TESTING OR HACKING

REAL ADVICE ON EFFECTIVE SECURITY TESTING STRATEGIES

DAN BILLING |
@THETESTDOCTOR

#TESTBASH

WE HAVE A PROBLEM

OUR
APPLICATIONS
AND SYSTEMS ARE
BEING HACKED

tunecore

CareFirst BlueCross BlueShield

TalkTalk

Sanrio

AdultFriendFinder

Support us on patreon

Paysafe

TF1.fr

Ashley Madison®.com

Scottrade®

vtech®

000webhost.com

Carphone Warehouse

Source: hackmageddon.com

TESTING CAN HELP

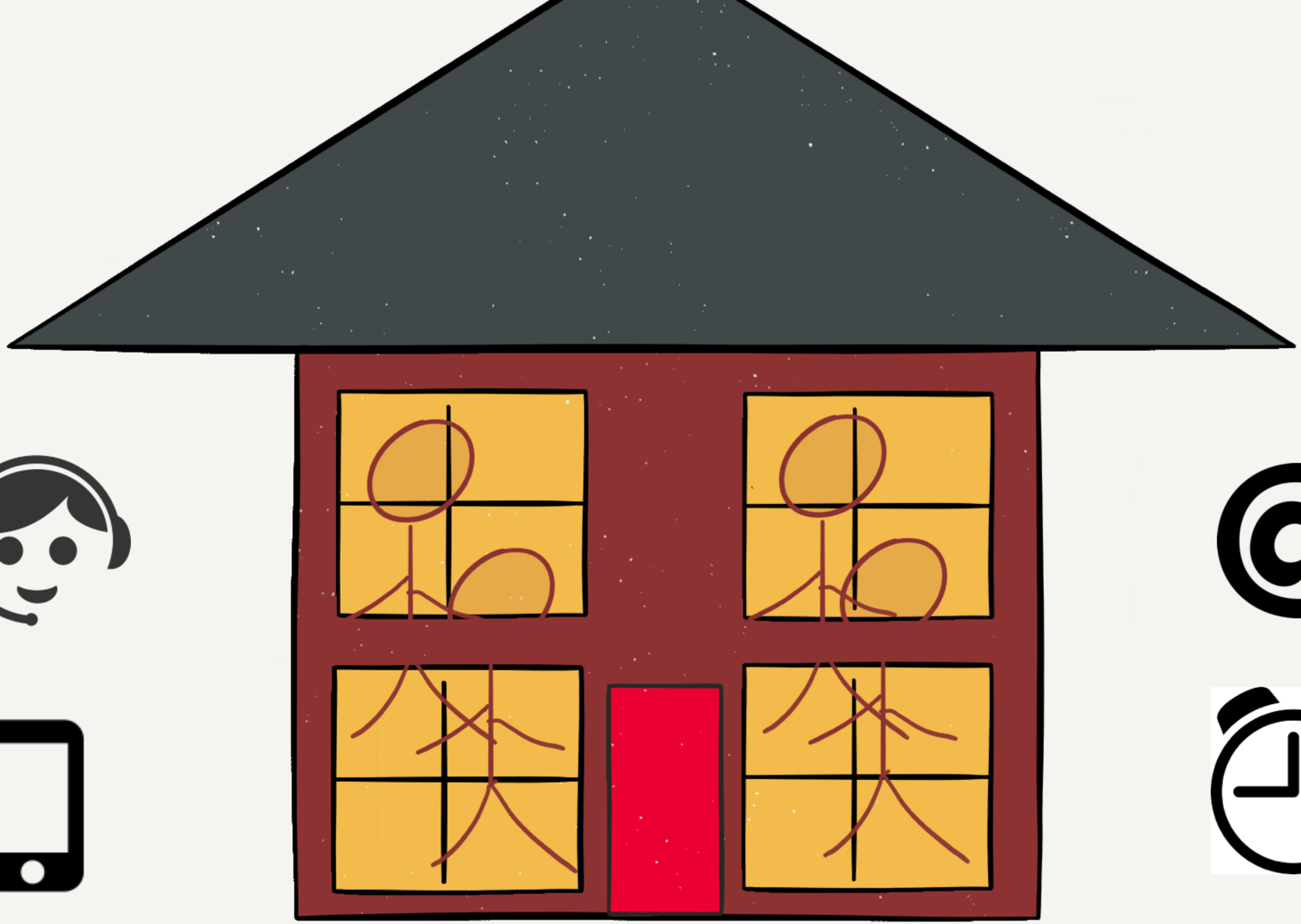
SECURITY
SHOULD BE
PART OF THE
CONVERSATION

WE NEED TO
LEARN FROM
THE HACKERS

“Hackers…they just might be the immune system for the information age…sometimes they make us sick, and they make us fix it.”

