RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

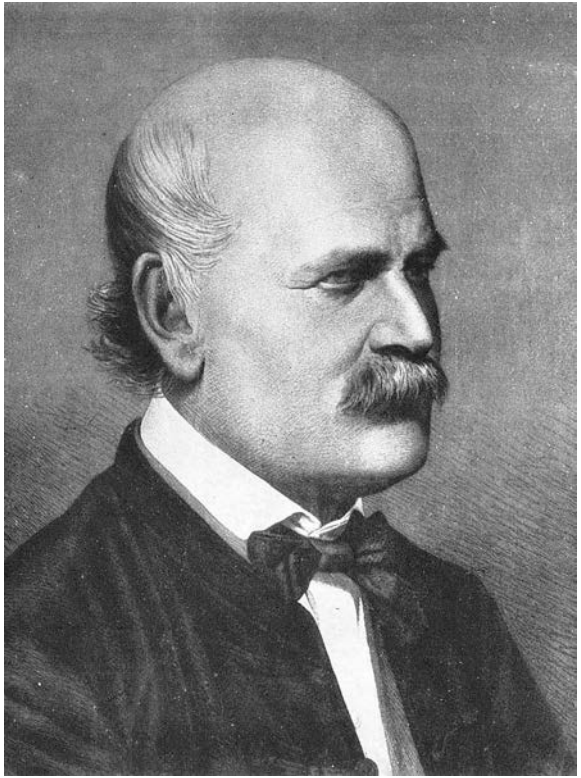
SESSION ID: HUM-W11

From Boot-to-Root
A Method for Successful Security Training

Dave Farrow
Senior Director, Information Security
Barracuda Networks, Inc.

The Stakes

Ignaz Semmelweis: a familiar story…



WHY?!?

- Bad news triggers the grief cycle:
  - Denial, anger, bargaining, depression, acceptance
- Hygeine (security) is only **indirectly** part of their primary purpose
  - The doctors were there to deliver babies… and not infect their patients
  - Developers are here to deliver features… and not introduce vulnerabilities

Aha!

We all agree that we must “First, do no harm”

Q: So how do we (the security team)

- Avoid the mistakes Ignaz made
- Which perpetuated the mistakes the doctors were making?

A: Invite them (the developers) into the “club”**…before** there is a crisis

Joining the club

- Inducts developers into the attacker's dark art
- Removes the mystery which had fueled the grief cycle
- Creates a connection between security and developers

Security starts to become second nature and the grief cycle is short circuited

Our invitation: boot2root

- Well known security gaming exercises
  - Participants start with a VM created with specific security flaws
  - They boot the VM and proceed through a variety of challenges
  - Eventually winning by gaining root access on the VM
- Related to, but different from, Capture the Flag contests
- Virtual machines allow us to “manufacture cadavers to autopsy”

Take that, Medicine!

