Murdoch
UNIVERSITY

Introduction to Computer Security

ICT287 Computer Security

What Is Security?

"The quality or state of being free from danger"

Security is achieved using several strategies simultaneously

Dimensions of Security

- Securing data in transit and rest
- Physical security of personnel and equipment
- Secure coding and application development
- The list goes on...

Hackers

- Those who enjoy the intellectual challenge of overcoming and circumventing limitations of systems and who try to extend their capabilities
- Act of engaging in activities (such as programming or other media) in a spirit of playfulness and exploration is termed **hacking**
- Hacking entails some form of excellence, for example exploring limits of what is possible
- Bad hackers were called crackers

Hacking in the Media

- Mainstream media tend to use the term “hacker” to describe predominantly negative and illegal activities

- What we do know though, is that there are plenty of them around

- Reported hacks are likely tip of iceberg only

Yahoo (2016)

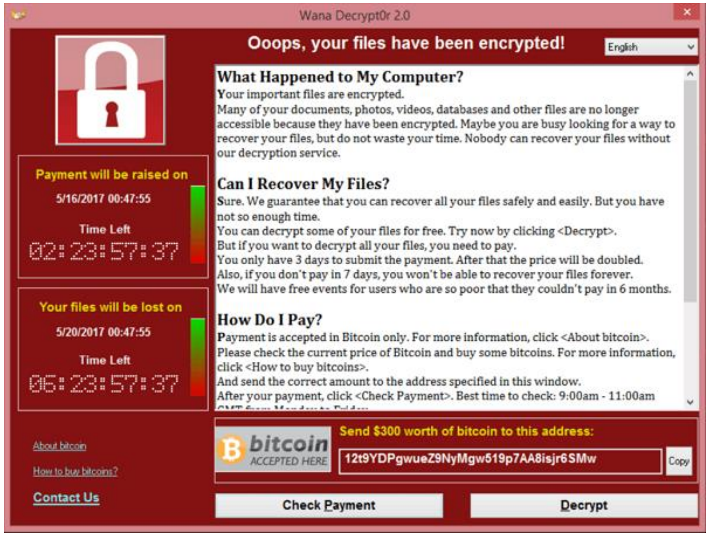
- Actual hack took place in 2014 but data was only dumped in dark web in mid 2016
- Hackers stole data of over 500 million users
- Names, emails, phone number, security question answers and responses (some as cleartext), hashed passwords (at least they were salted)
- Yahoo claims “state-sponsored” hackers to be responsible, but there is no evidence for that

OVH Mirai (2016)

- Largest DDoS attack reported so far (September 2016)
  - Attack launched from over 150,000 devices
  - Peak attack traffic from simultaneous DDoS was close to 1Tbps
  - Launched against (unconfirmed) websites belonging to customers hosted by France-based hosting provider OVH (hosts Krebs on Security blog)
  - Hijacked devices coerced into botnet
  - Many Internet of Things (IoT) devices, such as CCTV cameras and DVRs
  - Mirai botnet (https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/)

WannaCry Ransomware (2017)

- World-wide ransomware attack against Windows hosts
- Encrypt data files and show ransom note demanding bitcoin payment
- Once user pays, decryption key is sent to infected client
- Exploited vulnerability in SMB protocol
- Microsoft already released fixes months before, but many had updated



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

https://www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware-attack-spread-150-countries

Meltdown (2017)

- Hardware vulnerability of Intel x86 and ARM-based CPUs
- Exploits race condition between memory access and privilege checking during instruction processing
- Combined with cache timing attack allows unauthorised process to read data from any address that can be mapped to current process's memory
- Many OS map physical memory, kernel processes etc. into address space of every process, so bad process can read these
- OS developers deployed kernel patches to isolate kernel from user memory (performance loss) and Intel addressed issue in next generation of CPUs
- Many related newer attacks

Dallas Sirens (2017)

- Many other attacks and data breaches in 2017, but following is different (April 2017)
  - Dallas (US) has warning system with 156 sirens distributed across city
  - Hackers hacked system and managed to set sirens of for multiple times between 23:45 and 1:00 at night
  - This is turn clogged up 911 hotline with few thousand calls related to incident
  - System is not connected to Internet but controlled by special radio communication, so hackers must have had knowledge about radio frequencies and codes required for access

https://www.wired.com/2017/04/dallas-siren-hack-wasnt-novel-just-really-loud/

Equifax (2017)

- Data breach in July 2017 resulted in personal information being compromised
  - 145—148 million US citizens
  - 15.2 million UK citizens
- Included social security numbers and drivers license numbers
- Targeted flaw with Apache Struts used in Equifax’s dispute system
  - Flaw in parsing of certain HTTP headers
  - Patch was made available in March 2017
- Website allowing users to check if they were affected was equally insecure

Netlink Computer Inc (2018)

- Large electronics retailer based in Canada declared bankruptcy
- IT assets including servers, PCs, and hard drives sold without being deleted
- Contained records for 385,000 customers including names, email addresses, passwords (in plaintext!) and some credit card details

GREAT TECHNOLOGY, SELECTION & SERVICE

https://en.wikipedia.org/wiki/NCIX

Australia National University (2019)

- Attack in 2018 but only became known in 2019
- ANU employee fell to victim to spearphishing attack
- Based on learned credentials attacker was able to compromise legacy system with access to internal VLAN using it to collect more information about users and pivot to other systems
- More spearphishing attacks followed
- Eventually attacker obtained credentials for accessing HR/finance file shares from which he/she then exfiltrated data via compromised legacy system
- Public report: http://imagedepot.anu.edu.au/scapa/Website/SCAPA190209_Public_report_web_2.pdf

