Mitigation & Countermeasures

Dr Rob Hegarty

Aims & Objectives

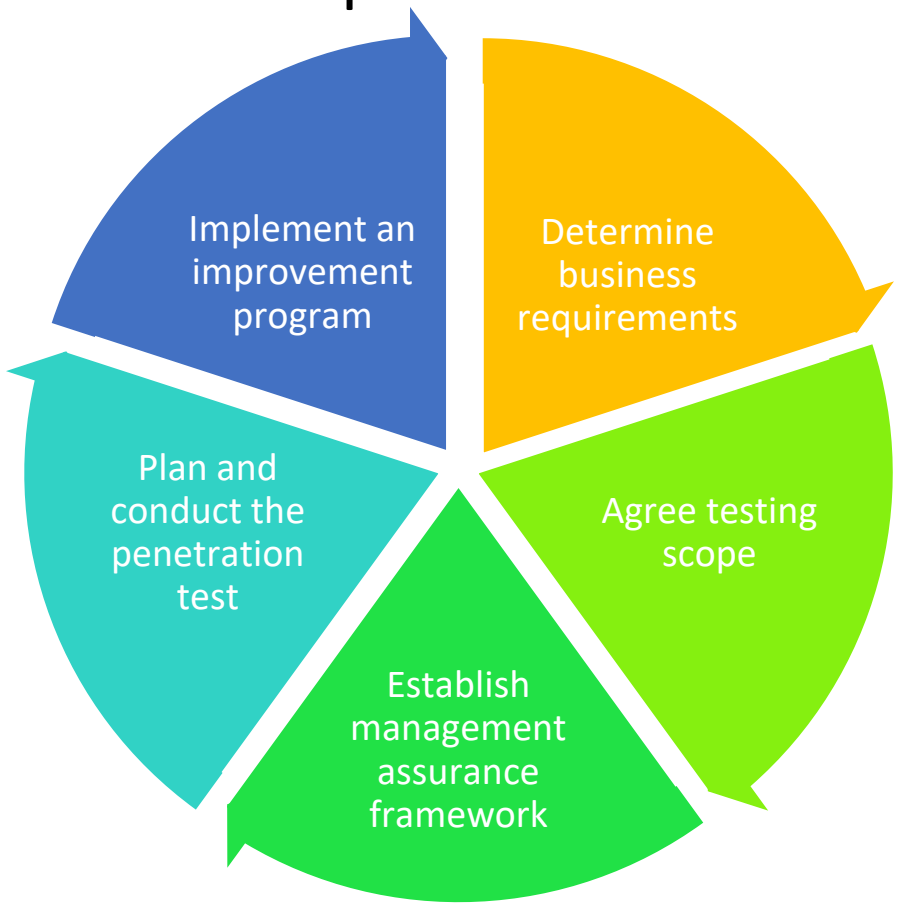
- Upon completion of this lecture you will be able to:
  - Describe the various hacking mitigation techniques
  - Distinguish between various access control methodologies that are employed in computer security
  - Summarise how a variety of countermeasures may be employed to increase the security of a computer system
  - Identify defence in depth strategies to improve the security of computer systems

Overview

- Recap on the ethical hacking procurement and implementation processes
- Business Impact
- Mitigation
- Access Control
- Configuration Management
- Contingency Planning
- Preventative Controls
- Technical Countermeasures
- Defence in depth
- Summary

Recap – Ethical Hacking

- There are well established procurement and implementation processes for ethical hacking
  - Reconnaissance
  - Gaining access
  - Maintaining access / Foot holding
  - Privilege escalation
  - Compromising the domain (optional)
  - Data exfiltration
  - Covering your tracks



What is Mitigation?