RSAConference2017

Preparing the Training

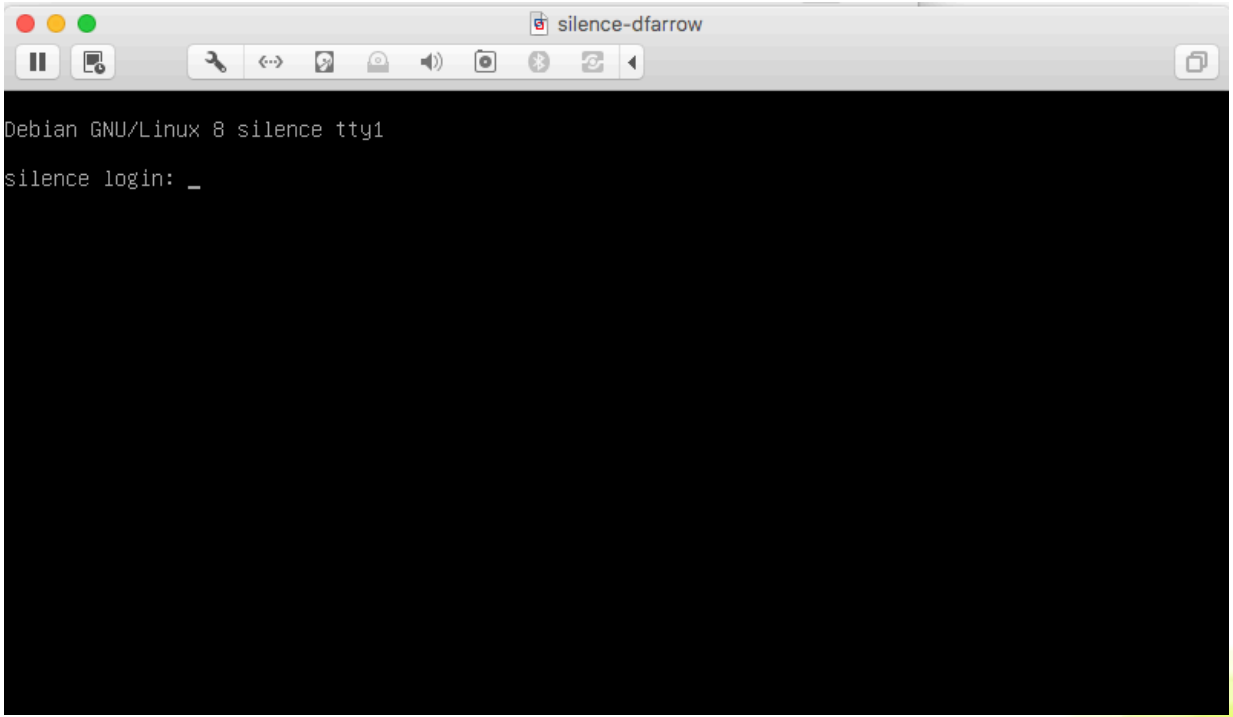
Steps for preparation

1. Set objectives
2. Create a narrative
3. Build the exercise and training material
4. Practice coaching