Toll Group Ransomware Attack (2020)

- Toll Group Australia reported cyber attack in February
- Shutdown range of systems and services
- Toll not very forthcoming with information but based on insiders/experts ransomware (known as "Mailto" or "Kazakavkovkiz",) affected their main data centre and at least hundreds of servers disrupting their operations
- Possibly most significant ransomware attack in Australia to date
- Toll said they didn’t pay ransom, damage unclear (Toll didn’t comment) but reportedly they lost customers
- https://www.afr.com/technology/toll-faces-customer-fallout-after-cyber-attack-20200214-p540s2

Twitter (2020)

- Several high-profile Twitter accounts hacked e.g. Barack Obama
- Social engineering attack via phone which enabled attackers to steal employees credentials
- Hacked accounts were then used for Bitcoin scams earning attacks over $100,000
- https://searchsecurity.techtarget.com/news/252486398/Twitter-breach-caused-by-social-engineering-attack

Case Study: Optus Data Breach (2022)

- In September 2022 Optus announced massive data breach affecting 10 million customers (about 40% of Aussies)
- Leaked names, birthdates, home addresses, phone numbers, email addresses, passport and driver license numbers, Medicare card numbers, …?
- Everything attacker needs for ID theft
- This breach exposed number of issues wrt system security, incident handling, remediation and laws
- Example of how not to do incident handling probably caused by lack of proper planning and controls ("never happens to us")

Case Study: Optus Data Breach (2022)

- Hasn’t been confirmed, but according to insider it was not sophisticated attack but rather data was accessible via **unprotected** API
- Likely multiple causes/chain, i.e. somebody made available unprotected API in assumption it was protected by lower layer while somebody else removed lower layer protection (the “test network”)
- Likely root cause “human error”, but those are inevitable and system should be designed to mitigate these, so really it is “system error”
- Did Optus follow proper data retention policy?
- Sensitive data properly protected inside Optus network?
- OAIC is investigating now

Medibank Private Data Breach (2022)

- Another large high profile breach that affects 10 million customers
- Various personal data compromised
- For some customers ID documents were also compromised
- For some customers health data was also compromised
- Stolen credentials from third-party IT service provider were used and “misconfigured firewall did not require additional security certificate”
- OAIC has opened investigation: https://www.oaic.gov.au/updates/news-and-media/oaic-opens-investigation-into-medibank-over-data-breach

Data Breaches Increasing (2019-2022)

- Could give whole lecture (or two) about ransomware or data breaches
- Not just increase media coverage but number has increased
- All data breaches in 2019 and 2020 – An alarming timeline
- 2021 Thales Data Threat Report found that almost half (45%) of US companies suffered data breach in 2020
- Notifiable data breaches in AU in 2022 (up to June only)
- Top 10 data breaches so far in 2022
- CNET 2022 is shaping up to be an epic fight to protect data

Have You been Pwned?

- Check if you have account that has been compromised in data breach by entering your email address
- https://haveibeenpwned.com/

White Hat / Black Hat Model

White hat

- Identify security weaknesses, but instead of performing malicious attacks and theft, they expose security flaw to alert owner
- Might be paid consultants or actual employees of company that needs its systems protected

Black hat

- Use their knowledge of security weaknesses to circumvent the law, illegally obtain information or deny service -- often for profit

Grey hat

- Somewhere in between

Hacker Profiles

Hacker Profile	Description
Novice (= Script Kiddy)	Limited knowledge Rely on toolkits Can cause extensive damage as they don’t understand attacks Looking for media attention
Old guard hackers	No apparent criminal intent More interested in the intellectual side
Internal/Insider	Disgruntled employees who may use privileges assigned through their job. These pose a big threat! Petty thieves: Opportunistic, taking advantage of poor internal security
Coders	Develop toolkits for sale, e.g. exploit kits, Ransomware-as-a-service
Nation states	State sponsored attackers or cyber spies
Professional criminals	Make money from hacking directly or subcontract for fee
Hacktivists	Often politically motivated activists using Internet as platform

Evolution of Hacking

“Hacker” was word for hobbyist in any technical area. This arose in the 1960s around the MIT mainframe programming community

First password hacks arose in 1960 around the same IBM mainframe’s time sharing system

Hackers circumvented this system to anonymously access the computer

Phreaking

In the 1970’s phone **phreaking** originated. Phone phreaks used variety of methods to access telephone networks to make free calls

