Advanced Network Security Revision (Part 1)

Dr Rob Hegarty

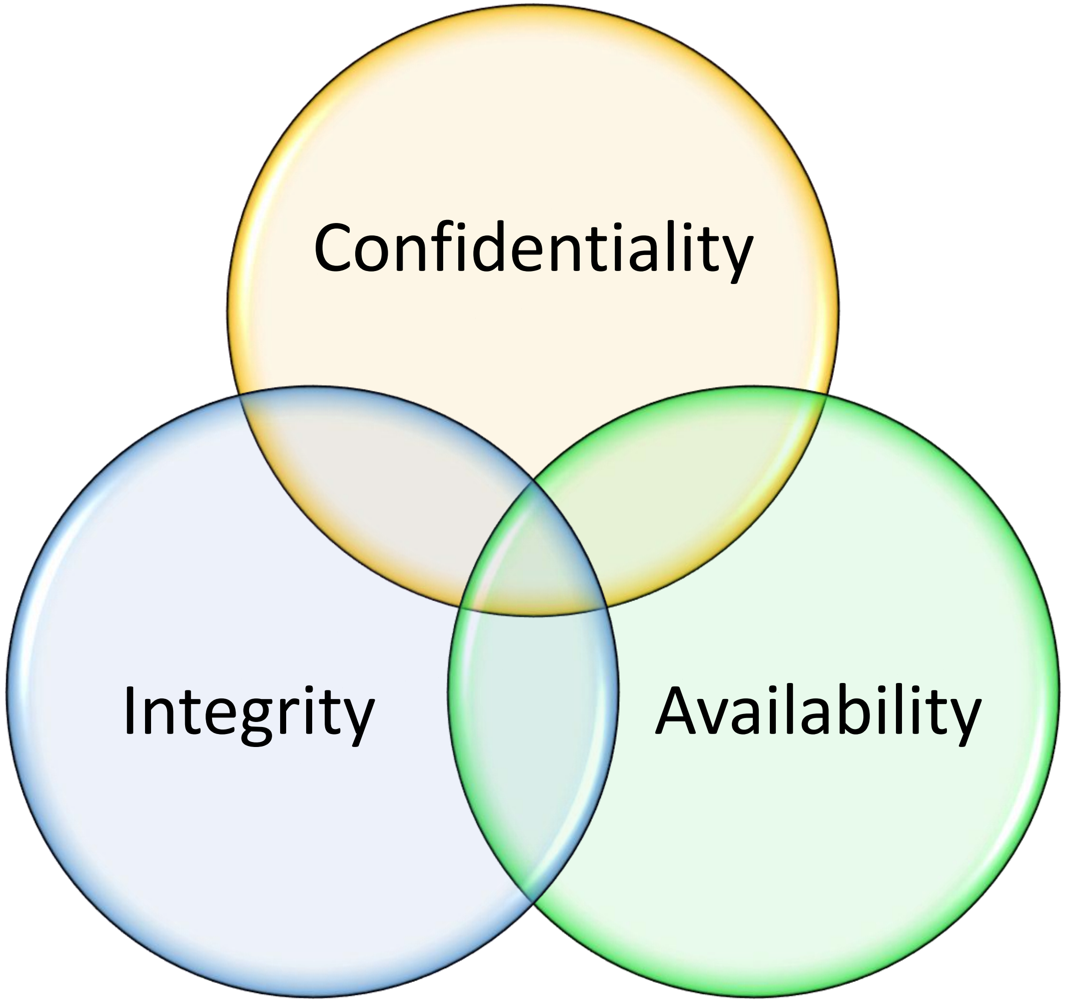
Aims and Objective

- To revise key topics for the exam
- To recap on fundamental topics and ensure they are understood

Topics

- CIA
- Terminology
- TCP Protocol and Misuse
- Password Attacks
- Ethical Hacking Procurement
- Lockheed Martin

CIA - Security Goals



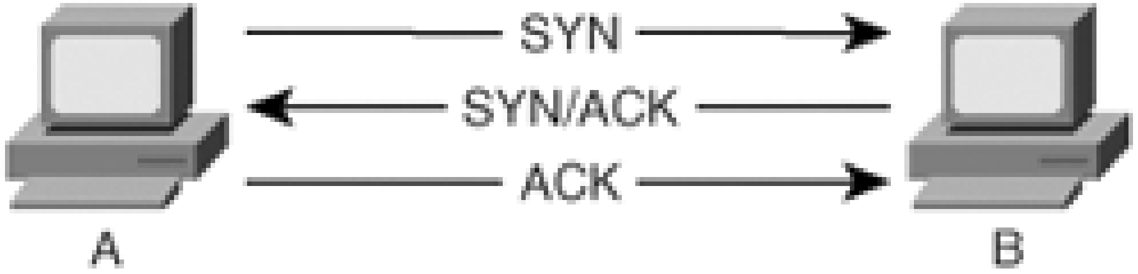
CIA - Descriptions

- Confidentiality
  - Restricting Access
    - To those authorised to access a resource
    - Preventing access by unauthorised users
- Integrity
  - Preserving
    - The accuracy and completeness of data
    - Preventing authorised modification
- Availability
  - Ensuring a resource is available when required