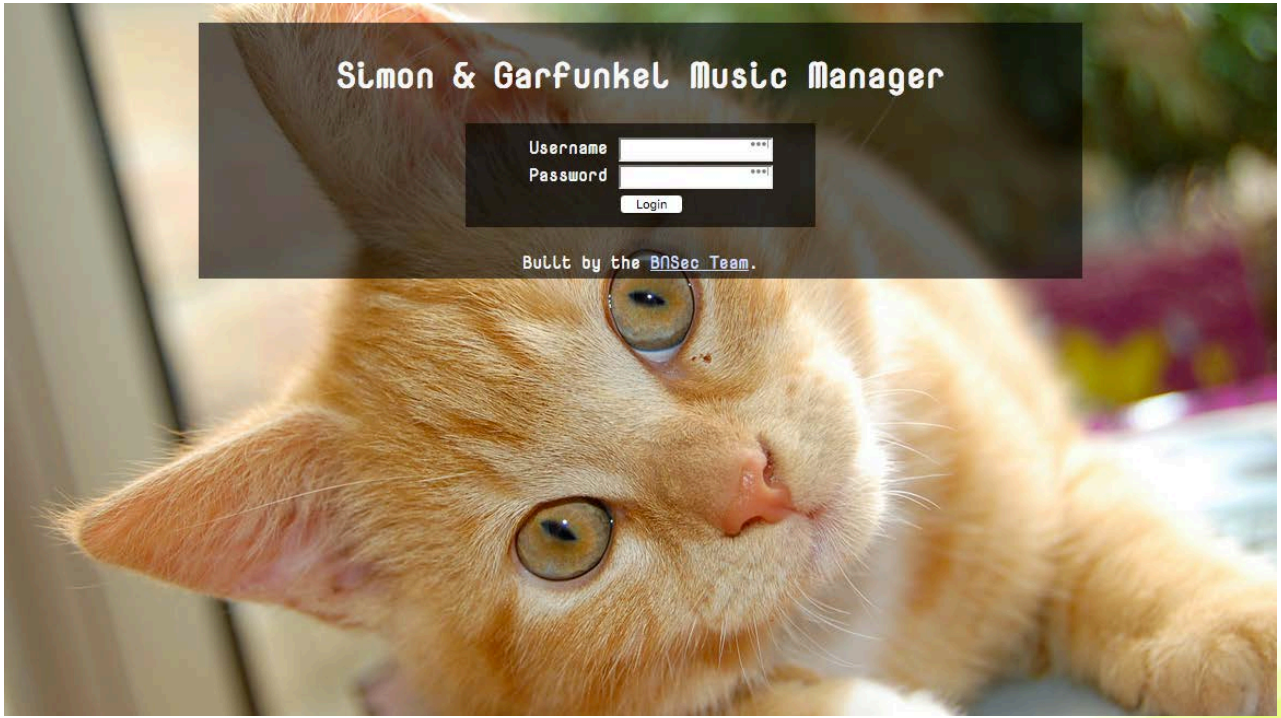
Example Objectives

- Operational
  - SSH key forwarding
  - Keeping a clean shop
- Coding
  - SQLi
  - CMDi
- Post exploitation
  - Privilege escalation
  - System misconfigurations

