

RSA[®]Conference2017

San Francisco | February 13–17 | Moscone Center

POWER OF
OPPORTUNITY

SESSION ID: HUM-W11

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



Dave Farrow

Senior Director, Information Security
Barracuda Networks, Inc.

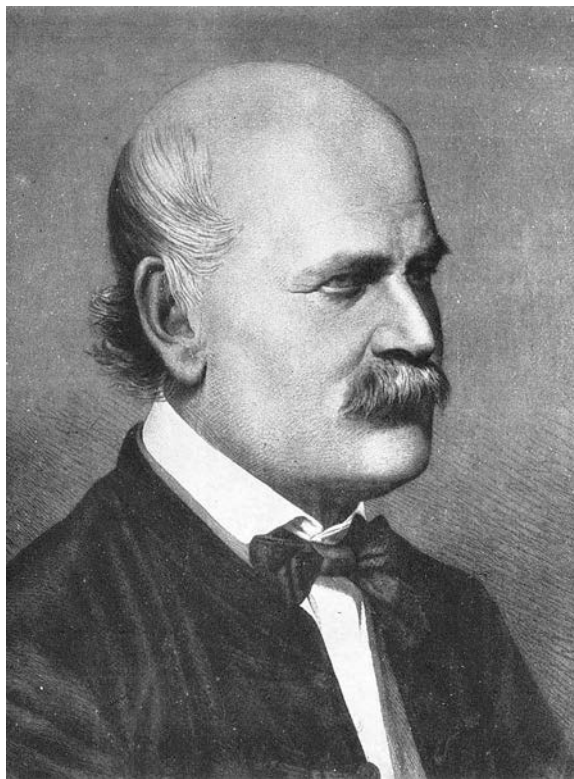
RSA®Conference2017

#RSAC

The Stakes

Ignaz Semmelweis: a familiar story...

#RSAC



WHY?!?

#RSAC

- Bad news triggers the grief cycle:
 - Denial, anger, bargaining, depression, acceptance
- Hygiene (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!

