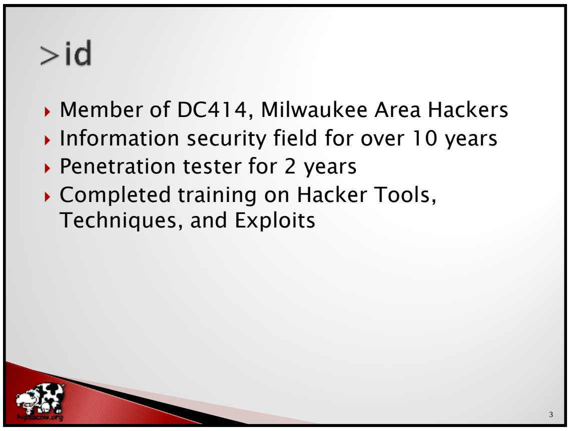
Hackers Doing Homework

Alex Minster



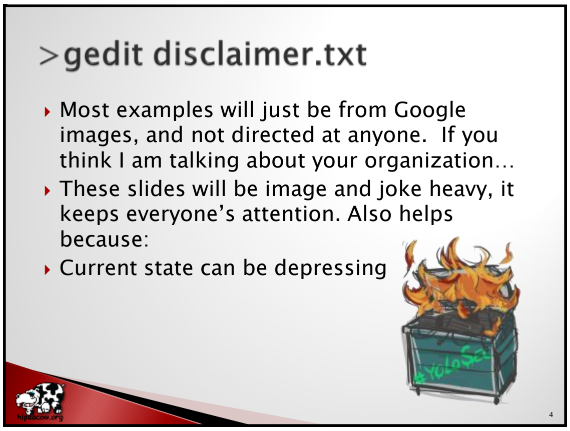
>whoami

- Technical Security Analyst
- Offensive Security Minded
- My card says Curious. *******. Hacker.
- Adversaries do not play fair. I tend to also not play fair.
- Shoutout to my mini-hackers (aka kids)



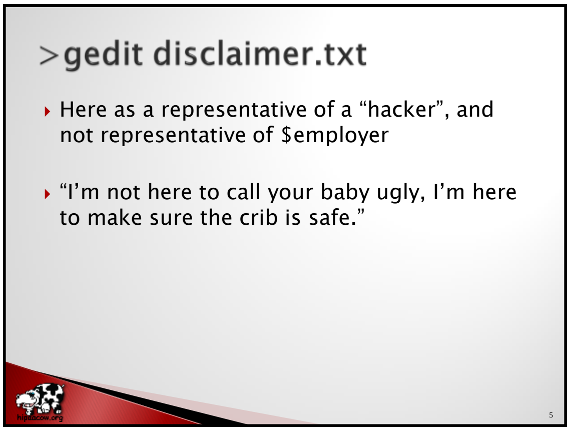
>id

- Member of DC414, Milwaukee Area Hackers
- Information security field for over 10 years
- Penetration tester for 2 years
- Completed training on Hacker Tools, Techniques, and Exploits



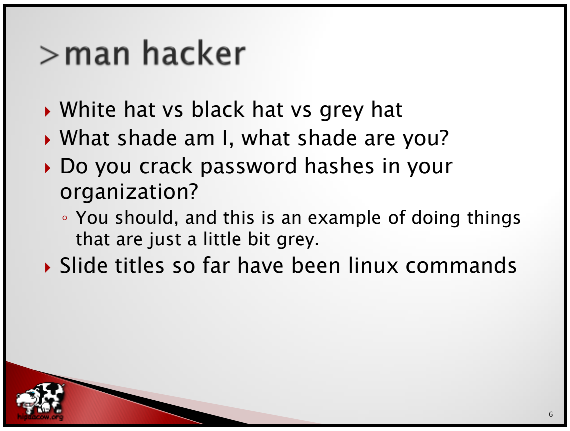
>gedit disclaimer.txt

- Most examples will just be from Google images, and not directed at anyone. If you think I am talking about your organization…
- These slides will be image and joke heavy, it keeps everyone's attention. Also helps because:
- Current state can be depressing



