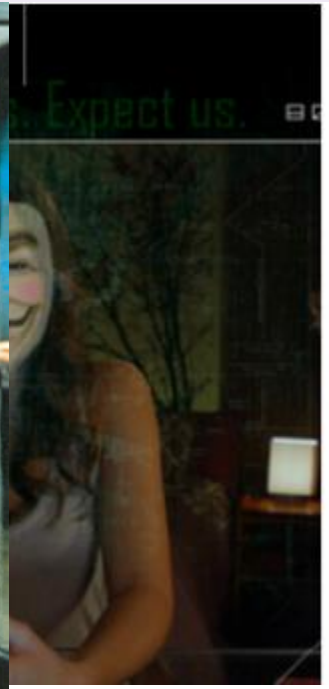
PWK, OSCP, WTF!

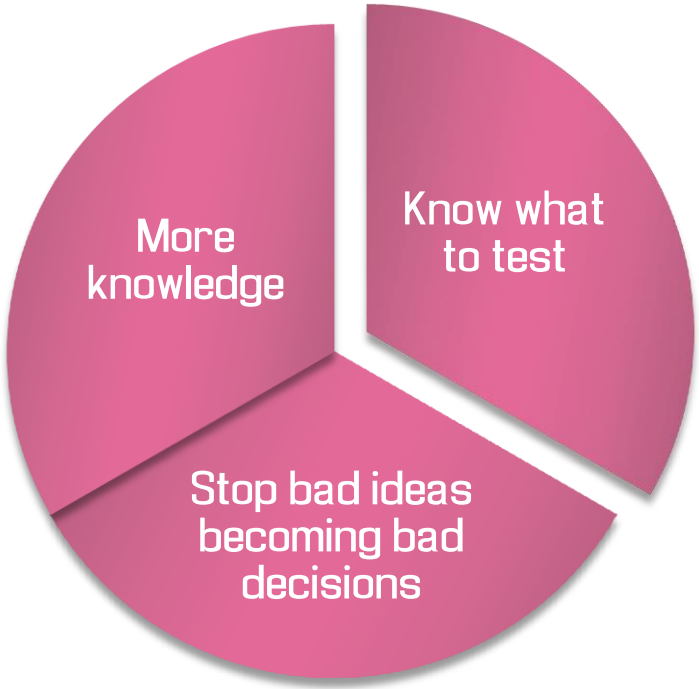
What is this all about?

Why I'm running these and what I'm aiming for

Hacking is cool



Better mind set === better systems



Teach a man to fish

- Being in security is stressful
  - Mainly because of the people that don't know security
- There's too much out there for just one person to learn
  - Lots of insight comes from hearing other people's experiences
  - Other people think in different ways and help challenge your pre-conceptions
- See slide about "Hacking is cool"

“Know the enemy and know yourself. In a thousand battles you will be victorious”

- You need to know what you’re up against.
  - Learn their tactics and use it against them
- Don’t train for golf if you’re playing American football
  - Train for the reality, not the tick-box certificate

Certifications

CREST: CPSA

- CREST Practitioner Security Analyst (CPSA)
  - 120 question, Multiple choice exam
  - Training is ~£1200
  - Exam is ~£250
  - Syllabus covers a variety of security focussed topics

(ISC)²

- Certified Information Systems Security Professional (CISSP)
  - Sometimes mocked, sometimes praised
  - Requires at least 5 years of education + experience (like being a certified engineer)
  - Expensive: >£5000

EC : CEH and CEH:Practical

- CEH is 25 question multiple choice
- CEH: Practical is 6 hour practical examination
  - New qualification. Not much known about it
  - £200 for 6 months lab access (?)
  - $550 for the examination

Offensive Security: PWK, OSCP

- Pentesting With Kali
  - An introductory course on the use of Kali within pentesting
  - 30/60/90 days of lab access
- Offensive Security Certified Personal
  - An industry recognised qualification
  - 24 hours of lab access to an example system
  - You are then examined on a self written report on that system, which must be delivered within 48 hours of the lab.
- $800 for 30 days lab access and cert attempt

OFFENSIVE® security

Syllabus

What I'm not going to talk about

- OWASP Top 10
- Lock picking
- "How to hack facebook"
- Incident response
- Risk management

What *am* I talking about?

1. PWK, OSCP, WTF?!
2. Setting up a PenTesting Environment
3. A few Linux basics
4. Networking is important in the tech industry
5. ARP poisoning and Man-In-The-Middle attacks
6. Recon: Technical information
7. Recon: The social side
8. Active Scanning and vulnerability scanning
9. Popping Shells and shellcode
10. Buffer overflow: where I stick my shellcode
11. Using Metasploit
12. Password cracking
13. Spectre and Meltdown

Where can I go to learn in my own time?

Theory and Facts

- Cybrary
  - Good courses on networks and system administration
- The internet in general
  - Once you know what you're looking for, check wikipedia and other classic information sources
- Books
  - "Advanced Penetration testing"

Fun

- Local meet ups
  - A great chance to meet people, hear interesting things and talk to like minded people
- Online videos from Cons
  - Nowadays many cons video their talks and make them available online
  - Defcon / Blackhat / Bsides / Steelcon
- Online CTFs
  - Puzzle games that utilise your “hacking” skills
  - ‘Over the wire’: http://overthewire.org/wargames/

Terminology

Hats

Hackers often get defined by hats. They tend to describe where on a spectrum of malicious -> altruistic you are.

This is obvious *very* subjective.

By way of example, a hacker finds a vulnerability:

- White hat tells the vendor and then, following responsible disclosure, releases public details.
- Grey hat sells it to the NSA.
- Black hat exploits it for personal profit, or sells to criminals.

Red team vs Blue team

Comes from the military:

- Red team
  - "*A red team or the red team is an independent group that challenges an organization to improve its effectiveness by assuming an adversarial role or point of view*"
- Blue team
  - "*A blue team is a group of individuals who perform an analysis of information systems to ensure security, identify security flaws, verify the effectiveness of each security measure, and to make certain all security measures will continue to be effective after implementation.*"

Penetration Testing

- "*A penetration test, colloquially known as a pen test, is an authorized simulated attack on a computer system, performed to evaluate the security of the system*" – Wikipedia

Bug vs Vulnerability vs Exploit

- A bug is a defect in a code or system: it works differently to intentions.
  - May or may not be explicitly against the intended specification.
- A vulnerability is a method by which something bad can happen.
  - It may result from a bug, or may intentionally part of the design.
- An exploit is something that takes advantage of a vulnerability in order to achieve some goal.
  - This may be cause data exfiltration