https://sites.google.com/site/whatisphreaking/

Phreaking

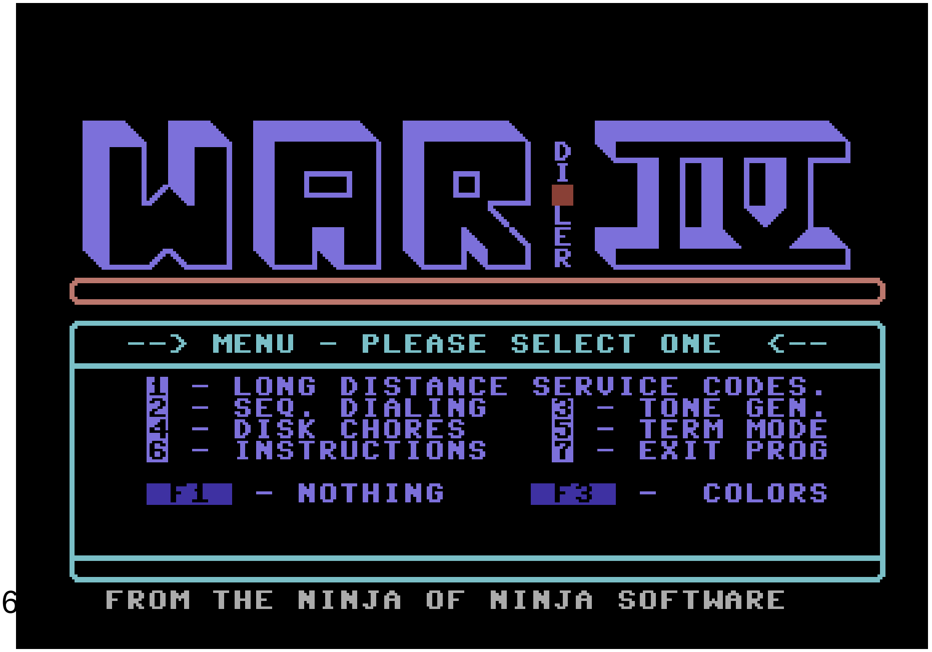
- Bell Labs published two papers in 1954 and 1960 titled "*In-Band Single-Frequency Signaling*" and "*Signaling Systems for Control of Telephone Switching*"

- People discovered that 2600Hz tone was used to signal unused trunk lines. Using certain other tones, phreakers could setup calls from their phone on "unused" trunk lines, allowing free calls around the world

- Famous phreakers included Steve Wozniak and Steve Jobs

First Network Hacking

- In 1980’s phreakers discovered that any server with modem could potentially be entered
- **War dialing** emerged, to search for open modems
- This pre-dates the Internet, so it all seems far fetched!



http://csdb.dk/release/?id=99106

Viruses and Trojans

- In late 80's, viruses and trojans started to appear on the scene
- Still here today, although motivations have changed
- In the past viruses or worms might have just been created for intellectual challenge, now its all about money

Fast Forward

- 1990s onwards brought us Internet, wireless, smart phones, …
- Many services online, new types of services or vastly scaled up existing services, i.e. social networks
- Lots of personal data stored online
- Critical infrastructure accessible and even controlled online
- Much much larger surface for attacks
- Bad guys also benefit from new technology

Attack Vectors Terminology

Malware: Short for malicious software, is umbrella term used for any kind of software that gathers information, disrupts computer system or attempts to spread to increase access

Malware can have very different objectives, sometimes to secretly spy on users, other times to deliberately disrupt use of system

Attack Vectors Terminology

Virus: Program that attaches itself to another program, replicates and at some stage executes (often malicious) payload; generally can’t replicate without host

Worm: Replicates and propagates without having to attach to host. Theoretically worm that can replicate unchecked could infect every computer in the world.

Worms sometimes don’t have a malicious payload but still cause damage. Those with payload may install backdoor into the system or do something malicious.

Attack Vectors Terminology

Trojan: Malicious program that disguises itself as useful program; does not replicate and often installs remote administration tool on victim machine so that attacker can remotely control it later

Spyware: Very broad category of software that sends information from infected computer to the attacker

If you search for “spyware” on Google you will find free spyware removal tools, many of these are actually spyware themselves

So you can see how hard it is for less technically literate people to get by!

Attack Vectors Terminology

Exploit: Software, data, or sequence of commands that takes advantage of bugs or vulnerabilities to cause unintended or unanticipated behaviour to occur in computer software or hardware. Often used for malicious purposes.

Zero-day exploit: Exploit or vulnerability that was previously unknown to creator of exploitable software or hardware and other people. Only known by hacker.

Attack Vectors Terminology

Phishing: Attempt to trick victim into providing sensitive information (e.g. usernames, passwords) through fake email (or SMS…) and / or website to entice potential victims by offering something they might want.

Social Engineering: Act of manipulating victim into performing specific actions or providing confidential information; often exploits psychological principles to convince target to comply.

Core Security Principles

- Security starts with several core principles integrated throughout organization
- These drive many security-related decisions at multiple levels so understanding them is important
- **Confidentiality, Integrity, and Availability (CIA) together form security triad**
- Each element is important to address in any system to be secured

Confidentiality

- Confidentiality aims to prevent unauthorized disclosure of data
- It uses multiple methods like authentication combined with access controls and cryptography
- Authentication and cryptography are presented later in this unit

Key Concepts Related to Confidentiality

Confidentiality ensures that data is only viewable by authorized users

Unauthorized personnel are unable to access information

Encryption algorithms make data unreadable. If the encrypted data falls into wrong hands, the unintended recipient will not be able to read it.

Besides encryption, many elements of security help to enforce confidentiality, including authentication plus access control methods / permissions and physical security.

