Ethical Hacking

Dr Rob Hegarty

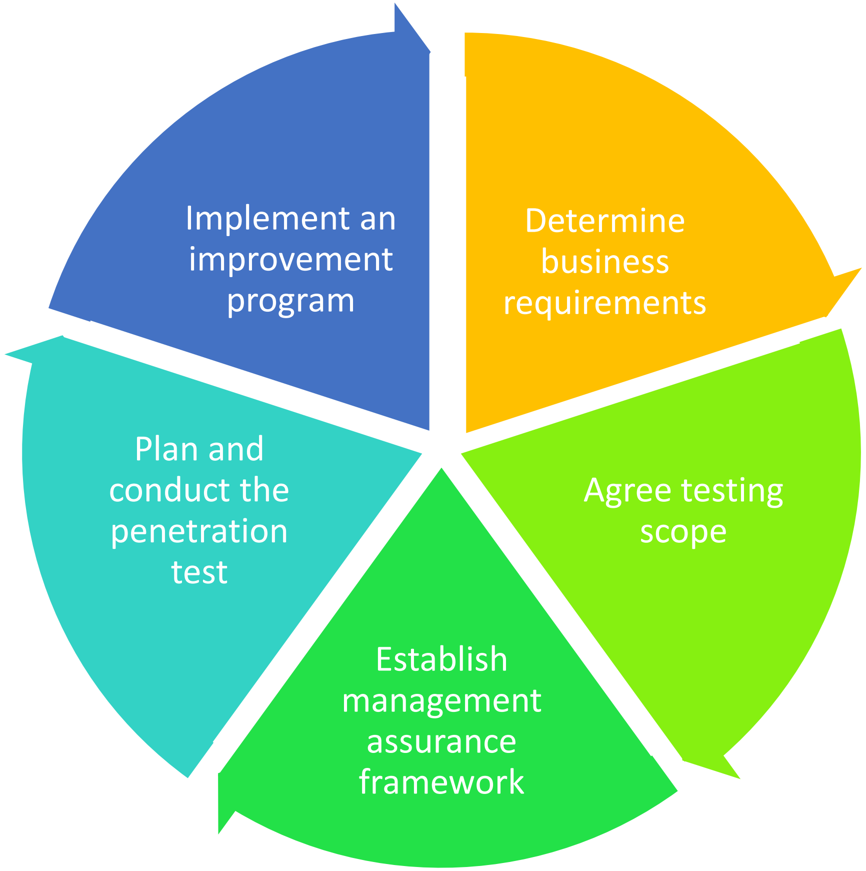
Aims & Objectives

- Upon completion of this lecture you will be able to:
  - Describe the various stages of the ethical hacking process
  - Categorise different types of vulnerabilities in computer systems
  - Explain how strong passwords can be selected
  - Describe a variety of password attack techniques

Overview

- Recap - Procurement
- Terminology
- Anatomy of a hack
- Understanding vulnerabilities
- Password Attacks

Recap - Procurement


Determine business requirements

Agree testing scope

Establish management assurance framework

Plan and conduct the penetration test

Implement an improvement program

Terminology

- Reconnaissance – Gathering information about a target system
- Vulnerability – Weaknesses in a system with the potential to be exploited
- Exploit – A mechanism for taking advantage of a vulnerability to compromise a system’s security
- Payload – The code that executes a malicious activity on a compromised system

Anatomy of a Hack

- Reconnaissance
- Gaining access
- Maintaining access / Foot holding
- Privilege escalation
- Compromising the domain (optional)
- Data exfiltration
- Covering your tracks

Reconnaissance

- Passive
  - Google hacking/dorking (http://www.hackersforcharity.org/ghdb/)
  - Whois – Find information about a domain name
  - DNSStuff – Collection of admin tools, that provide lots of info
  - Social engineering – watching a building, shoulder surfing
  - Network sniffing (monitor mode)
  - Shodan
- Active
  - Ping sweeps
  - Scanning
    - Port scanners
    - Network mappers
    - Vulnerability scanners
    - Network foot printing
    - User enumeration

Gaining Access

- Vulnerabilities identified during the scanning phase are exploited
  - Trivial vulnerabilities e.g. weak passwords, sniffer passwords
  - Software vulnerabilities
- All software has flaws, many of which can be exploited
- Shellcode is the payload delivered during an exploit, it is malicious code that typically aims to provide a remote shell on to the target machine
- Metasploit and other tools provide databases of shellcodes that you can use.
- More on shellcodes :
  - http://www.vividmachines.com/shellcode/shellcode.html

Privilege Escalation

- Exploiting a vulnerability to obtain access to additional privileges
- Vertical privilege escalation
  - Gain greater access to the system, typically admin privileges
- Horizontal privilege escalation
  - Gain access to another user’s account with the same privileges as your own

- Goal is often to obtain root access and own the system

Attacking the Domain / Network

- Extract information from the staging machine
    - Network config (IP address, Subnet, Hostname, Gateway, Routing Table)
    - Sniff internal network traffic
    - Extract user credentials
- Map the network / identify other hosts on the network
    - Repeat recon phase
- Compromise other hosts on the network