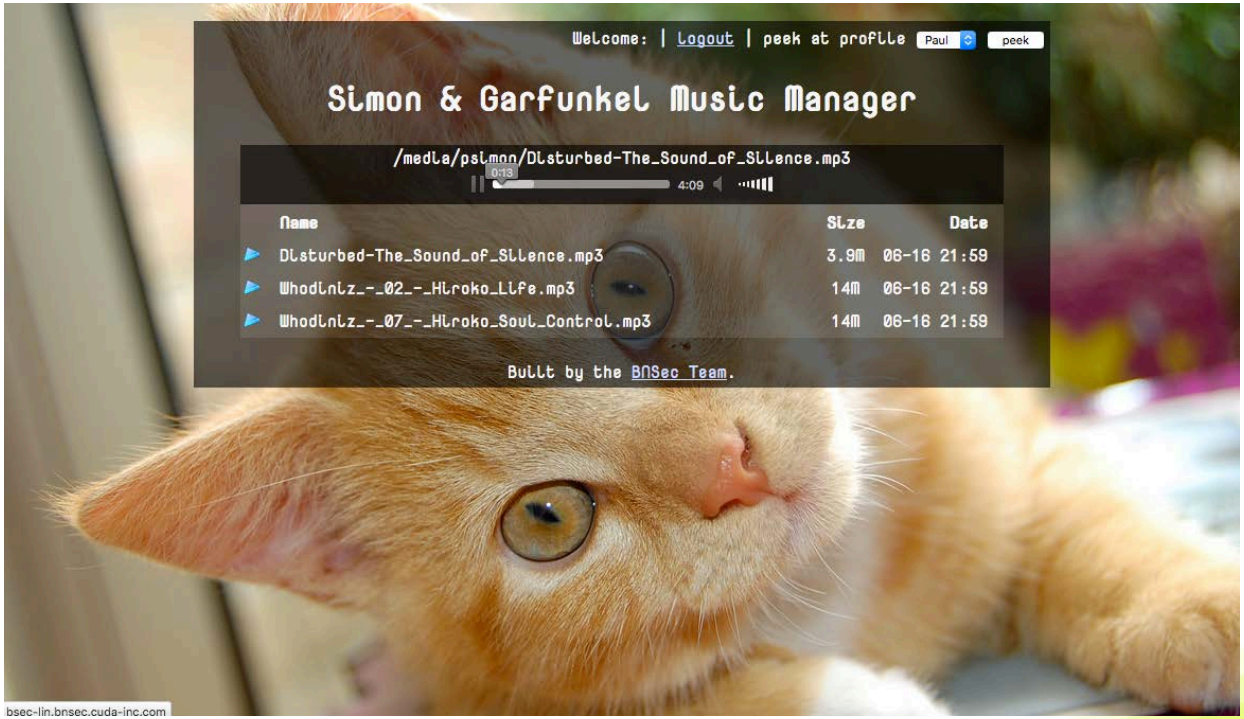
Narrative step 1: find the machine



Narrative step 2: bypass authentication



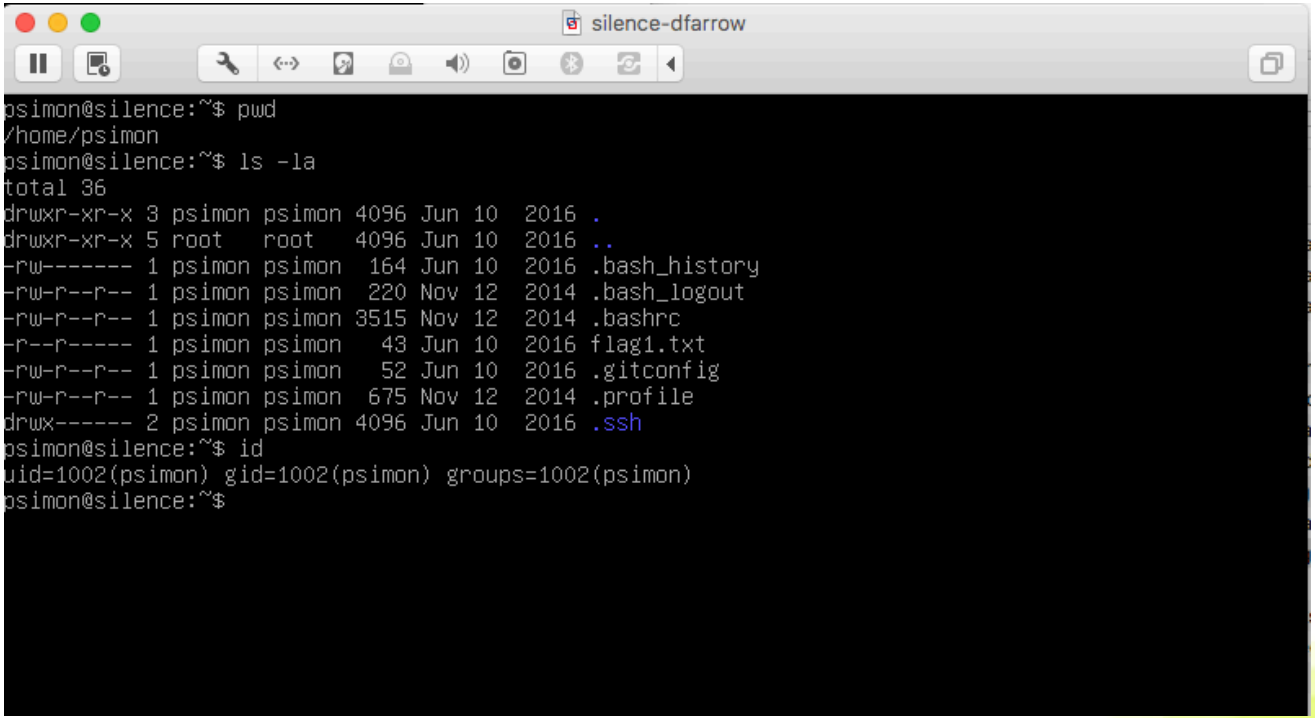
Narrative step 3: command injection



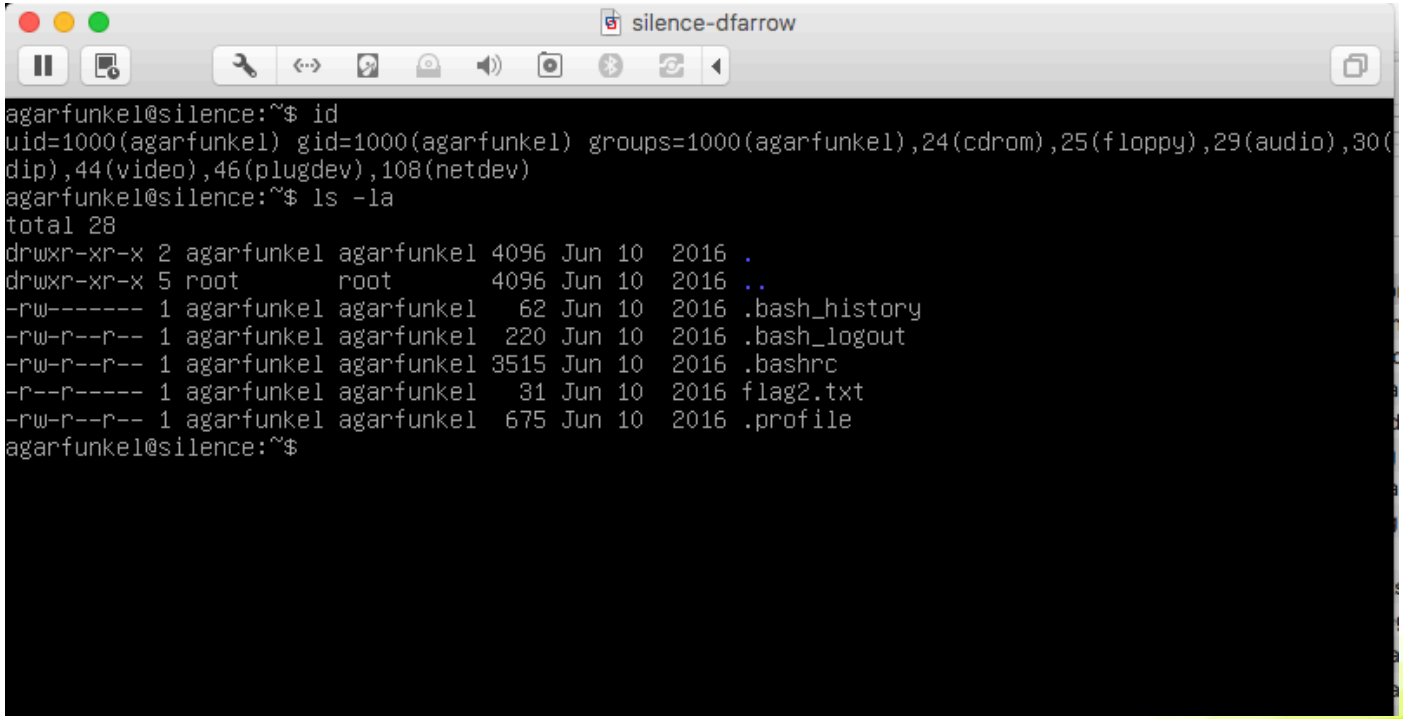
Narrative step 4: reverse shell

```
kali [~]: nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.24.11] from (UNKNOWN) [192.168.24.146] 42174
hostname
silence
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
ls -l /var/www/html
total 40
-rw-r--r-- 1 root root  166 Jun 16 21:59 dbconfig.pl
-rw-rw-r-- 1 root root   30 Jun 16 21:59 flag0_zHHkyfZJUWnx.txt
drwxr-xr-x 2 root root 4096 Jun 16 21:59 images
-rwxr-xr-x 1 root root 6880 Jun 16 21:59 index.bak
-rwxr-xr-x 1 root root 6880 Jun 16 21:59 index.pl
drwxr-xr-x 4 root root 4096 Jun 16 21:59 media
drwxr-xr-x 2 root root 4096 Jun 16 21:59 styles
drwxr-xr-x 2 root root 4096 Jun 16 21:59 templates
```