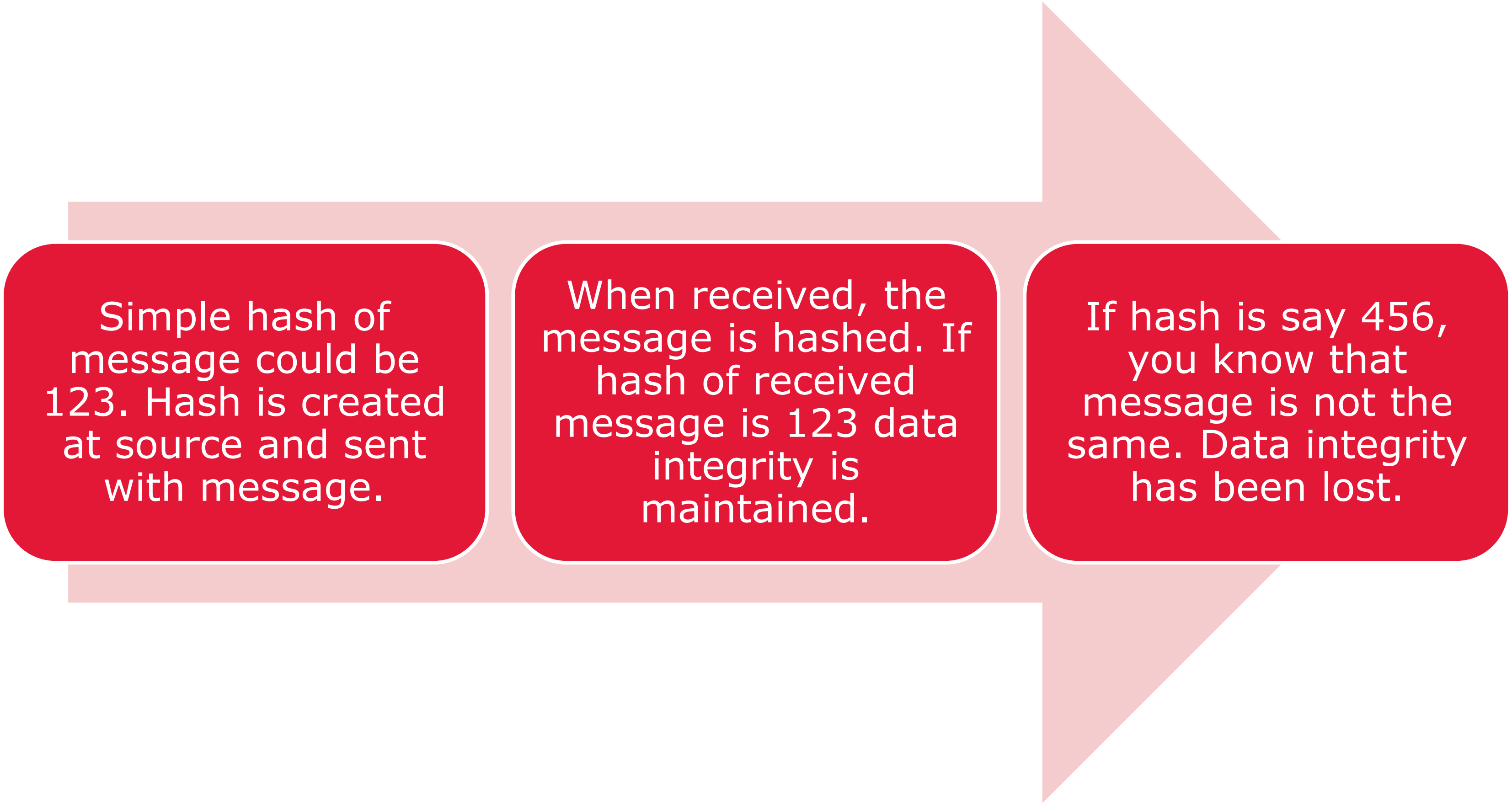
Integrity

- Integrity provides assurances that data has not been modified, tampered with or corrupted
- Only authorized users should be able to modify data
- However, there are times when unauthorized or unintended changes occur - can be from unauthorized users or through system or human errors
- When this occurs, the data has lost integrity

Key Concepts Related to Integrity

- Cryptographic hashing techniques like MD5 (outdated) or SHA can enforce integrity
- Briefly, **hash** is simply number created by executing hashing algorithm on data, such as file or message
- As long as data is unchanged, resulting hash will always be same
- Comparing hashes created at two different times, you can determine if original data is still unchanged - if hashes are the same, the data is the same

Hashing Example



Simple hash of message could be 123. Hash is created at source and sent with message.

When received, the message is hashed. If hash of received message is 123 data integrity is maintained.

If hash is say 456, you know that message is not the same. Data integrity has been lost.

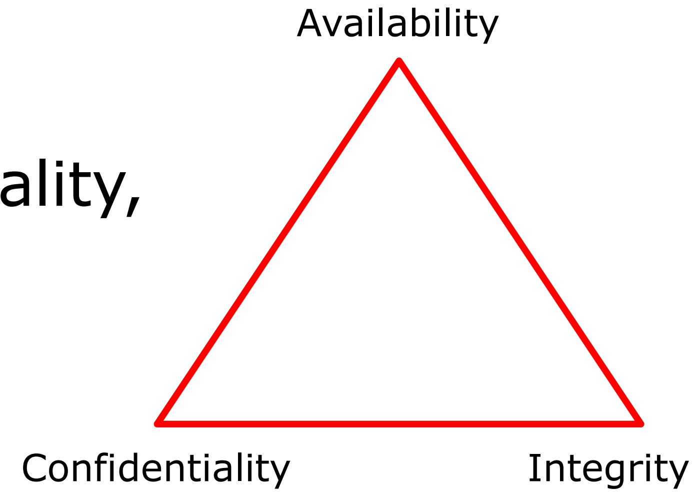
Availability

- Availability means that data and services are available for legitimate users when needed
- For some companies, this simply means that the data and services must be available between 8am and 5pm ☺
- Common goal is to remove single points of failure (SPOF)