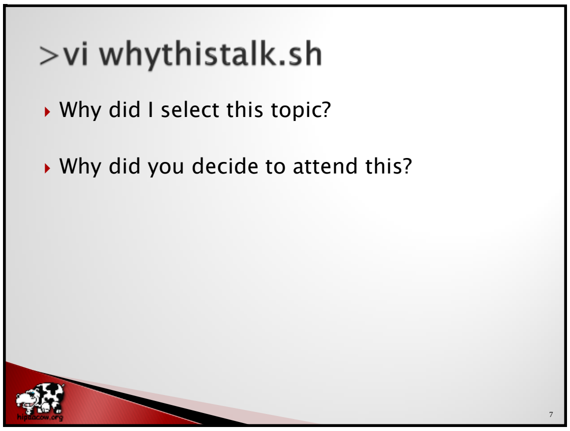
>gedit disclaimer.txt

- Here as a representative of a "hacker", and not representative of $employer
- "I'm not here to call your baby ugly, I'm here to make sure the crib is safe."



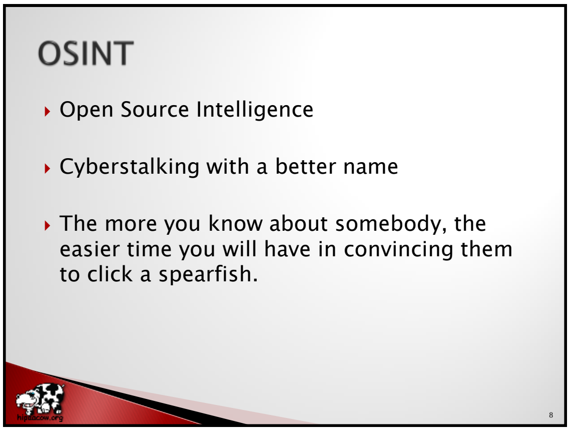
>man hacker

- White hat vs black hat vs grey hat
- What shade am I, what shade are you?
- Do you crack password hashes in your organization?
  - You should, and this is an example of doing things that are just a little bit grey.
- Slide titles so far have been linux commands



>vi whythistalk.sh

- Why did I select this topic?
- Why did you decide to attend this?



OSINT

- Open Source Intelligence
- Cyberstalking with a better name
- The more you know about somebody, the easier time you will have in convincing them to click a spearfish.

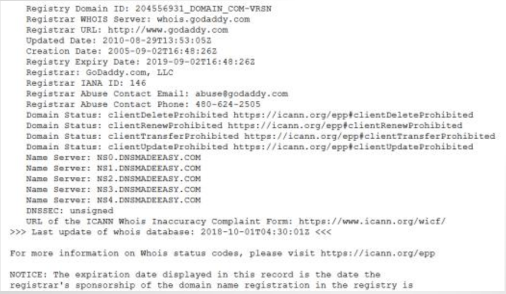
OSINT

- Let's talk free
- Or cheap
- Or shared
- And with a light touch, which makes defenses difficult

Whois

- Used to gather contact names, DNS information, other data
- Can start at internic.net/whois.html
- Then dig to the domain registrar's site (Like Network Solutions or GoDaddy)
- GDPR changed this a little, but we're still finding a lot of data out there

Whois

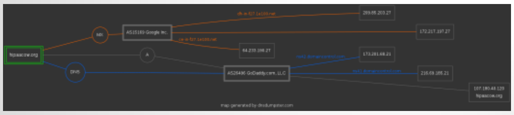


```
   Registry Domain ID: 204556931_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2010-08-29T13:53:05Z
   Creation Date: 2005-09-02T16:48:26Z
   Registry Expiry Date: 2019-09-02T16:48:26Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS0.DNSMADEEASY.COM
   Name Server: NS1.DNSMADEEASY.COM
   Name Server: NS2.DNSMADEEASY.COM
   Name Server: NS3.DNSMADEEASY.COM
   Name Server: NS4.DNSMADEEASY.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2018-10-01T04:30:01Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
```