RSA®Conference2017

Preparing the Training

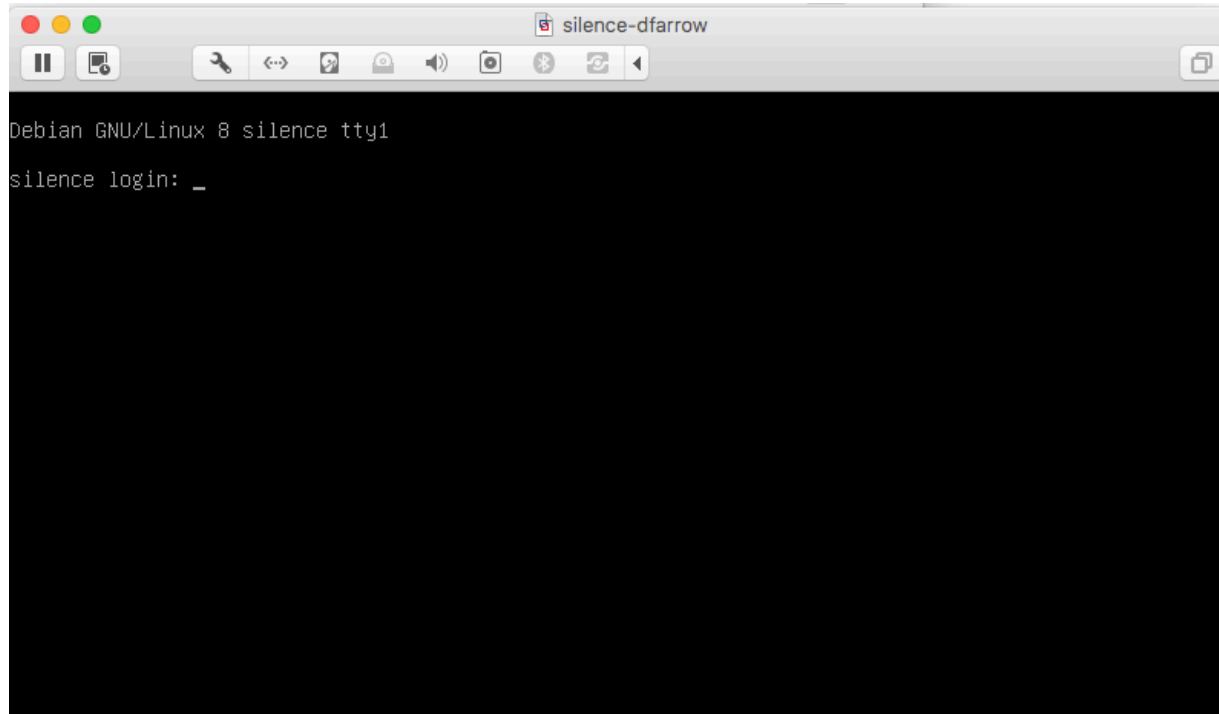
Steps for preparation

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

Example Objectives

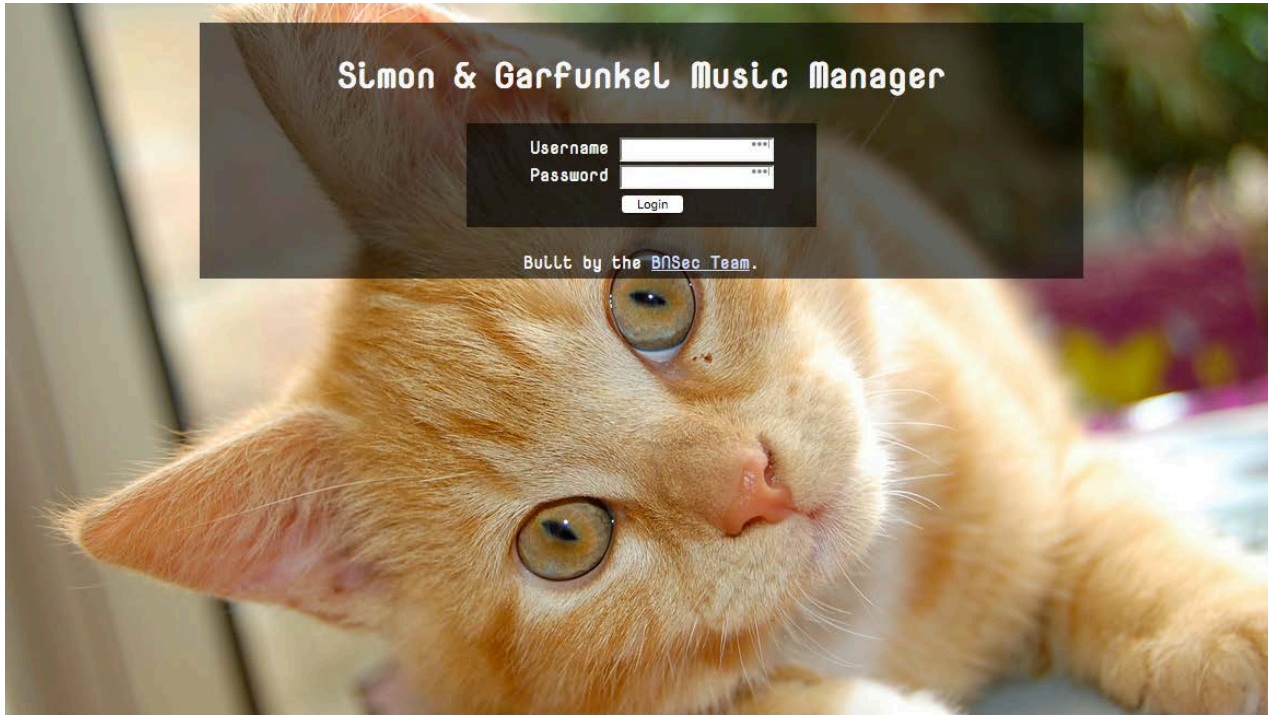
- Operational
 - SSH key forwarding
 - Keeping a clean shop
- Coding
 - SQLi
 - CMDi
- Post exploitation
 - Privilege escalation
 - System misconfigurations