Key Concepts for Availability

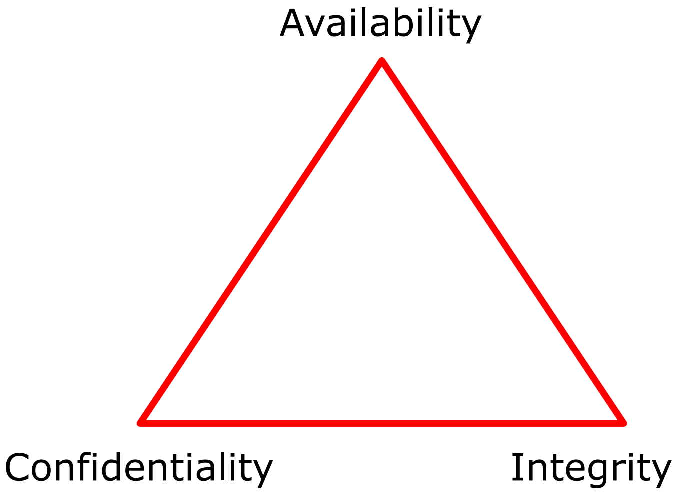
- Fault tolerant systems are up and operational when needed and often addresses single points of failure
    - Redundancy
    - Fail-over
- Availability also means making data accessible to the right people when needed
- In networking concepts, detect and mitigate Denial of Service (DoS) attacks

Balancing CIA



- It’s possible to ensure confidentiality, integrity and availability of data
- However, organization may have priorities
- One way of prioritizing these is with simple values such as low, medium, and high
  - For example, if system holds proprietary secrets, confidentiality is of primary importance and value of confidentiality is high
  - If information is shared anonymously with the public, importance of confidentiality is low

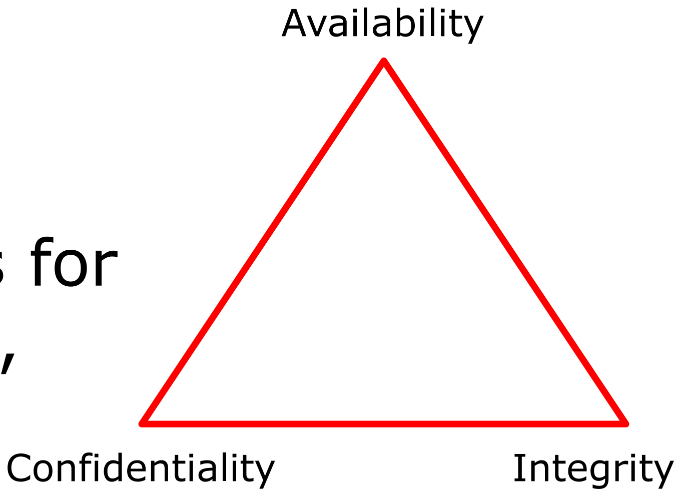
Balancing CIA



- Imagine that you host online forum for users to share information about IT security
- Users can read data anonymously and post data after logging in

What would your priorities be in this example?

Balancing CIA



- Instead, now you host online gaming site that holds accounts for hundreds of thousands of users, including their credit card data
- Users pay for time they’re online playing games

What would your priorities be in this example?

Non-repudiation

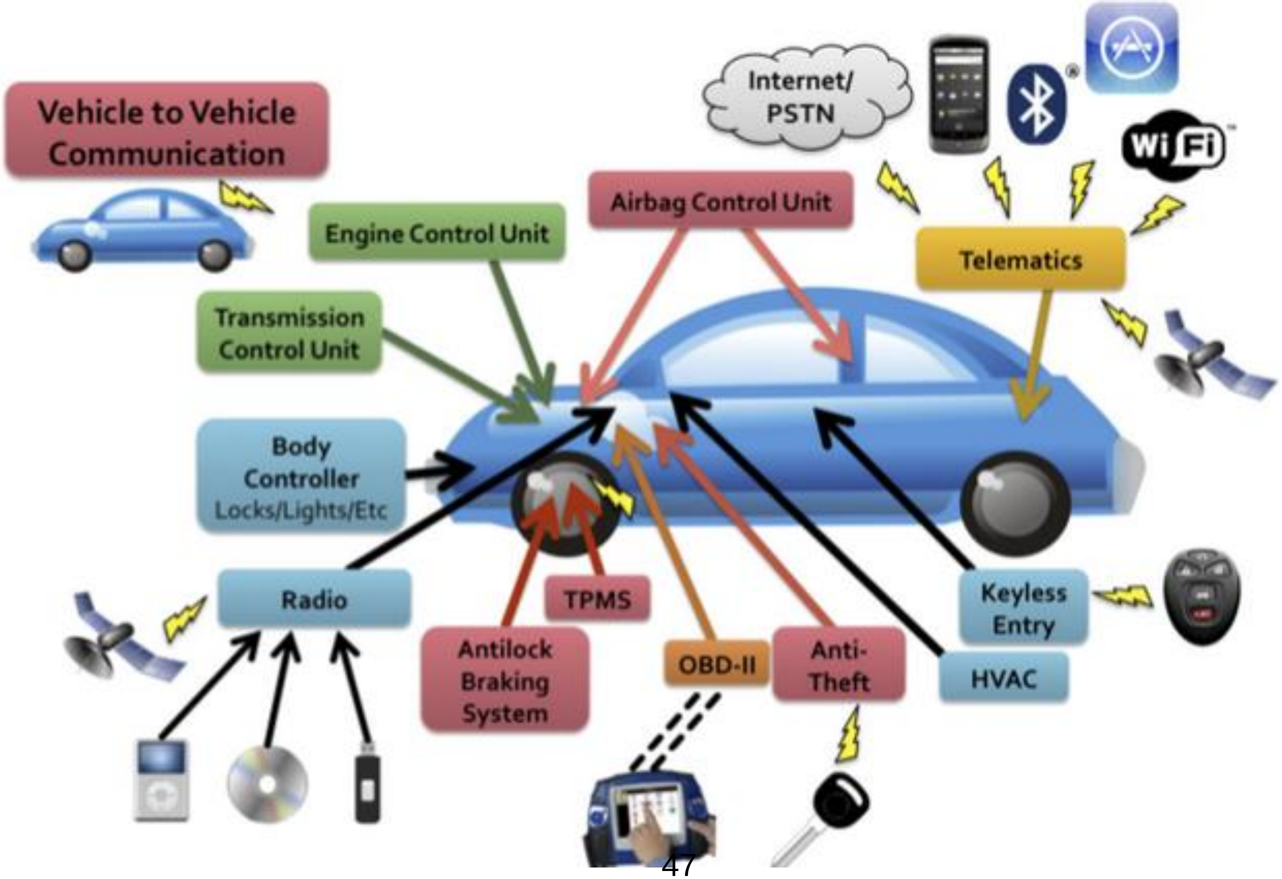
- Non-repudiation isn’t one of core principles, but it is closely related and often specifically mentioned
- Non-repudiation provides proof of person’s identity linked to some actions; can be used to prevent individuals from denying they took specific actions
- Commonly used with credit cards (or contracts more generally). If I buy something and sign receipt, I can’t later deny making purchase. My signature can be used to repudiate me if I deny making purchase. In other words, my signature is used for non-repudiation.