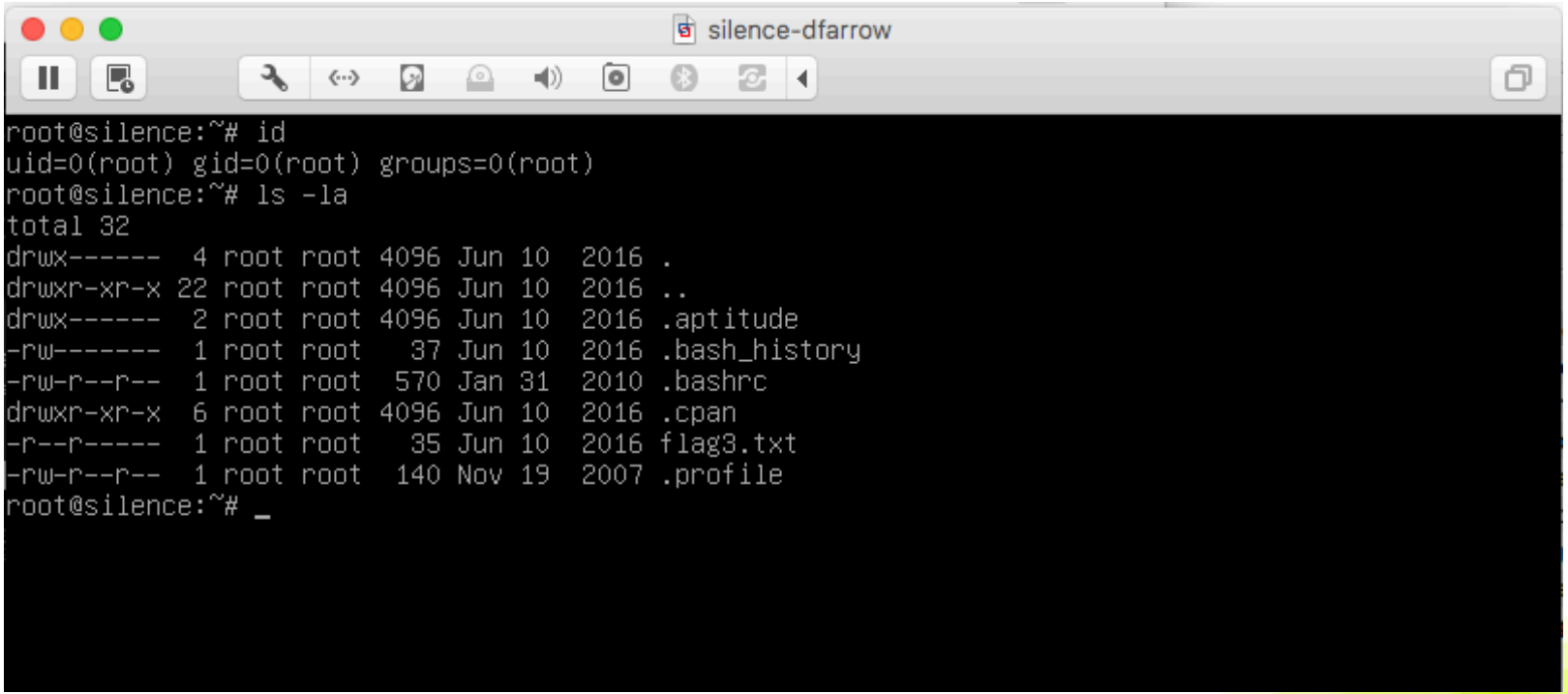
Narrative step 5: low priv user - psimon



Narrative step 6: low priv user - agarfunkel



Narrative step 7: Qapla!



Building silence

- Built using a 32-bit linux OS for max supportability
- Package for VMWare and Virtualbox
- Automate the build – you will end up building it repeatedly
- Test the boot2root
  - Watch for unintended “ways forward”
  - Validate the playability
  - Clean up!
- Leave easter eggs!

Presentation materials

- Use (and reference) existing online materials
- Present materials in the same order as the narrative
- Develop some demonstration scripts
- Balance offensive with defensive information

RSAConference2017

Game Day

Game day

- Logistics
  - Reserved 4-6 hours
  - Invited entire technical team in the location
  - Took 4-5 members of the security team to support/coach
- Observations
  - Once the boot2root started, it was heads down… the whole time
  - People work alone or in small groups; but everyone had their own machine
  - As we got better at coaching, more people completed the entire exercise

RSAConference2017

Lessons Learned

Responses from participants

- Post event surveys indicate: boot2root has what developers crave
- Some participant feedback:
  - “I had wanted to hack but didn’t know where to start”
  - “I grabbed another boot2root from vulnhub on my own last weekend”
  - “I’d like to be involved with building the next one”
  - “I’m now officially terrified of what is possible. And I’ll be calling you about my own code”
- Many participants who didn’t finish the first time enthusiastically came to the next event to make more progress

Challenges

- Getting participants up and running
  - Standardize on a supported VM platform
  - Hand out the image early so people can set it up before the training
  - Participants should come to the exercise with prerequisites installed
- Game dependencies
  - Make your exercise completely stand alone
- Insufficient time
  - Consider alternating teaching and applying
  - Don’t expect attendees to finish the entire exercise the first time