Narrative step 1: find the machine

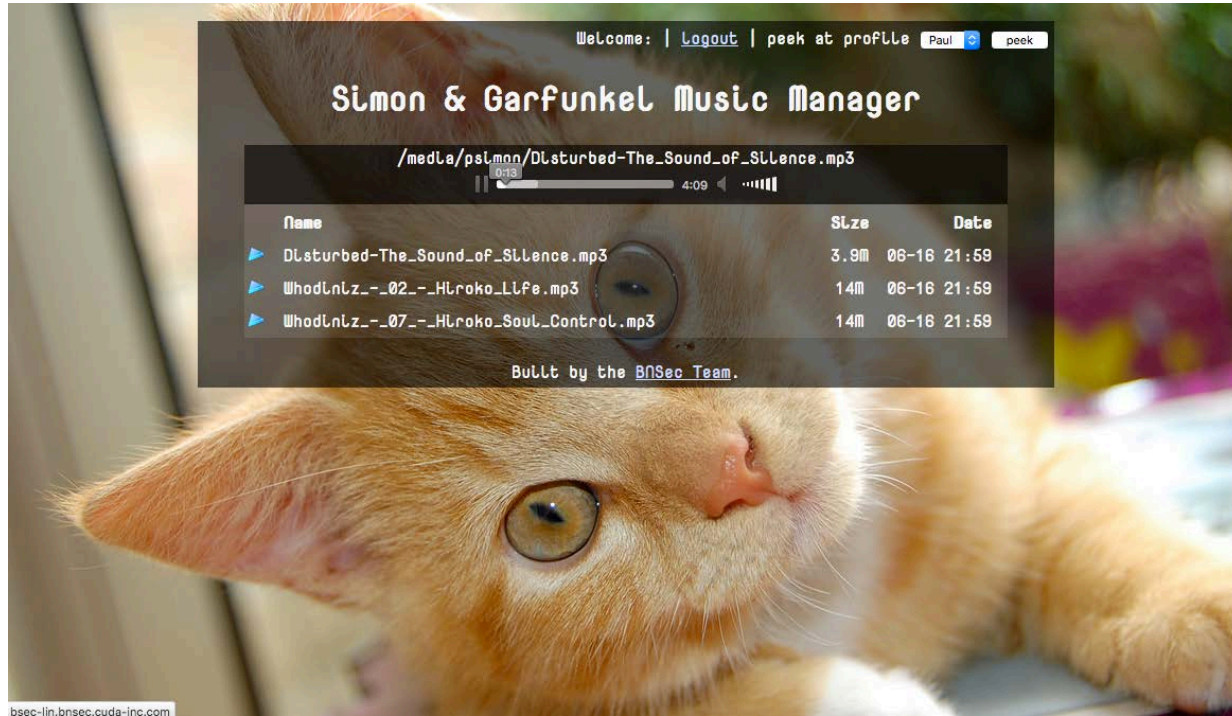


```
Debian GNU/Linux 8 silence tty1
silence login: _
```