Non-repudiation

- Non-repudiation is used to prevent entities from denying they took an action
- Some common examples of non-repudiation within computer systems are:
- **Using digital signatures to verify someone sent message**. If I send you e-mail that is signed with my digital signature, you know that I sent it
- **Logging activity in audit log**. Audit logs will log details, such as who, what, when, and where; “who” in audit log provides non-repudiation

Attack Surface

- Components of system with which attacker can interact with, giving highest-level entry points for attacker



https://www.peerlyst.com/posts/attack-surface-of-cars-connected-to-each-other-and-the-internet-ben-ferris

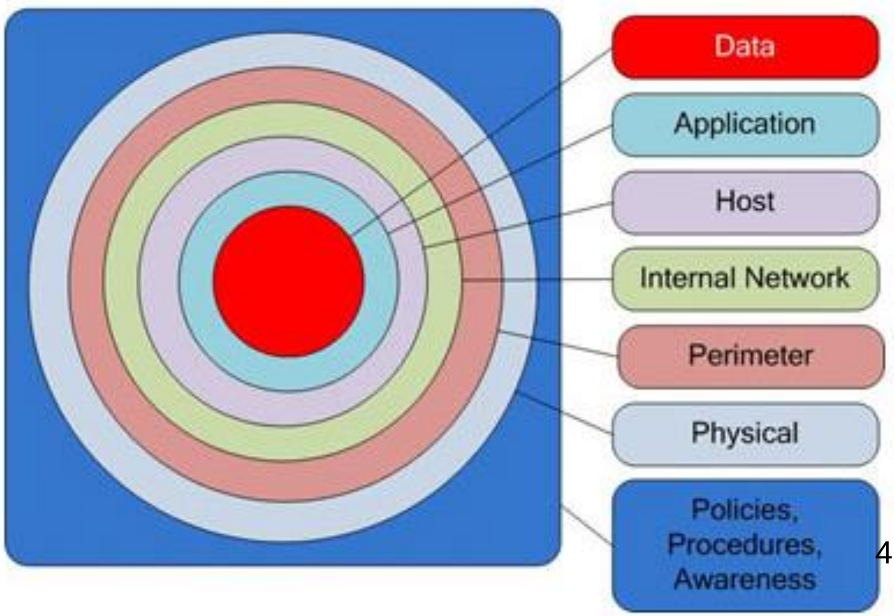
Defence in Depth

- Defence in depth refers to security practice of implementing **several layers of protection**
- You can’t simply take single action, such as implementing firewall or installing antivirus (AV) software, and consider yourself protected
- You must implement security at several different layers

Defence in Depth

Multiple countermeasures are taken to protect information assets

Strategy is based on principle that its harder to beat multi-layered defence system than to penetrate single barrier



https://technet.microsoft.com/en-us/library/cc512681.aspx

Implicit Deny

- Implicit deny indicates that unless something is explicitly allowed, it is denied
- Routers and firewalls often have access control lists (ACLs) that explicitly identify allowed traffic
- If traffic doesn’t meet any explicit rules, the traffic is blocked

Implicit Deny

- Firewall configured to allow HTTP or HTTPS traffic on ports 80 and 443 respectively would have explicit rules defined to allow this traffic to server
- With no other rules, all other traffic would be implicitly denied
- For example, any SMTP traffic sent to this web server on port 25 would be implicitly denied

Implicit Deny

- Same idea applies to file and folder permissions
- For example, in NTFS you can grant permissions, such as Full Control, Read, and Modify
- If Sally is granted Full Control permission to file named Projects and she is only person granted permission, then she would have full control
- What permissions does Bob have? Since Bob is not explicitly granted any permissions, he is implicitly denied all access to file