Keren Elazari @k3e3n3
Cyber Security Researcher, TED 2014

MY TESTING CONTEXT




Alaska (US)
Bering Sea
Greenland (Dk.)
Greenland Sea
Baffin Bay
Hudson Bay
Gulf of Alaska
Iceland
Norwegian Sea
Barents Sea
C a n a d a
R u s s i a
PACIFIC
OCEAN
United States
Mexico
Gulf of Mexico
ATLANTIC
OCEAN
Sweden
Finland
Norway
Ukraine
Kazakhstan
Mongolia
China
Japan
South Korea
North Korea
East China Sea
Sea of Ochotsk
Sea of Japan
Spain
Portugal
Italy
Greece
Turkey
Mediterranean Sea
Black Sea
Iran
Afghanistan
Pakistan
India
Saudi Arabia
Oman
Yemen
Arabian Sea
Bay of Bengal
Morocco
Algeria
Libya
Egypt
Mauritania
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
Somalia
Kenya
Tanzania
Angola
Zambia
Namibia
Botswana
South Africa
Madagascar
Democr. Rep. of the Congo
Cameroon
Cuba
Caribbean Sea
Venezuela
Colombia
Peru
Brazil
Bolivia
Paraguay
Argentina
Chile
Uruguay
Equator
Tropic of Cancer
Tropic of Capricorn
INDIAN
OCEAN
Philippines
Malaysia
Indonesia
South China Sea
Papua New Guinea
Australia
Coral Sea
Tasman Sea
New Zealand
French Polynesia
Kiribati
Vietnam
Thailand
Myanmar (Burma)
Sri Lanka
Falkland Islands (GB)
South Georgia (GB)
Cape Horn

WHY DO WE NEED TO DO SECURITY TESTING?

THAT'S OUT
OF SCOPE

WE ARE

OUTSOURCING

THAT

THAT'S A NON FUNCTIONAL REQUIREMENT

WE DON'T HAVE
THE SKILLS

WE NEED TO
DELIVER FAST, NOT
SLOW THINGS
DOWN

I THINK WE NEED
TO DO SOME
SECURITY TESTING

WHERE DO WE START?