- Mitigation – mitigate or moderate the effects of an action

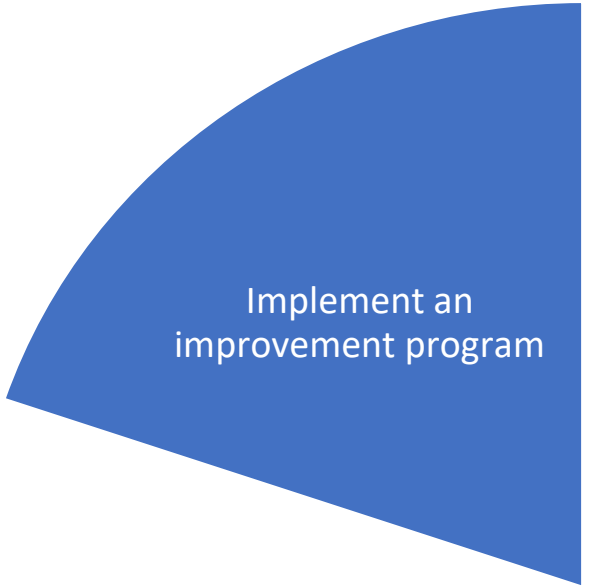
- Reduce severity of the impact of an attack/incident

Mitigation Approaches

- Preventative
  - “Prevention is better than a cure” preventing an incident from occurring should be the first goal
- Detective
  - Identifying when a system has become vulnerable, and/or when it has been exploited
- Corrective
  - Counteracting the impact of an incident after the fact

Mitigation

- The mitigation strategy should take into account the process employed formally/informally by hackers, and form part of the improvement plan
  - Reconnaissance
  - Gaining access
  - Maintaining access / Foot holding
  - Privilege escalation
  - Compromising the domain (optional)
  - Data exfiltration
  - Covering your tracks