Narrative step 2: bypass authentication



Narrative step 3: command injection

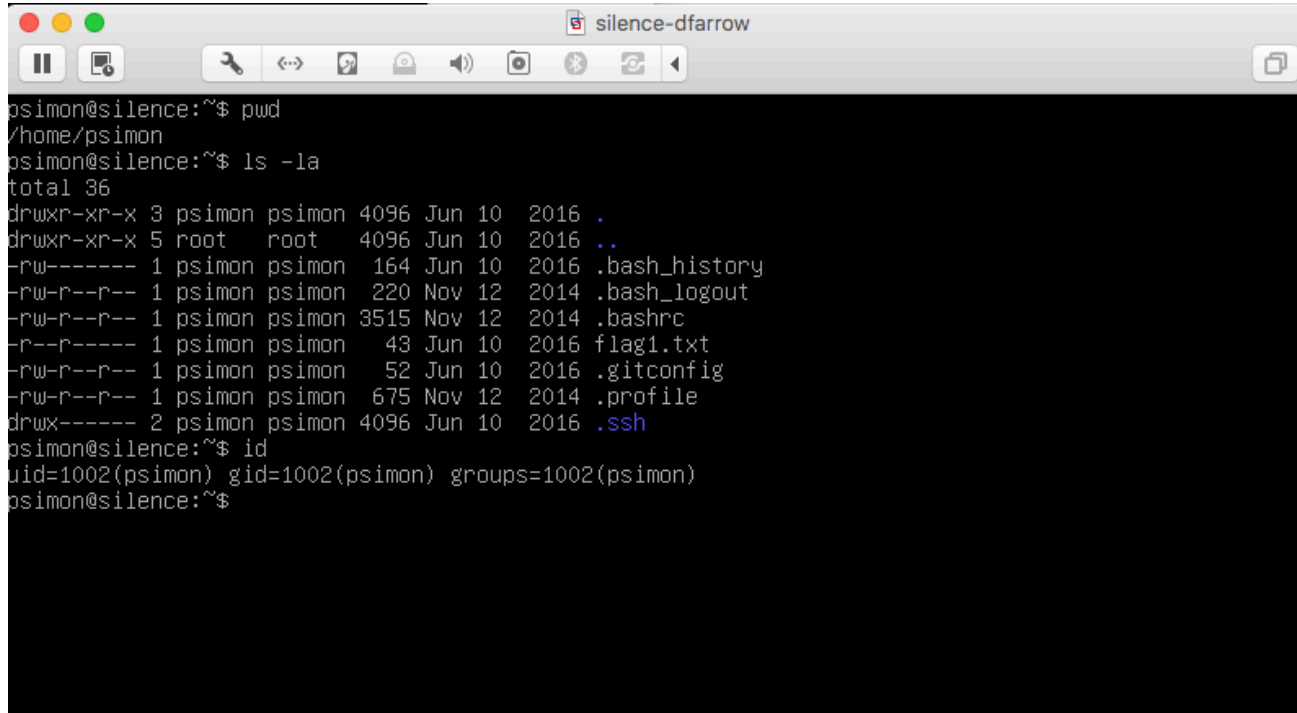


bsec-lin.bnsec.cuda-inc.com

Narrative step 4: reverse shell

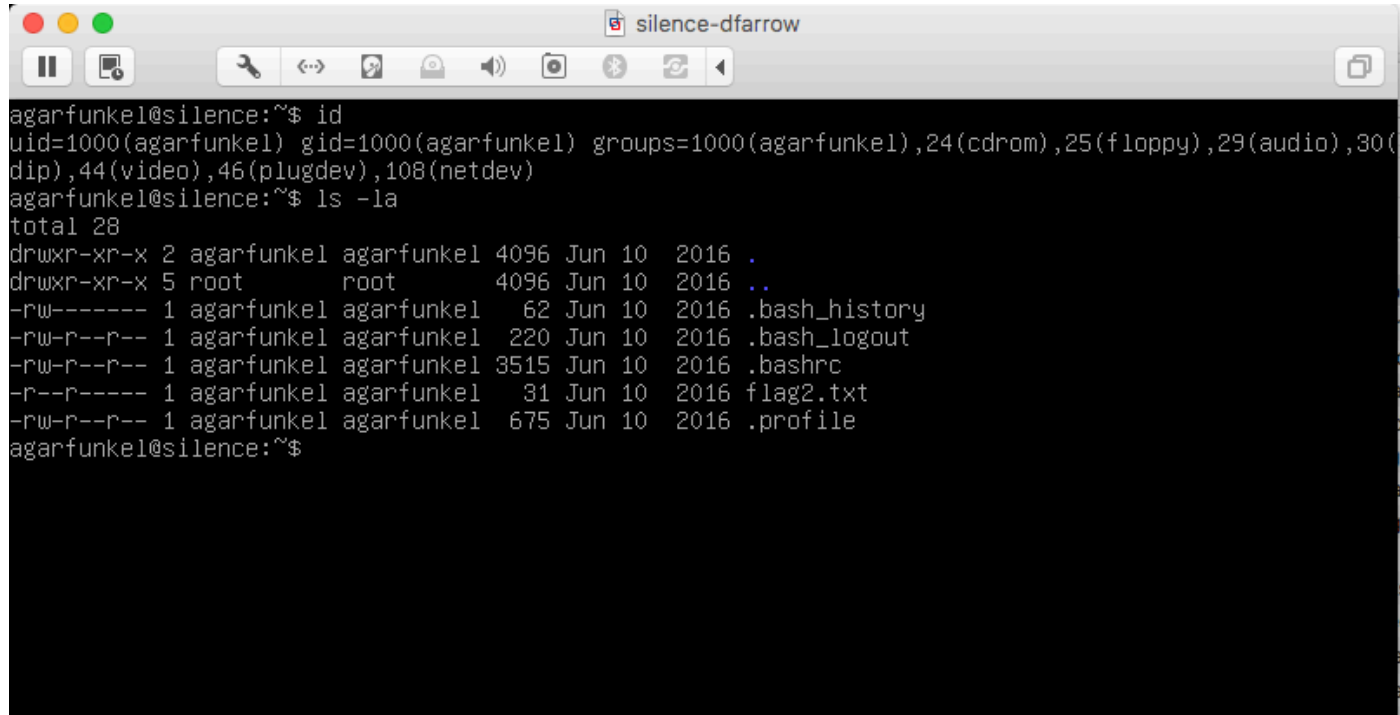
```
kali [~]: nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.24.11] from (UNKNOWN) [192.168.24.146] 42174
hostname
silence
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
ls -l /var/www/html