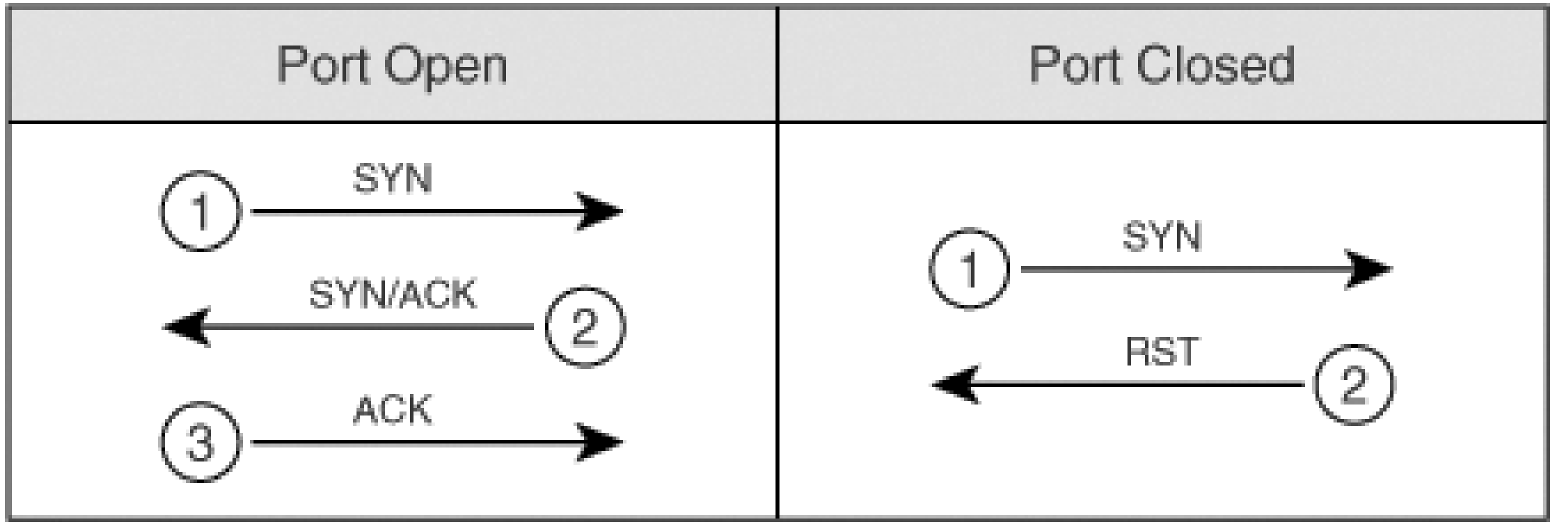
Concepts & Terminology

- Threats, Vulnerabilities, Risks
  - Threats: Possible attack vectors
  - Vulnerabilities: Weaknesses that could be exploited
  - Risks: Possibility of a security breach, and severity of resultant damage
- Trade-offs
  - Security = Constraints on functionality/operational properties
  - Which in turn impacts system usability/ease of use
- Non-Repudiation (of origin)
  - Proving a message was sent by the person claiming to send the message
  - Digital signature used

Protocols (TCP, UDP)

