Introduction to Ethical Hacking

Dr Rob Hegarty

Aims & Objectives

- Upon completion of this lecture you will be able to:
  - Describe the role of an ethical hacker
  - Recognise UK legislation applicable to ethical hacking
  - Categorise different types of hacking activity
  - Summarise the ethical hacking procurement process.

Overview

- Introduction to ethical hacking
- Penetration testing vs vulnerability assessments
- Testing methodologies
- Ethical hacking and the law
- Overview of recent hackers and hacking groups
- Procuring ethical hacking services

Introduction to Ethical Hacking

- Ethical hackers
  - Employed by companies to perform penetration tests
- Penetration test
  - Legal attempt to break into a company's network to find its weakest link
  - Tester only reports findings, does not solve problems
- Security test
  - More than an attempt to break in; also includes analyzing company's security policy and procedures
  - Tester offers solutions to secure or protect the network

Vulnerability Assessment

- Vulnerability assessment, identification of vulnerabilities often using automated tools and techniques.
  - Frequently used to determine a baseline (ideally monthly)
  - Should be run when network configuration changes (new equipment, software etc)
  - **Looks for know software vulnerabilities**
  - Generates lengths report
  - Does not necessarily propose or recommend fixes
  - Internal staff

Penetration Testing

- Demonstrates a vulnerability can be identified and exploited.
  - Ideally carried out annually
  - Tester uses experience, wits, technical knowledge to identify vulnerabilities, identified and exploits weaknesses in the way the system is used e.g. CEO password reuse, poorly configured databases, etc
  - **Looks for exploits associated with the business**
  - Provides an explanation of how the exploitation was carried out
  - Generates short report
  - Does not necessarily propose or recommend fixes
  - External staff

Classification of Hackers

- Hackers
  - Exploit computer system vulnerabilities to gain unauthorized access
  - Illegal, if caught can serve a custodial sentence.
- Crackers
  - Unauthorized access, exfiltration and destruction of data
  - Commonly referred to as hackers
- Ethical hacker
  - Carry out the above activities, with owners permission, get paid, do not go to jail (hopefully ☺)

Classification of Hackers

- Script kiddies
  - Young inexperience (often immature) hackers
  - Copy code and techniques from knowledgeable hackers
- Professional penetration testers
  - Write programs and scripts (Perl, Python, C, C++, etc)
  - Identify new vulnerabilities and exploits

Becoming a Hacker

- This unit won’t make you a hacker or expert
- Respect is earned in hacking circles, through years of practice, study, identification and disclosure of new vulnerabilities
- Hacking is a lifestyle and attitude
  - Figuring out how things work
  - Taking advantage of flaws
  - Reporting the flaws
    - Ethical hackers use responsible disclosure
    - Hackers / Crackers disclose exploits and data without warning

Penetration Testing Methodologies

- White box model
  - Test given information about the network
    - Topology
    - Technology
  - Tester is allowed to interview staff
  - This sometimes make the testers job a bit easier.

Penetration Testing Methodologies

- Black box model
  - Staff not informed of the test
  - No network details provided to the tester
    - Tester has to determine these
  - Evaluates the security outlook of personnel
    - How does the security team respond?
    - Are general staff aware of their responsibility?

Penetration Testing Methodologies

- Grey box model
  - Hybrid of white and black box approaches
  - Partial information provided to the tester

UK Legislation

- Computer Misuse Act 1990
  - Unauthorised access to computer material
  - Unauthorised access with intent to commit other offence
  - Unauthorised modification of computer material
- Police and Criminal Evidence Act 1984
  - General power of seizure
  - The power for requiring information held on a computer must be handed over
- Criminal Justice and Police Act 2001
  - Describes the power by which an item can be seized if it is believed it may contain an item for which there is lawful authorisation to search

RIPA – Regulation of Investigatory Powers Act 2000

- If any person with the appropriate permission under Schedule 2 believes, on reasonable grounds—
  - (a)that a key to the protected information is in the possession of any person,
  - (b)that the imposition of a disclosure requirement in respect of the protected information is—
    - (i)necessary on grounds falling within subsection (3), or
    - (ii)necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty,
  - (c)that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition, and
  - (d)that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this section, the person with that permission may, by notice to the person whom he believes to have possession of the key, impose a disclosure requirement in respect of the protected information.