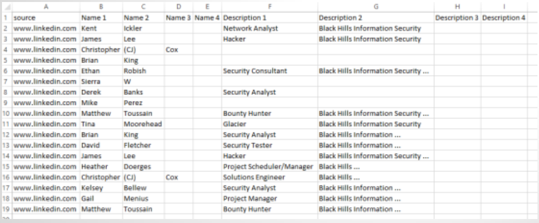
DNS Dumpster



LinkedIn data

- Burp Suite has an extension that will just scrape Google's crawling of LinkedIn sites.
- You'll get the output quick, and it can be parsed into Excel very quick as well.

LinkedIn data



	A	B	C	D	E	F	G	H	I
1	source	Name 1	Name 2	Name 3	Name 4	Description 1	Description 2	Description 3	Description 4
2	www.linkedin.com	Kent	Ickler			Network Analyst	Black Hills Information Security		
3	www.linkedin.com	James	Lee			Hacker	Black Hills Information Security		
4	www.linkedin.com	Christopher	(CJ)	Cox					
5	www.linkedin.com	Brian	King						
6	www.linkedin.com	Ethan	Robish			Security Consultant	Black Hills Information Security ...		
7	www.linkedin.com	Sierra	W						
8	www.linkedin.com	Derek	Banks			Security Analyst			
9	www.linkedin.com	Mike	Perez						
10	www.linkedin.com	Matthew	Toussain			Bounty Hunter	Black Hills Information Security ...		
11	www.linkedin.com	Tina	Moorehead			Glacier	Black Hills Information Security		
12	www.linkedin.com	Brian	King			Security Analyst	Black Hills Information ...		
13	www.linkedin.com	David	Fletcher			Security Tester	Black Hills Information ...		
14	www.linkedin.com	James	Lee			Hacker	Black Hills Information Security ...		
15	www.linkedin.com	Heather	Doerges			Project Scheduler/Manager	Black Hills ...		
16	www.linkedin.com	Christopher	(CJ)	Cox		Solutions Engineer	Black Hills ...		
17	www.linkedin.com	Kelsey	Bellew			Security Analyst	Black Hills Information ...		
18	www.linkedin.com	Gail	Menius			Project Manager	Black Hills Information ...		
19	www.linkedin.com	Matthew	Toussain			Bounty Hunter	Black Hills Information ...		

Level up the OSINT

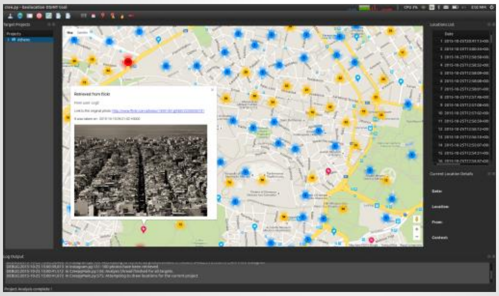
- Starts to get a little creative and creepy
- Carsowners.net
  - Let's search Google for site:carsowners.net "Jon Read"
  - Look at the results
  - It gives us: Type of car he drives, address, phone number, and VIN.
- Can pivot and start searching by phone number, or address, or VIN.