Least Privilege

- Principal of least privilege or least authority
- Subject must only be able to access information and resources required for legitimate purposes
- For example, user account created for sole purpose of creating backups should not be able to do other things such as installing software
- In cases where some occasional elevated permissions are required, it is best to grant specific temporary elevated privileges rather than blanket access to higher privileges
- For example, on Linux we use tool sudo

Basic Risk Concepts

Basic goal of implementing IT security is to reduce risk

- **Risk** is possibility or likelihood of threat exploiting vulnerability and resulting in loss
- **Threat** is any circumstance or event that potentially compromises confidentiality, integrity or availability
- **Vulnerability** is weakness; can be weakness in hardware, software, configuration or even in users operating a system

Information Security Threats

Network Threats

- Sniffing/Eavesdropping
- Session Hijacking
- Spoofing
- Denial of Service (DoS)

Host Threats

- Malware attacks
- Privilege escalation
- Unauthorized access
- Tampering

Application Threats

- Information disclosure
- Buffer overflows
- Configuration management
- Broken authentication, encryption

Threat Modelling

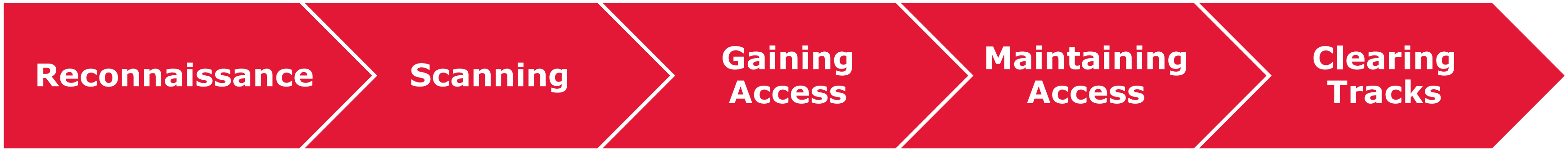
- Identification of potential security threats against system
- Goal: threats can be enumerated, mitigations can be prioritised and fixes can be rolled out
- Process usually involves system diagrams with data flows and brain storming about threats
- Several methodologies exist for Cyber Security purposes, e.g. STRIDE, PASTA
- There are also several tools to support process
- More next week

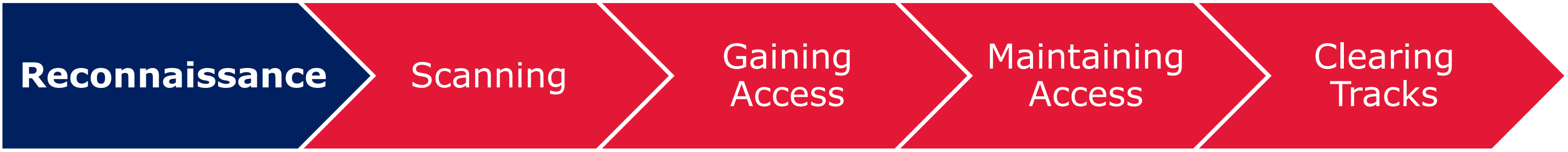
Common Vulnerabilities and Exposures (CVE)

- Common Vulnerabilities and Exposures (CVE) is dictionary of common names (i.e. CVE Identifiers) for publicly known information security vulnerabilities
- CVE’s common identifiers make it easier to share data across separate network security databases and tools, and provide baseline for evaluating coverage of organization’s security tools
- If report from security tool incorporates CVE identifiers, you can quickly and accurately access fix information in one or more separate CVE-compatible databases to remediate problem
- For example https://cve.mitre.org/

Hacking Phases

Let’s consider phases that would be followed when gaining access to system




Reconnaissance → Scanning → Gaining Access → Maintaining Access → Clearing Tracks

Preparatory phase where attacker seeks to gather information about target, prior to launching attack

Recon targets may include, clients, staff, networks and systems

Passive Reconnaissance

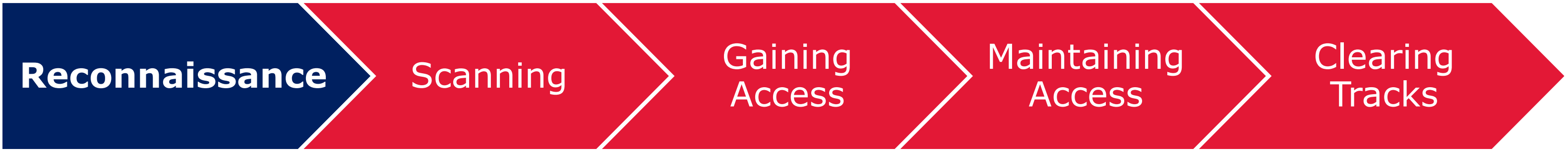
Don't directly interact with target

E.g. searching public records or news

Active Reconnaissance

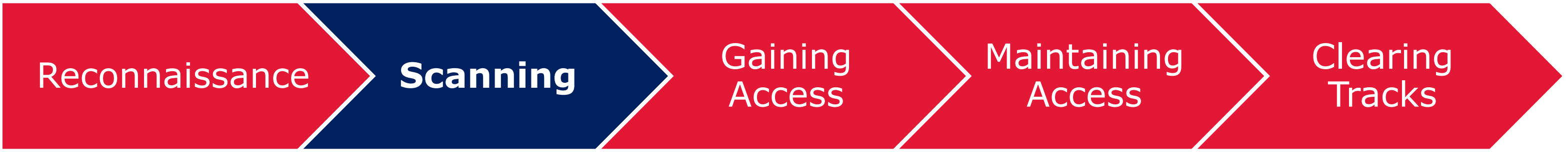
Directly interact with target by some means