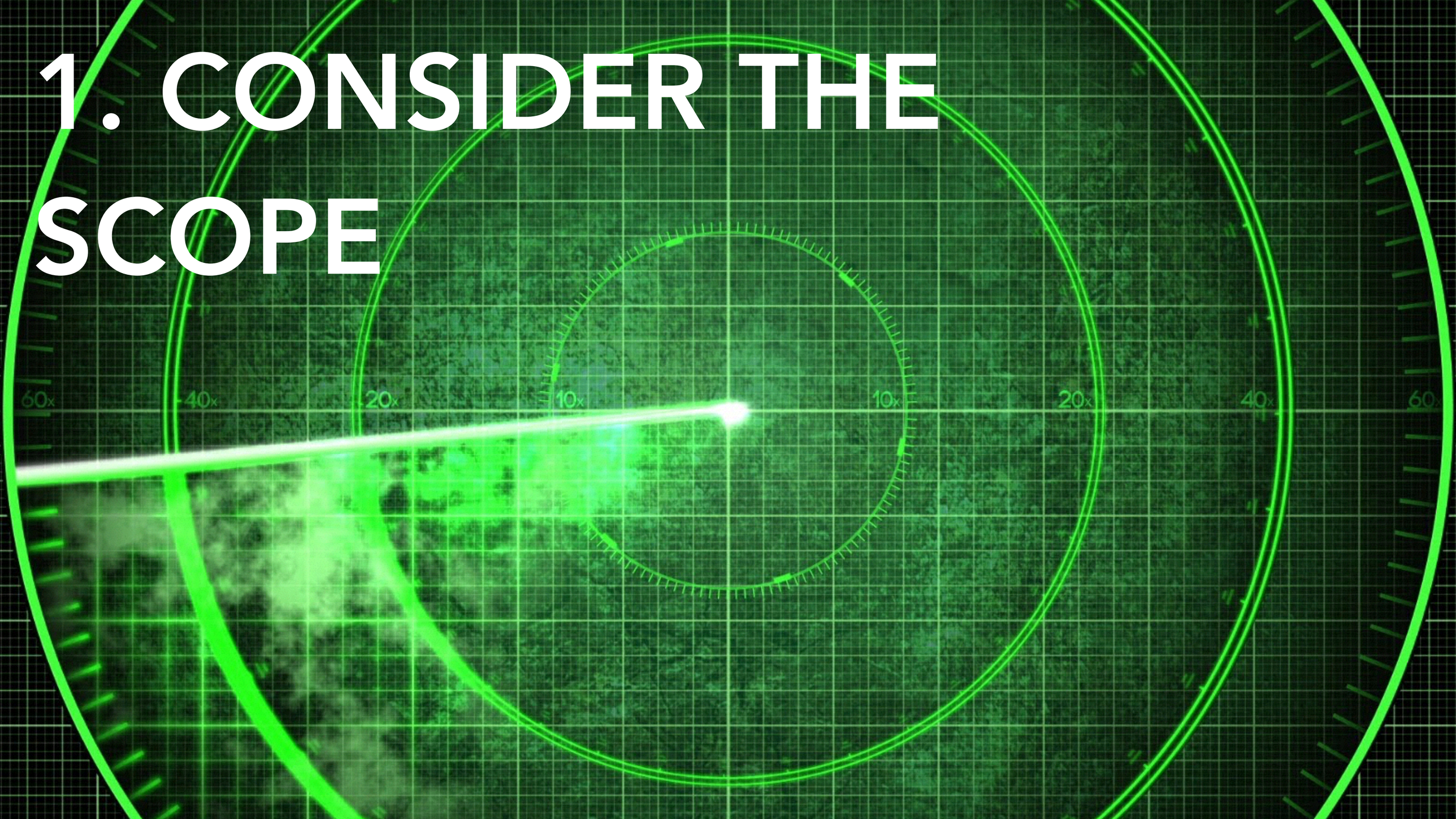
HOW DO WE DO IT?

WE NEED
SOME
TRAINING

WHAT TOOLS DO WE NEED?

HOW DO WE KNOW IF WE ARE SECURE?