total 40
-rw-r--r-- 1 root root 166 Jun 16 21:59 dbconfig.pl
-rw-rw-r-- 1 root root 30 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



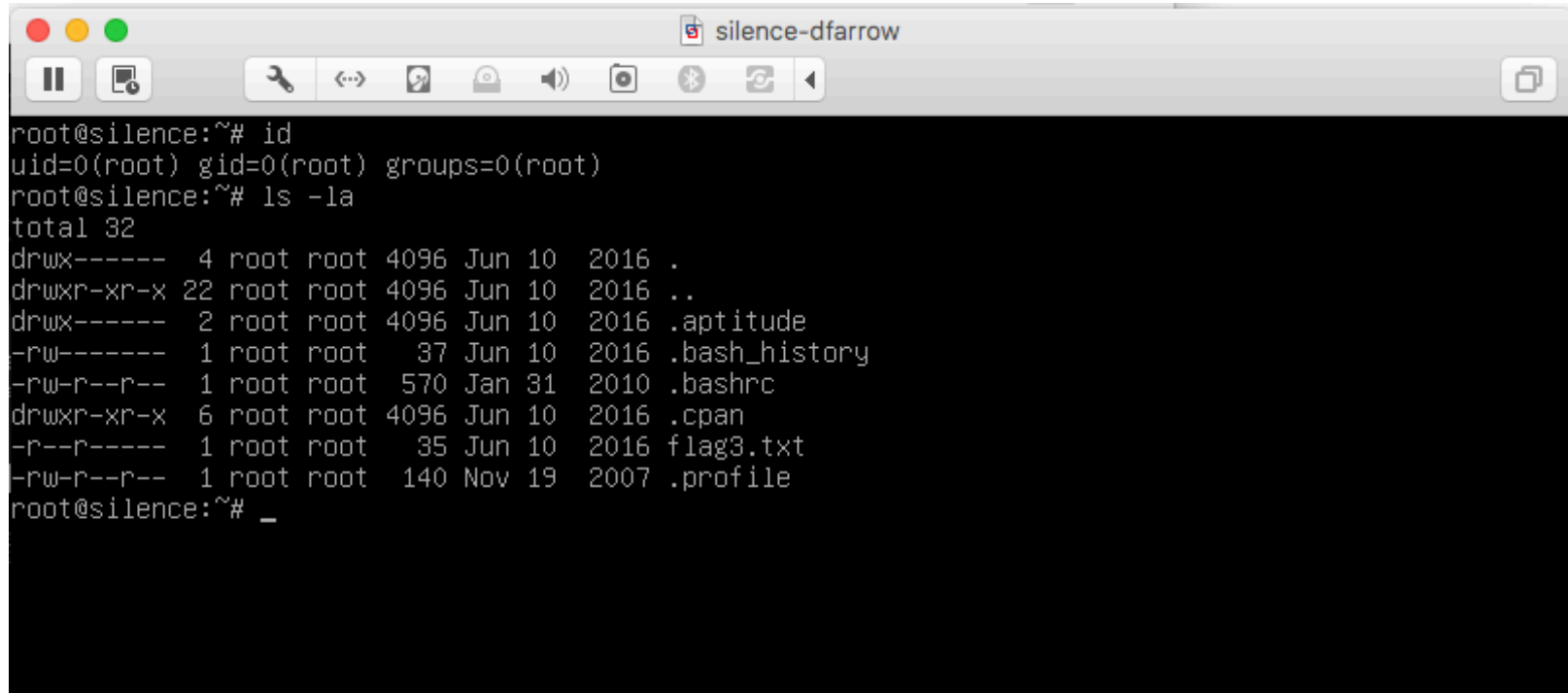
```
psimon@silence:~$ pwd
/home/psimon
psimon@silence:~$ ls -la
total 36
drwxr-xr-x 3 psimon psimon 4096 Jun 10 2016 .
drwxr-xr-x 5 root root 4096 Jun 10 2016 ..
-rw----- 1 psimon psimon 164 Jun 10 2016 .bash_history
-rw-r--r-- 1 psimon psimon 220 Nov 12 2014 .bash_logout
-rw-r--r-- 1 psimon psimon 3515 Nov 12 2014 .bashrc
-r--r----- 1 psimon psimon 43 Jun 10 2016 flag1.txt
-rw-r--r-- 1 psimon psimon 52 Jun 10 2016 .gitconfig
-rw-r--r-- 1 psimon psimon 675 Nov 12 2014 .profile
drwx----- 2 psimon psimon 4096 Jun 10 2016 .ssh
psimon@silence:~$ id
uid=1002(psimon) gid=1002(psimon) groups=1002(psimon)
psimon@silence:~$
```

Narrative step 6: low priv user - agarfunkel