Getting cree.py

- Cree.py is an OSINT geolocation tool. It can pull from Flickr, Google+, Instagram, and Twitter.
- Good feature is to search by location, to within 100 meters, and list users that have posted from there.
- Search the GPS location of your target, and start getting a list of twitter users from there.
- Pivot, pivot, pivot.

hipposcow.org

Getting cree.py



hipposcow.org

Many more sources

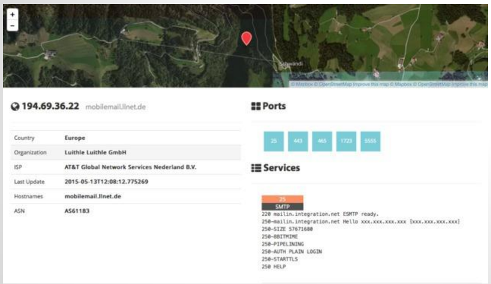
- Such a very long list.
  - WI Circuit Court Access
  - PowerMeta
  - FOCA (Fingerprinting Online Collected Archives)
  - Twitter Advanced Search

hipposcow.org

Shodan

- This is basically the Google of service banners
- Attackers can ask Shodan for a list ftp banners, or telnet, and results will display.
- Can also search by IP range, hostname…things from previous recon
- Example: cisco net:“216.219.143.0/24”

Shodan


+
−
Schwandi
© Mapbox © OpenStreetMap Improve this map © Mapbox © OpenStreetMap Improve this map

194.69.36.22 mobilemail.llnet.de

Country	Europe
Organization	Luithle Luithle GmbH
ISP	AT&T Global Network Services Nederland B.V.
Last Update	2015-05-13T12:08:12.775269
Hostnames	mobilemail.llnet.de
ASN	AS61183

Ports

25 443 465 1723 5555

Services

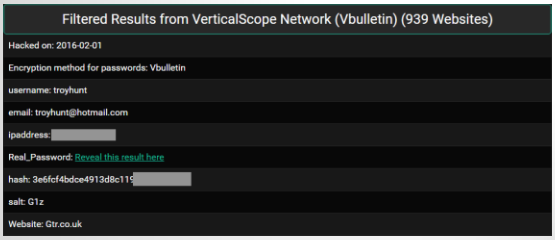
25
SMTP

```
220 mailin.integration.net ESMTP ready.
250-mailin.integration.net Hello xxx.xxx.xxx.xxx [xxx.xxx.xxx.xxx]
250-SIZE 57671680
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
```

PunkSpider

- Such a very long list.
  - WI Circuit Court Access
  - PowerMeta
  - FOCA
  - Twitter Advanced Search

Leakedsource



Filtered Results from VerticalScope Network (Vbulletin) (939 Websites)

Hacked on: 2016-02-01

Encryption method for passwords: Vbulletin

username: troyhunt

email: troyhunt@hotmail.com

ipaddress: [redacted]

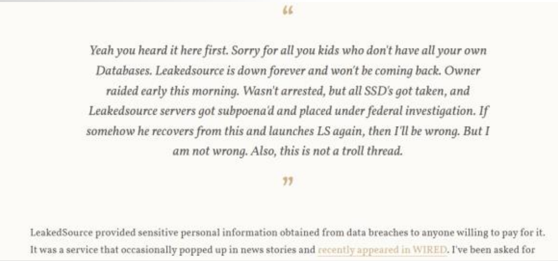
Real_Password: Reveal this result here

hash: 3e6fcf4bdce4913d8c11[redacted]

salt: G1z

Website: Gtr.co.uk

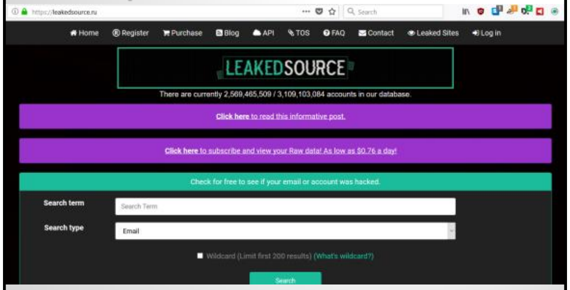
Leakedsource



> *Yeah you heard it here first. Sorry for all you kids who don't have all your own Databases. Leakedsource is down forever and won't be coming back. Owner raided early this morning. Wasn't arrested, but all SSD's got taken, and Leakedsource servers got subpoena'd and placed under federal investigation. If somehow he recovers from this and launches LS again, then I'll be wrong. But I am not wrong. Also, this is not a troll thread.*

LeakedSource provided sensitive personal information obtained from data breaches to anyone willing to pay for it. It was a service that occasionally popped up in news stories and recently appeared in WIRED. I've been asked for

Whoops.