Source http://tinyurl.com/7jp73me

DRIPA - Data Retention and Investigatory Powers Act 2014

- Retaining phone records and ICR (Internet Connection Records)
- Sections 1 & 2 deemed unlawful by high court
- Restricts the period that data can be held to 12 months
- Review of RIPA every two years
- Deemed illegal by EU

- Link to DRIPA
  - http://tinyurl.com/maqxe7r

IPA – Investigatory Powers Act 2016

- Replacement for DRIPA
- Retaining of bulk phone records and ICR (Internet Connection Records)
- Allows for equipment interference / computer network exploitation
- Being challenged in court

What You Can Do Legally

- Laws are continually being updated, in an attempt to keep pace with technology
- Different jurisdictions have different laws
  - e.g. German privacy and hacking laws are much stricter than other E.U. states
- Become familiar with what is legal and what isn’t in your jurisdiction

Guidelines

- Tools on your computer may be illegal in some jurisdictions, check before you travel
- Written words are open to interpretation, your interpretation may differ from that of a police officer or judge!
- Governments are reacting to the perceived and actual threat posed by cybercrime
  - Encrypted communication if a hot topic in the post Snowden era
  - Some seemingly minor offences carry serious sentences

Port Scanning

- Legal on your own network
- Legitimate tool
- Probably in breach of your ISP's acceptable use policy
- Definitely in breach of the Universities Policy!
  - Though not explicitly stated
  - http://www2.mmu.ac.uk/media/mmuacuk/content/documents/it-services/policies/policy_ref_StudentRegulations.pdf
- The laws around port scanning are the subject of interpretation

What you Cannot do Legally

- While penetration testing, the following activities are not legal
- Unauthorised access
  - Be it shoulder surfing or password cracking
- Installing worms and viruses
- Denial of Service attacks
- Denying users access to the network

Covering Your Back

- Have a contract, explicitly stating what you are allowed to do.
- Contracts may be useful if you end up in court
- Books on working as an independent contractor
  - *The Computer Consultant's Guide* by Janet Ruhl
  - *Getting Started in Computer Consulting* by Peter Meyer
- Internet can also be a useful resource
- Find a solicitor who understands cybercrime and technology (& let me know who they are ☺)

Ethical Hacking Skillset Summary

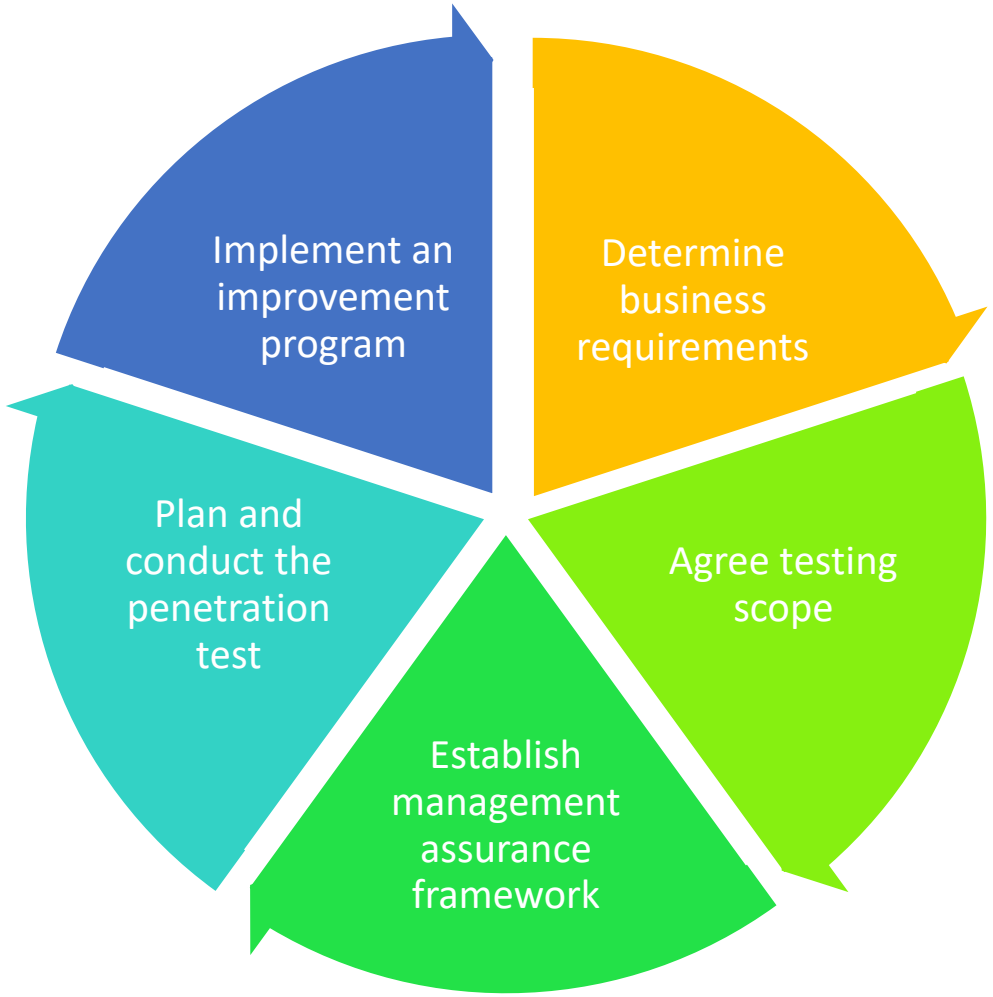
- Knowledge of network and computer technology
- Ability to communicate with management and IT personnel
- Understanding of the laws
- Ability to use necessary tools