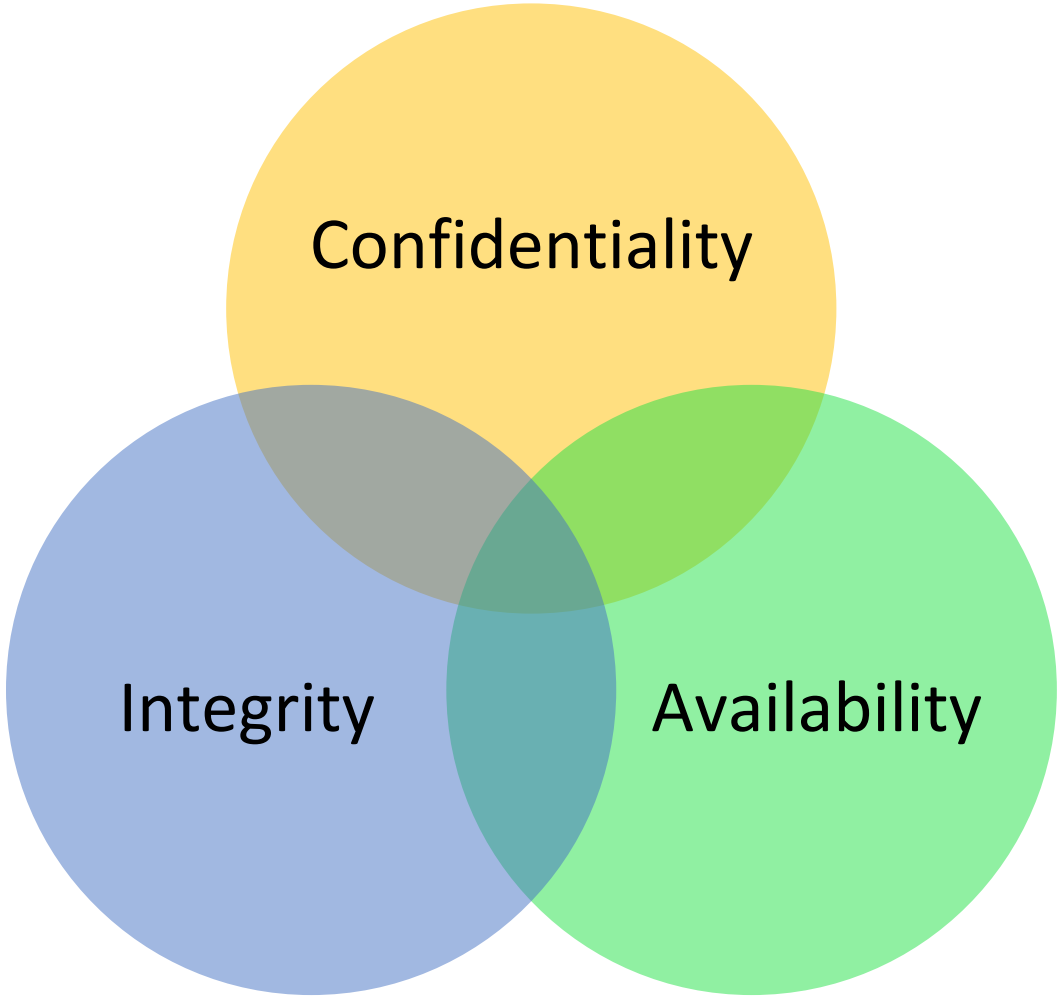


Business Impact Analysis

- Which systems are considered critical?
- How does each and every system relate to the other systems
  - Hidden critical systems?
- What are the consequences of disruption to critical and non-critical systems?

Why Access Control?

- In order to achieve the three properties of security, access control is required
- Access control is the selective restriction of access to a resource of information, access control is concerned with **authorisation and authentication**
- **Authorisation = What you are authorised to do**
- **Authentication = Proving your identity**



Approaches to Access Control

- DAC (Discretionary Access Control)
  - Access is provided at the owner's discretion, the owner of an object defines who and what level of access if granted
  - Most operating systems provide DAC
  - e.g. a user can specify who is allowed to view/read/write to a file
- MAC (Mandatory Access Control)
  - Access is enforced by the system according to security labels (classification levels) Unclassified, Official, Restricted, Confidential, Secret, Top Secret
  - Subject clearance is matched to object clearance according to a model
  - MAC is used were security is vital
  - SE-Linux provides MAC

Access Control Lists

- Object has permission attributes that specify which subjects or processes are granted access.
- e.g. Document.txt (Alice: read; Bob: read, write)

- Security is largely dependant on how ACLs are generated/modified

Access Control Models - Biba

- Goal - Integrity preservation
  - Prevent unauthorised modification by unauthorised subjects
  - Prevent unauthorised modification by authorised subjects
- Rules - “no read down, no write up”
  - No read down – A subject with a given integrity level must not read an object with a lower integrity level
  - No write up – A subject with a given integrity level must not write to an object with a higher integrity level
- Allows orders to flow down the chain of command, without their integrity being damaged

Access Control Models - Bell-LaPadula

- Goal – Confidentiality preservation
  - Prevent objects with a high clearance level being viewed by subjects with a lower clearance level
  - Prevent subjects with a high clearance level writing to objects with a lower clearance level
- Rules– “no read up, no write down”
  - No read up - Subjects can not read higher than their clearance level
  - No write down - Subjects can not write to an object at a lower clearance level
- Restricts access to information to subjects with suitable clearance levels

Operational Controls

- Awareness and Training
  - Security awareness training
    - e.g. Don’t open email file attachments from unknown senders
- Configuration Management
- Contingency Planning

Configuration Management

- Hardware
  - Devices don’t ship secure
    - e.g. Default login credentials
  - Inventory, including serial numbers, configuration settings
- Software
  - Licence inventory
  - Patch & service pack management

Contingency Planning

- Contingency Plan (CP) Development
  - Business Impact Analysis
    - What are the risks, impacts and interdependencies?
  - Identify Preventative Controls
  - Develop recovery strategies
  - Deploy CP
  - Test CP
  - Maintain / Update CP

Preventative Controls

- UPS (Uninterrupted Power Supply)
- Generators
- Fire suppression system (Not Halon)
- Scheduled offsite backups
- Access Control
- Cooling Systems

Data Backups

- In the event of an incident do you have:
  - Data backups
  - System images
- Are your backups:
  - Up to date
  - Accessible / Available (Think Cryptolocker)
- How would you achieve the above?

Backups vs Redundant Storage

- Resilient systems require both data backups and redundancy
- Backups
  - Allow recovery of data
  - Full – The entire repository is backed up
  - Incremental – Data changed since the last full backup is backed up
  - Differential – Data changed since the last differential or incremental
- Redundant Storage – RAID (Redundant Array of Inexpensive Disks)
  - Prevents system down time
  - Mirrored (RAID 1) – Two disks contain identical data
  - Striped (RAID 5) – Data is split up and striped across multiple disks

In Class Task

- Contingency planning – Describe you contingency plans for each of the follow:

- Your laptop hard drive fails the day before a coursework deadline
- You suspect your primary email account has been compromised
- You discover a virus on your laptop or PC

- Consider:
  - Data
  - Software
  - Time required to recover from the incident

Countermeasures

- Countermeasures typically fall into three broad categories

Approach	Perimeter	Internal	Extending
Firewall	X		
IDS	X	X	
VPN			X

Why Firewalls?