Maintaining Access (Foot holding)

- Ensure that you can continue to access the system
- Harden the system to prevent other hackers taking control
  - Steal legitimate credentials to allow login
  - Patch the system to prevent the same vulnerability being used by other

Data Exfiltration

- Extract useful information from the system
  - Passwords / password hashes
  - Confidential data
  - User account info

Covering Tracks

- This should begin as soon as you breach the system
- Remove traces of your activities
- Setup a VPN to attempt to blind the IDS
- Modify IDS/Firewall rules
- Remove or alter log files

Lockheed Martin Cyber Kill Chain

- Recon
- Delivery
- Installation
- Exploitation
- Command & Control
- Actions on Objectives

- https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

In Class Task - Programming

- Discuss your programming experience using the following discussion points.
  - What is programming?
  - Why is it important to learn to program?
  - What programming experience do you have?
  - What program are you going to write for your final year project?

- The following resources will help you learn to program in Python.
  - http://learnpythonthehardway.org/book/
  - http://www.lynda.com/Python-training-tutorials/415-0.html

- Programming is learned rather than taught, we will offer assistance, but significant effort is required to learn to program independently
- Both the University and Industry expect you to be able to program basic scripts

Vulnerabilities

- Human
- Technical
  - Architectural
  - Password strength
  - Software flaws

Social Engineering (Human Vulnerabilities)

- Tricking someone in to giving you information they shouldn’t
- Common approaches
    - Telephone call pretending to be from tech support / a fellow employee
    - Befriending a high value target (longer term attack)
    - Phishing / Spear-phishing attack (419’s)
    - Email/Phone number spoofing
    - Mining social network posts (date of birth, pets name, etc)
    - Typo squatting (setting up a con website with a similar URL to a legit one)
    - Appearing to be an authority figure

Password Vulnerabilities

- Poor selection
- Re-use
- Plain text storage
- Poor choice of hash function
- Not salting
- More on password cracking
  - http://arstechnica.com/security/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/1/

Password Attacks

- Online – Attempting to access a service via a network, using a password login hacker
  - Hydra - https://www.thc.org/thc-hydra/
  - Brutus - http://www.hoobie.net/brutus/
- Offline – Attempting to crack a password hash using a password cracker
  - John the ripper - http://www.openwall.com/john/
  - Cain & Abel - http://www.oxid.it/cain.html
- Dictionary – Try each word in a dictionary
- Brute force – Try every possible combination

Password Attacks – Strengths and Limitations

- Online – Limited by bandwidth, loud and likely to be detected
- Offline – You need the password / hash file, limited by computational resources

- Dictionary – Faster than brute force, may not always be successful
- Brute force – Will always work given enough time, can take forever

- https://howsecureismypassword.net/

Software Vulnerabilities

- Software is written by humans, therefore it contains errors, software is often highly complex and errors can go undetected for years.
  - E.g shellshock/bash bug (http://tinyurl.com/p67xw2z)
- Vulnerability Databases – (Use these to find descriptions for the vulnerabilities you identify with MSF)
  - Common Weakness Enumeration
  - Common Vulnerabilities & Exposures
  - National Vulnerability Database (NIST)
- More on software vulnerabilities
  - http://www.sans.org/top25-software-errors/
  - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Buffer Overflow

- Data and instructions are stored in RAM
- Programs use buffers to act as a temporary data store
- If an attacker is able to write beyond the end of the buffer, they can overwrite the contents of memory
  - Causing a system crash
  - Executing malicious code
- Example
  - http://www.wired.com/2009/03/conficker-how-a/#more

Relative Path Traversal

- We typically store data in a hierarchical structure containing directories, subdirectories and files
- Paths are used to specify the location of files
  - Absolute paths e.g. www.test.com/logo.gif
  - Relative paths e.g. /logo.gif
- Users are often given access to specific directories
- Attackers may attempt to navigate outside of the restricted directory using relative path syntax ".."
- E.g.
  - http://some_site.com.br/get-files.jsp?file=report.pdf
  - http://some_site.com.br/get-files?file=../../../../some dir/some file

Integer Overflow

- Integers are whole numbers stored in memory by computer programs
- e.g. 10, 5, 1
- Integers are stored as number of bits
- If a number is too large to represent with the number of bits available it wraps around
- Signed 8 bit integers can contain store -128 to 127 inclusive
- This can cause problems
  - E.g. -128 + -1 = 127
- If this number way used to calculate the size of a buffer, an overflow situation may occur

Summary

- Systems contain many vulnerabilities that can be exploited by attackers
- In order to identify vulnerabilities in systems, hackers employ the following process when attacking systems
  - Reconnaissance
  - Gaining access
  - Maintaining access / Foot holding
  - Privilege escalation
  - Compromising the domain (optional)
  - Data exfiltration
  - Covering your tracks
- Password cracking techniques, are used to recover passwords from hashes, password hacking techniques are used to attempt to log in to systems

Next Week

- Mitigation and web security