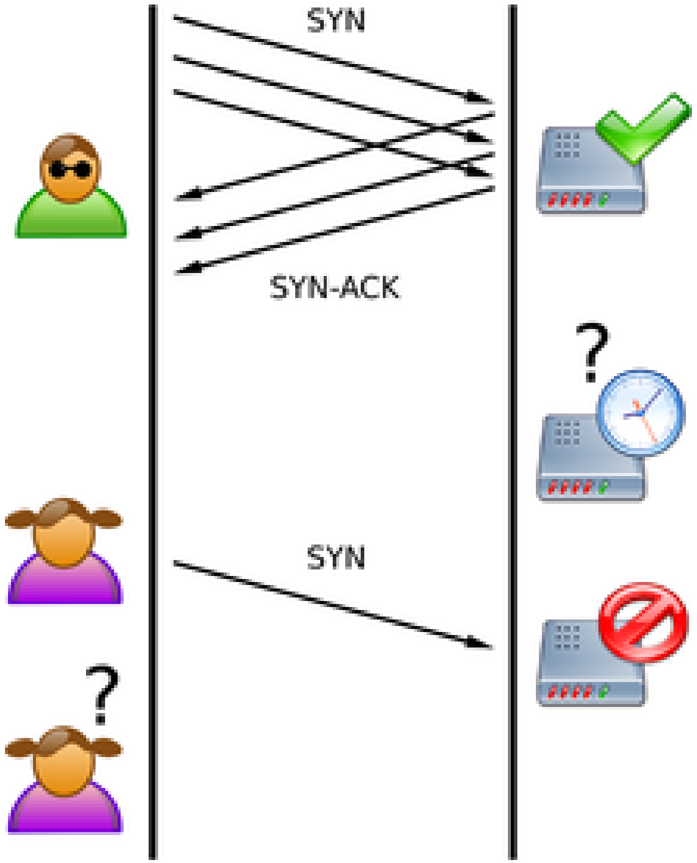


Port Scanning (TCP Connect Responses)



http://www.ciscopress.com/articles/article.asp?p=469623&seqNum=3

SYN Flood



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

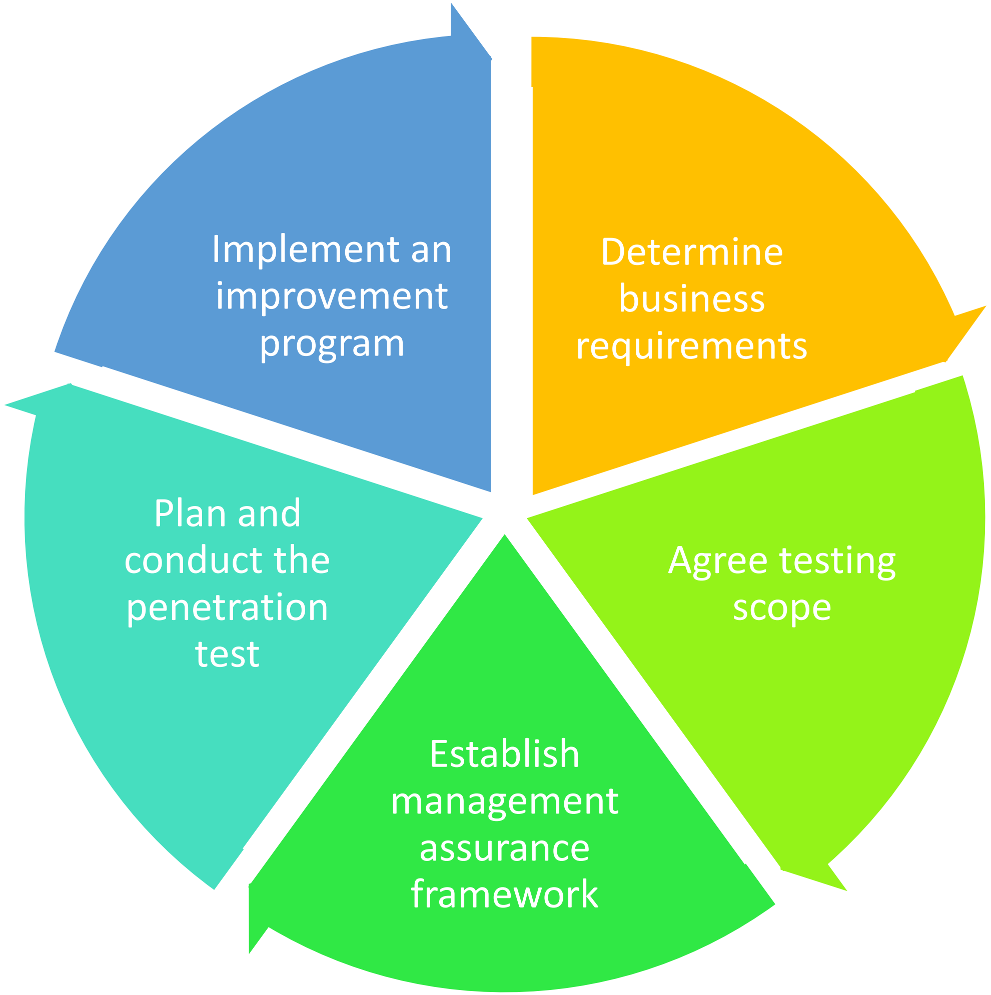
Password Attack – Strengths and Limitations

- 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/

CREST - Procuring Ethical Hacking Services



Determine business requirements

Agree testing scope

Establish management assurance framework

Plan and conduct the penetration test

Implement an improvement program

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.

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

Summary

- This lecture recapped on key revision topics, it does not provide an exhaustive list of topics, however it should help guide your revision.