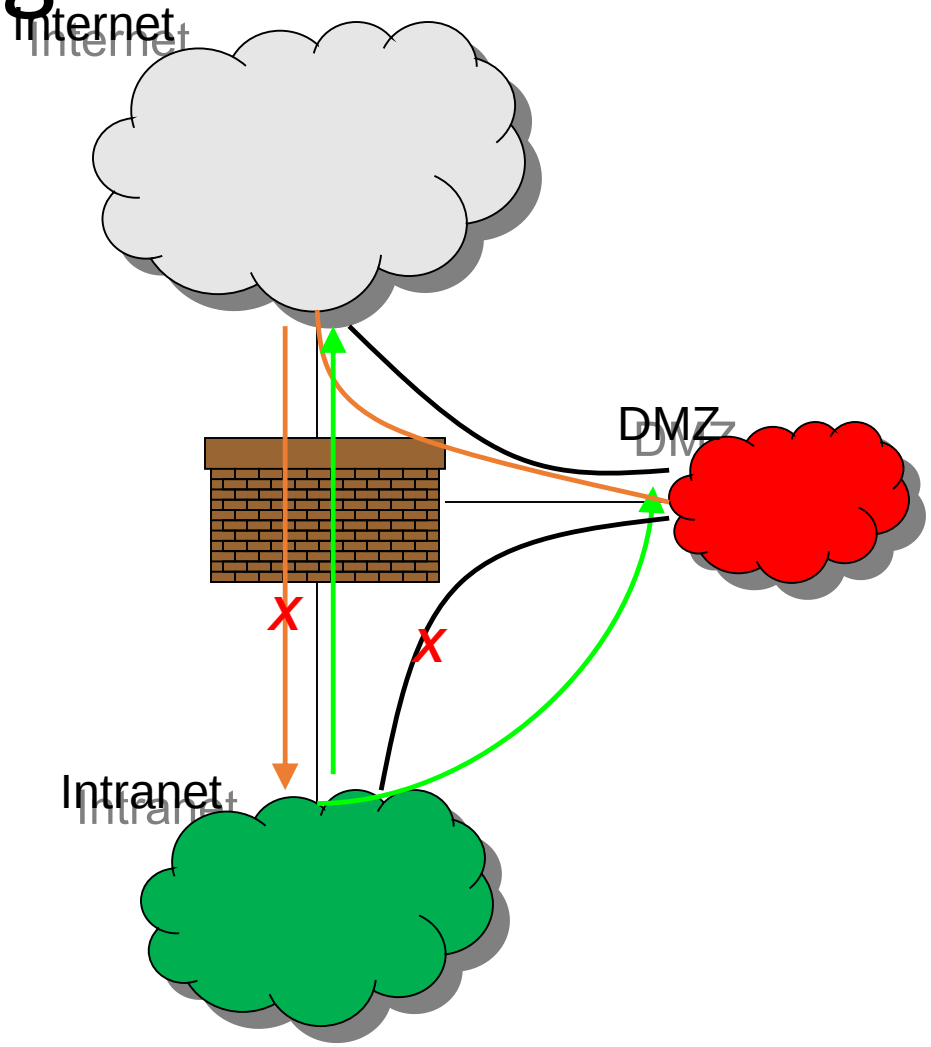
- Hosts are vulnerable due to their complexity, vulnerabilities in operating systems, application software, and poor user practice (systems not kept up to date)
- Firewalls restrict access to the network
- Firewalls at the perimeter of a network help mitigate the vulnerable hosts

Firewalls

- Based on the concept of physical walls that prevent the spread of fire, hence the name “firewall”
- First line of defence, based on the perimeter model
- Hardware and software based solutions
  - Software – Protects a single host, installed and configured by the end user
  - Hardware – Protects a network, installed and configured by service provider, administrator
- Firewalls are considered a high value target, for modification or DoS type attacks