Coaching: where the magic happens

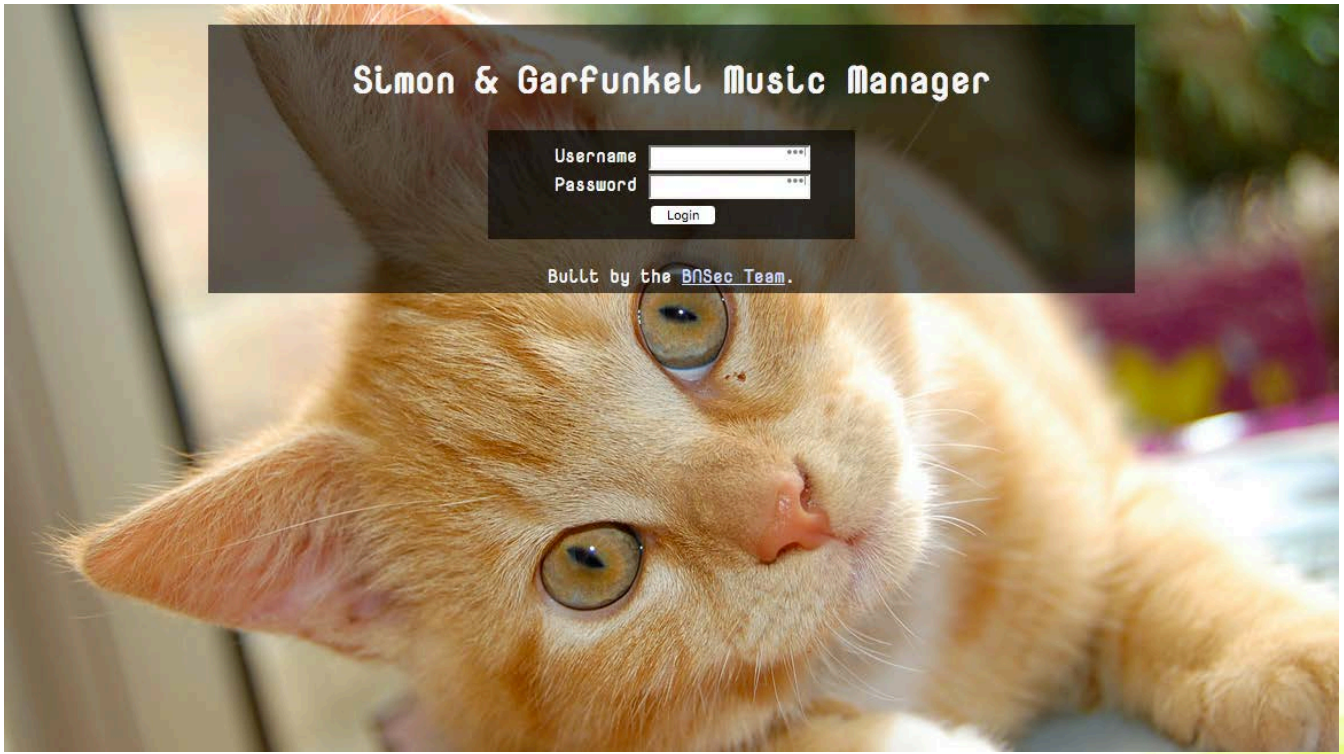
By proctoring the exercise and offering one-on-one coaching, your security team can…

- Develop the language to communicate effectively with developers
- Create for developers a positive association with security and your team
- Reveal how your security team really feels about vulnerabilities

Coaching basics

- Do the exercise yourselves before you deliver a boot2root
- Be prepared for a wide variety of experience
- Don’t spoil the fun… or the impact
- Manage frustration
- Too many coaches spoil the soup
- Stay engaged

Coaching example



Our next steps

- Technical
  - Build fixing into the exercise
  - Break tool setup into stand alone exercises
  - Considering using docker
- Organizational
  - Set up recurring training opportunities for existing and new hires
  - Set up company scoreboard
  - Have success with exercises contribute to job/career advancement?

Resources

- Complete source for Silence and the related training is available upon request
- I can be reached at:
  - dfarrow@barracuda.com
- Acknowledgments
  - Matt Trimble

What happened to Ignaz?

Apply: your next steps

- Create the pull to join the club, then welcome the developers in
  - And respect that they still have features to deliver
- If you choose to use boot2roots to do so:
  - Identify your objectives
  - Create a narrative
  - Develop the materials
  - Prepare to coach

Boot2roots are achieving these goals for us.

We'd love to hear what works for you.

Questions?