There are currently 2,569,465,509 / 3,109,103,084 accounts in our database.

Click here to read this informative post.

Click here to subscribe and view your Raw data! As low as $0.76 a day!

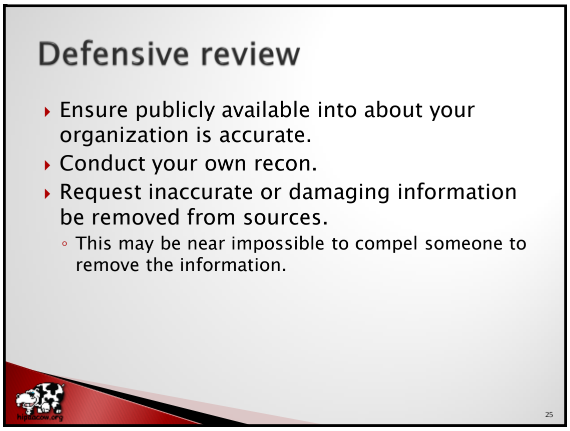
Check for free to see if your email or account was hacked.

Search term: Search Term

Search type: Email

□ Wildcard (Limit first 200 results) (What's wildcard?)

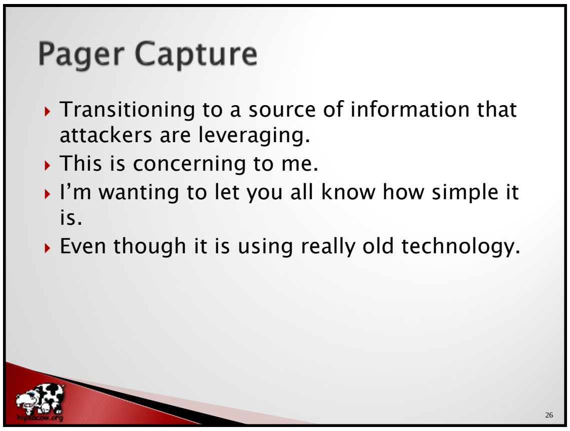
Search



Defensive review

- Ensure publicly available into about your organization is accurate.
- Conduct your own recon.
- Request inaccurate or damaging information be removed from sources.
  - This may be near impossible to compel someone to remove the information.

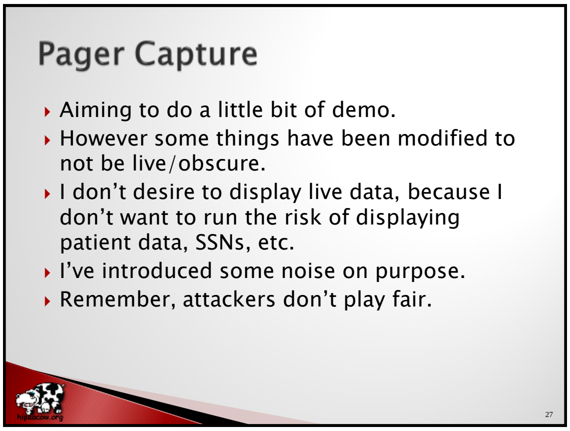
25



Pager Capture

- Transitioning to a source of information that attackers are leveraging.
- This is concerning to me.
- I'm wanting to let you all know how simple it is.
- Even though it is using really old technology.

26



Pager Capture

- Aiming to do a little bit of demo.
- However some things have been modified to not be live/obscure.
- I don't desire to display live data, because I don't want to run the risk of displaying patient data, SSNs, etc.
- I've introduced some noise on purpose.
- Remember, attackers don't play fair.