Typical Firewall Configuration

- Internal hosts can access DMZ and Internet
- External hosts can access DMZ only, not Intranet
- DMZ hosts can access Internet only
- Advantages?
  - If a service gets compromised in DMZ it cannot affect internal hosts



IDS (Intrusion Detection Systems)

- Detect malicious behaviour inside a network
- Two approaches:
  - Misuse Detection
    - Create signature for know attacks (Capture attack, extract unique characteristics)
    - Compare network traffic with signatures to detect attack
  - Anomaly detection
    - Model normal network behaviour (Statistics on use of Ports, Bandwidth, etc against time)
    - Report any non-normal behaviour

HIDS - Host Based Intrusion Detection System

- Monitoring carried out on a host to detect attacks
- Examines
  - Log files
  - Changes to system files
  - Suspicious activity (e.g. failed logon attempts)
- Examples
  - Tripwire
  - Symantec ESM

NIDS - Network Based Intrusion Detection Systems

- Network based detection of attacks
- Examines
  - Internal and external network attacks (Inside firewall, or in the DMZ)
  - Traffic from multiple hosts (strategic placement required)
  - Alert the administrator if an attack is suspected
- Examples
  - Snort
  - Netprowler

IDS Challenges

- Misuse detection
  - Failure to identify novel attacks
- Anomaly detection
  - Modelling “Normal behaviour is difficult”
  - Data drift, updating the normal model can mask a slow incremental attack
  - Many attacks may look like normal traffic
  - False positive rate can be high
- Securing the IDS
  - IDS are considered high value targets, strong passwords and encryption of traffic on configuration ports are manditory

VPN – Virtual Private Networks

- Ensure confidentiality, preserve integrity

- Two main modes of use
- Tunnel mode
  - Used for site-to-site communication
  - Encapsulates the entire original IP packet

- Transport mode
  - Typically used for client-to-site communication
  - Original IP header is not encapsulated, payload is encrypted

Malware Detection

- Pattern scanners – look for strings in code that may be indicative of malware
  - Fast
  - Easily fooled with obfuscation
- Integrity checkers – Produce a database of signatures from files using hash functions. If the files are altered their signature changes
  - No need to know what a virus looks like
  - Problematic to keep up to date (software updates etc)
- Behaviour blocking – Prevent applications that exhibit malicious behaviour from executing

Policy - Passwords

- Specify minimum length
- Character inclusion rules
  - e.g. Alpha + Numeric + Symbol (Non-alpha-numeric)
- Specify an expiry date/time or validity period
- Disallow re-use
  - Force users to select different passwords without commonality
- Encourage the use of passphrases
  - “So long & thanks for all the fish!” is a strong password that is easy to remember
  - “716&*$KKcl3T” is a strong password that is difficult to remember
    - So the user will write it down somewhere!

Passwords - Slow hashing

- Passwords should never be stored in plain text
- Hashed passwords may be stolen in a breach, the attacker will then go about calculating hash values from their dictionary for comparison (assuming they know the salt or the passwords are unsalted)
- Select a hash function that increases the computational work required for password cracking such as PBKDF2 or bcrypt
  - PBKDF2 performs many iterations, increasing the computational workload
- For more information on password cracking and mitigation
  - https://crackstation.net/hashing-security.htm

Defence in depth

- A layered approach to defence
- Providing multiple barriers to the adversary
- Strategy should involve
  - People
    - e.g. Management, Training
  - Technology
    - e.g. Countermeasures
  - Operations
    - e.g. Policy

- https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Defence is Depth

- In order to reduce the vulnerability of a system and prevent exploitation a number of steps can be taken:
  - Regular updating and patching of OS and application software
  - Deployment and correct configuration countermeasures
    - Firewalls
    - IDS
  - Closure of unused open ports
  - Policy and training on information assurance / disclosure

Summary

- In order to preserve the confidentiality, integrity, and availability of resources, access control mechanisms are required.
- Various models and approaches to access control may be applied to achieve some or all of the above goals.
- Defence in depth is a multi-layered approach to securing computer systems
- There are a variety of technical and policy based countermeasures available to help protect computers systems

Next Week

- OpSec and Research