1. CONSIDER THE SCOPE




©Colin Thomas

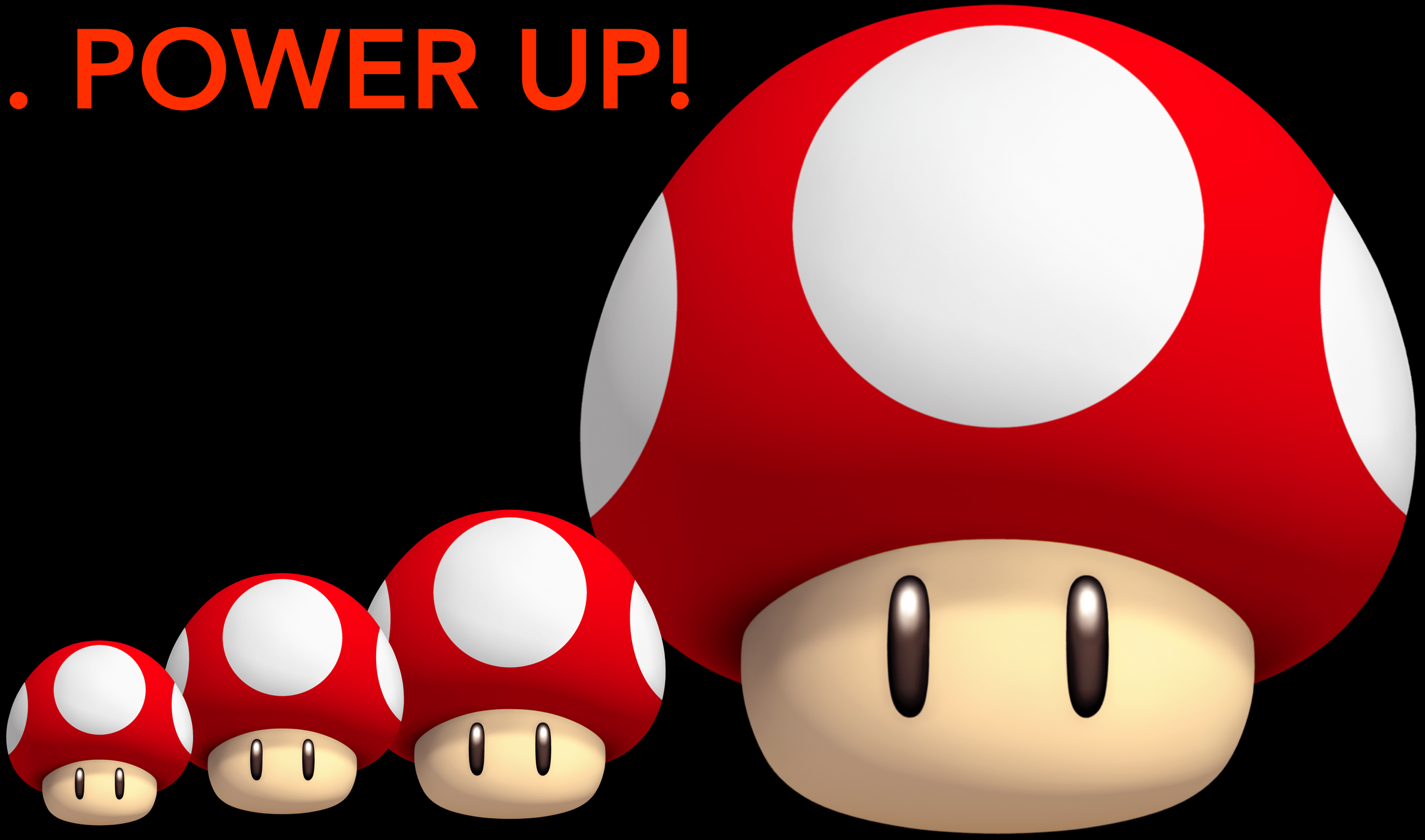
2. KNOW YOUR STACK

Steve McFarland https://flic.kr/p/bHSM6

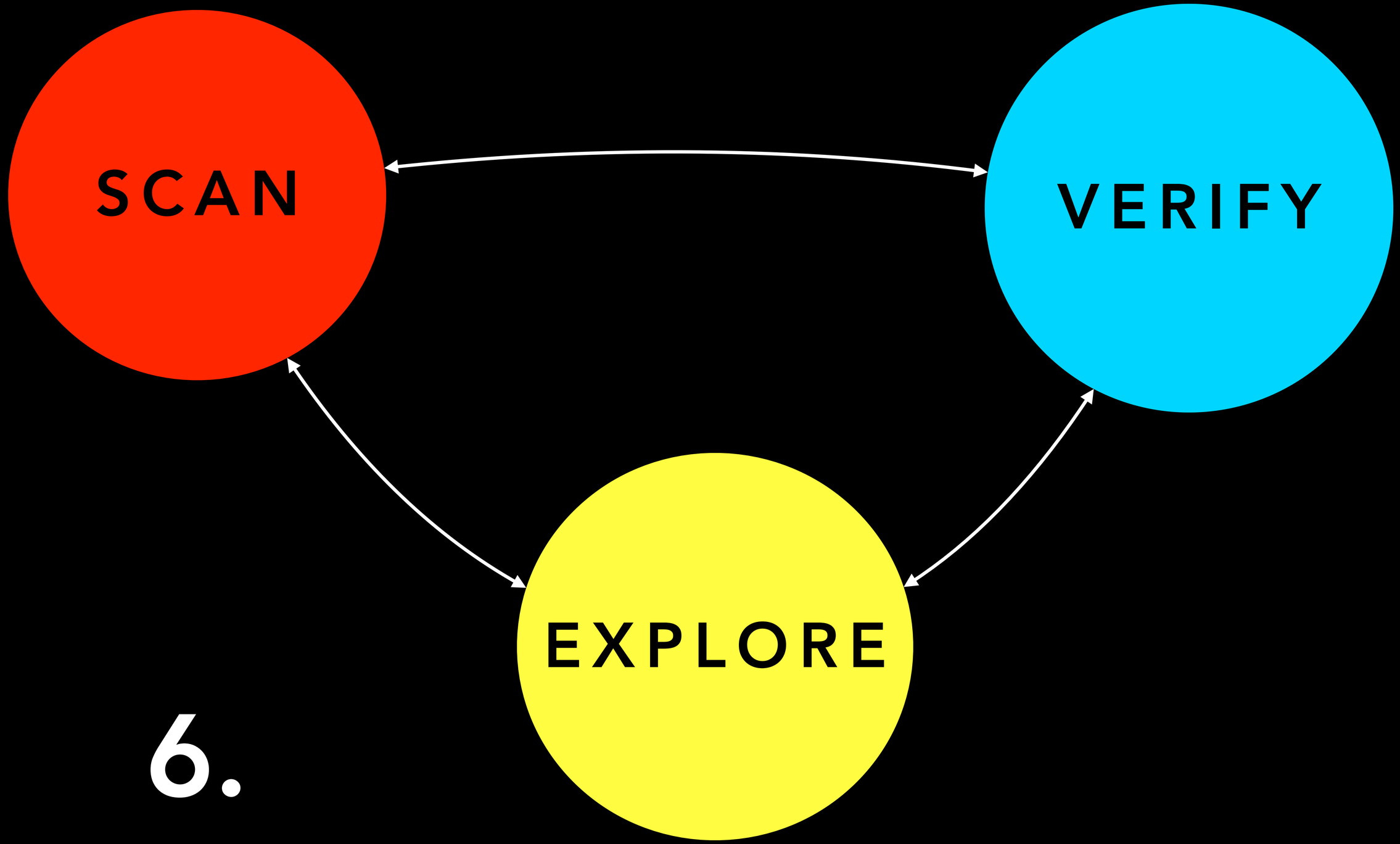
3. UNDERSTAND YOUR WEAKNESSES

Nathan Rupert https://flic.kr/p/jCErTo

4. POWER UP!



5. USE TOOLS EFFECTIVELY



6.


7. BE (OCCASIONALLY) EVIL

“As a hacker, I can

- send bad data in URLs, so I can access data and functions for which I am not authorised
- send bad data in the content of requests…
- send bad data in HTTP headers…