27

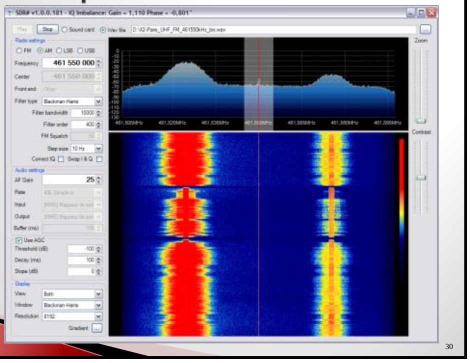
Software-Defined Radio

- Using some inexpensive receivers (they work for as low as $20)
- And FREE software, in SDR# and PDW
- You can receive live pages over the air, display them on screen, or capture in a log to put together later
- Let's do a demo

SDR Sharp

- Set up and tune to the pager frequency.
- Capture and relay that audio to a decoder program (PDW in this case).
- Note: This is not on protected bands (like cellular) and it is decoding, not breaking encryption.

SDR Sharp



SDR# v1.0.0.181 - IQ Imbalance: Gain = 1,110 Phase = -0,801°

Play | Stop | ○ Sound card | ● Wav file | D:\IQ\Pass_UHF_FM_461550kHz_bis.wav

Radio settings
○ FM ● AM ○ LSB ○ USB
Frequency 461 550 000
Center 461 550 000
Front end Other
Filter type Blackman-Harris
Filter bandwidth 10000
Filter order 400
FM Squelch 50
Step size 10 Hz
Correct IQ □ Swap I & Q □

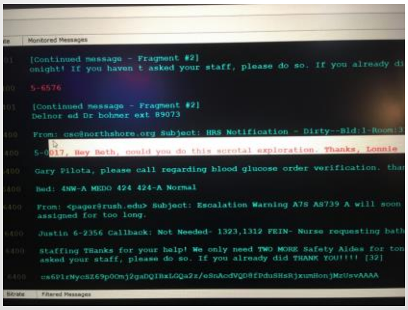
Audio settings
AF Gain 25
Rate 48k Sample/s
Input [MME] [illegible]
Output [MME] [illegible]
Buffer (ms) 100
☑ Use AGC
Threshold (dB) -100
Decay (ms) 100
Slope (dB) 0

Display
View Both
Window Blackman-Harris
Resolution 8192
Gradient ...

SDR Sharp

- What sort of things have I seen:
  - SSNs in clear text
  - Patients and mental states
  - Patients on their way in, ambulance page-ahead
  - Patients under arrest, and tazed
  - Should look at some sample results, either provided by external contacts, some live data here, or screenshots

Pager Capture Results



```
[Continued message - Fragment #2]
onight! If you haven t asked your staff, please do so. If you already di

5-6576

[Continued message - Fragment #2]
Delnor ed Dr bohmer ext 89073

From: csc@northshore.org Subject: HRS Notification - Dirty--Bld:1-Room:3

5-0017, Hey Beth, could you do this scrotal exploration. Thanks, Lonnie

Gary Pilota, please call regarding blood glucose order verification. thar

Bed: 4NW-A MEDO 424 424-A Normal

From: <pager@rush.edu> Subject: Escalation Warning A7S AS739 A will soon
assigned for too long.

Justin 6-2356 Callback: Not Needed- 1323,1312 FEIN- Nurse requesting bath

staffing THanks for your help! We only need TWO MORE Safety Aides for ton
asked your staff, please do so. If you already did THANK YOU!!!! [32]

cs6PlrNycSZ69p0Omj2gaDQIBxLGQa2z/eSnAcdVQD8fPduSHsRjxumHonjMzUsvAAAA
```

Conclusions

- Some soapbox
  - Wizards impressing other wizards
  - Does this look compliant to you?
- Defensive Review
- Questions