In Class Task - Employability

- Identify either;
  - Computer Security companies located near to where you wish to work.
  - Or
  - Existing or emerging security challenges in your current place of work.

- Describe
  - The skills you will require to become employed in the security sector.
    - Review job adverts to find employer requirements.

CREST - Procuring Ethical Hacking Services



Determine business requirements for a penetration test, considering the:

- Drivers for testing, such as compliance, serious (often cyber-related) incidents, outsourcing, significant business changes and the need to raise security awareness
- Target environments to be tested, such as critical or outsourced business applications (and infrastructure), or those under development
- Purpose of testing (eg to identify weaknesses in controls, reduce incidents and comply with legal, regulatory or customer requirements).

Agree the testing scope, which includes:

- Approving the testing style (eg black box, where no information is provided to testers; white box, where full access is provided; or grey box, somewhere in between)
- Determining the type of testing to be done, such as web application or infrastructure
- Assessing test constraints, due to legal, operational, timing or financial requirements.

Establish a management assurance framework to:

- Assure the quality of penetration testing, monitoring performance against requirements
- Reduce risk (eg degradation or loss of services; disclosure of sensitive information)
- Manage changes (eg to the testing scope or to the configuration of the target system)
- Address problems, using a problem resolution process, to ensure that any issues are resolved satisfactorily, in a timely manner
- Agree scope, defined in a legally binding contract, signed by all parties prior to testing.

Plan and conduct the penetration test itself, which consists of:

- Developing a detailed test plan that identifies the processes, techniques or procedures to be
- used during the test.
- Conducting research, analysing information and performing reconnaissance
- Identifying vulnerabilities (eg technical vulnerabilities or control weaknesses)
- Exploiting weaknesses (eg to gain unauthorised access)
- Reporting key findings, in an agreed format in both technical and business terms
- Remediating issues, addressing identified vulnerabilities and associated ‘root causes’.

Implement an improvement programme, to:

- Address weaknesses, including root causes, evaluating potential business impact
- Evaluate penetration testing effectiveness, to help determine if objectives were met and that value for money has been obtained from your supplier
- Identify lessons learned, and record them, to help avoid weaknesses recurring
- Apply good practice, beyond the target, across a wide range of other environments
- Create an action plan, to ensure remedial actions are prioritised, allocated to accountable individuals and monitored against target dates for completion
- Agree an approach for future testing, considering results from previous tests.

Summary

- Ethical hacking and penetration testing entail hacking a computer system with the owners permission
- Three predominant models exist
  - White box, Black Box, Grey Box
- Hacking is now gaining attention from the media
- A strict process should be followed when procuring ethical hacking services

Next Lecture

- Ethical Hacking
- Coursework review