- read and even modify all data that is input/output by your application

Source: owasp.org Evil User Stories

8. DON’T DO IT ALONE

9. BE CLEAR, BE HEARD

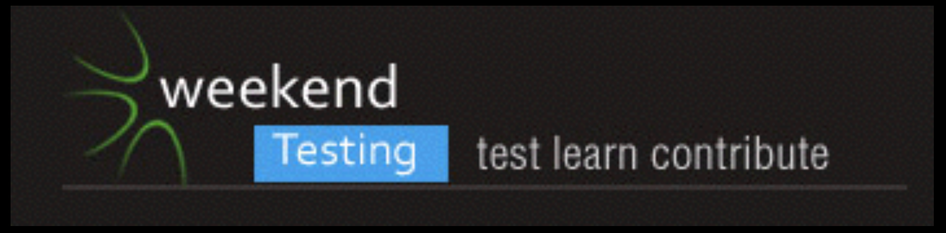
Eden, Janine and Jim https://flic.kr/p/ajC5WF

10. BE DETERMINED

1. CONSIDER THE SCOPE
2. KNOW YOUR STACK
3. UNDERSTAND YOUR WEAKNESSES
4. POWER UP!
5. USE TOOLS EFFECTIVELY
6. SCAN > VERIFY > EXPLORE
7. BE (OCCASIONALLY) EVIL
8. DON'T DO IT ALONE
9. BE CLEAR, BE HEARD
10. BE DETERMINED

MANY THANKS!

QUESTIONS?



DAN BILLING |
@THETESTDOCTOR

#TESTBASH