```
agarfunkel@silence:~$ id
uid=1000(agarfunkel) gid=1000(agarfunkel) groups=1000(agarfunkel),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev)
agarfunkel@silence:~$ ls -la
total 28
drwxr-xr-x  2 agarfunkel agarfunkel 4096 Jun 10  2016 .
drwxr-xr-x  5 root        root      4096 Jun 10  2016 ..
-rw-----  1 agarfunkel agarfunkel   62 Jun 10  2016 .bash_history
-rw-r--r--  1 agarfunkel agarfunkel  220 Jun 10  2016 .bash_logout
-rw-r--r--  1 agarfunkel agarfunkel 3515 Jun 10  2016 .bashrc
-r--r-----  1 agarfunkel agarfunkel   31 Jun 10  2016 flag2.txt
-rw-r--r--  1 agarfunkel agarfunkel  675 Jun 10  2016 .profile
agarfunkel@silence:~$
```


Narrative step 7: Qapla!

A terminal window titled 'silence-dfarrow' showing a root shell session. The user runs 'id' and 'ls -la' to verify permissions and list files. The output shows root access and a list of files in the home directory.

```
root@silence:~# id
uid=0(root) gid=0(root) groups=0(root)
root@silence:~# ls -la
total 32
drwx----- 4 root root 4096 Jun 10 2016 .
drwxr-xr-x 22 root root 4096 Jun 10 2016 ..
drwx----- 2 root root 4096 Jun 10 2016 .aptitude
-rw----- 1 root root  37 Jun 10 2016 .bash_history
-rw-r--r-- 1 root root  570 Jan 31 2010 .bashrc
drwxr-xr-x 6 root root 4096 Jun 10 2016 .cpan
-r--r----- 1 root root  35 Jun 10 2016 flag3.txt
-rw-r--r-- 1 root root  140 Nov 19 2007 .profile
root@silence:~# _
```

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

RSA®Conference2017

#RSAC

Game Day

Game day

#RSAC

- 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

RSA®Conference2017

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

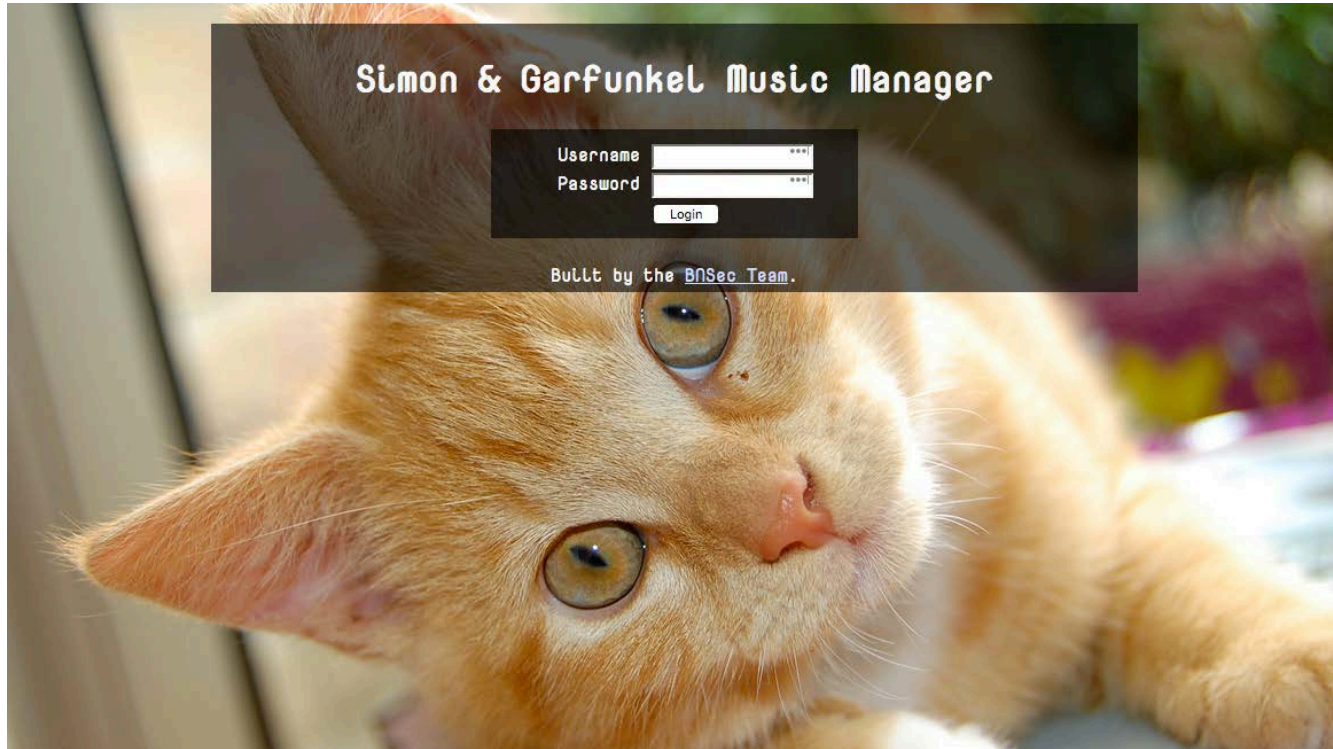
By proctoring the exercise and offering one-on-one coaching, your security team can...

- 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.

RSA®Conference2017

Questions?