E.g. phoning up the technical department



Reconnaissance → Scanning → Gaining Access → Maintaining Access → Clearing Tracks

- This phase allows attacker to plan strategy and may take time
- There are numerous recon techniques, many of them don’t involve computers at all
- In this week’s lab we will do some basic technical recon investigating Internet addresses, domain names and contacts



Reconnaissance

Scanning

Gaining Access

Maintaining Access

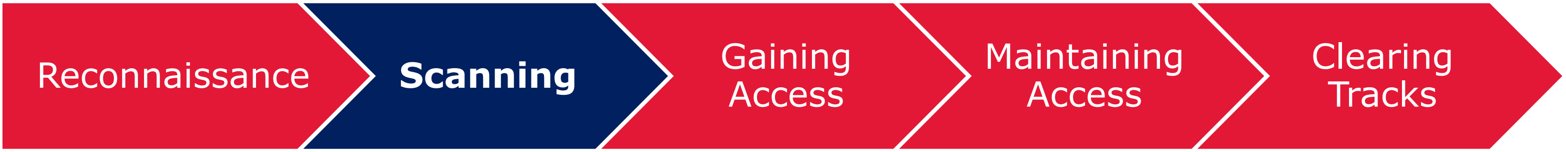
Clearing Tracks

- Active Recon and Scanning overlap a little
- Scanning involves more in-depth analysis though, e.g. port scanning, user lists (CEH differentiates between *scanning* and *enumeration*)

- Active recon and scanning pursued only if attacker is confident that there is low chance of detection

- Newcomers often jump straight into this phase and get caught very fast indeed

Some activities of scanning may be illegal, even though no access to system is gained!


Reconnaissance

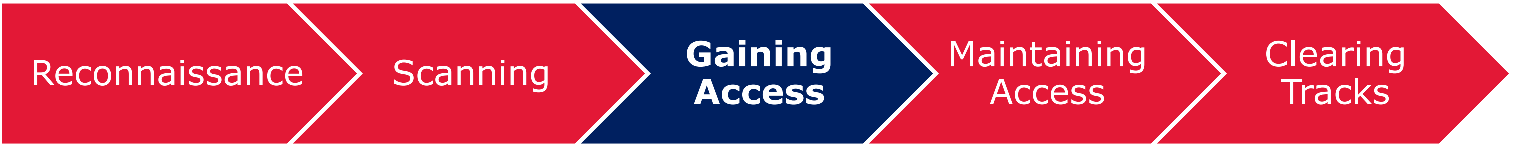
Scanning

Gaining Access

Maintaining Access

Clearing Tracks

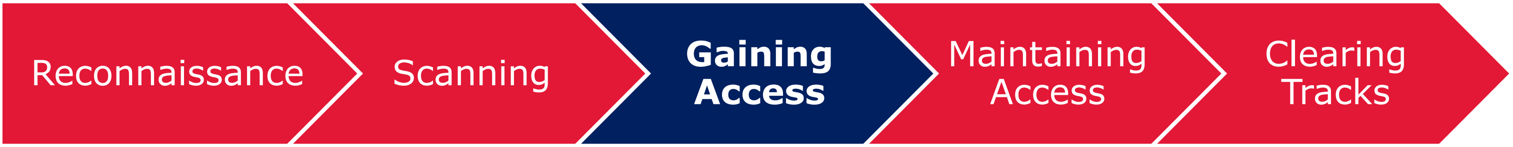
- Scanning is done prior to attacking network
- Automated tools may be used, such as port scanners for network scanning
- We might also use automated vulnerability scanners to determine security baseline


Reconnaissance → Scanning → **Gaining Access** → Maintaining Access → Clearing Tracks

- This is where attacker gets access to system or network at application level, OS level or network level

- Generally attacker tries to get any minimal access as foothold – from here they will attempt to escalate privileges to obtain complete control of system

- At this stage, concepts of **privilege escalation** and **pivoting** are relevant



Reconnaissance

Scanning

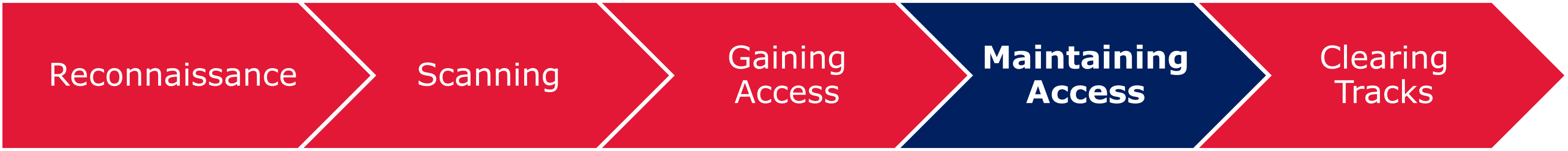
Gaining Access

Maintaining Access

Clearing Tracks

Pivoting refers to using compromised system to attack other systems on same network to avoid restrictions such as firewalls, which may prohibit direct access to all machines

https://techienutzz.wordpress.com/2016/09/25/data-flow-in-computer-network/



Reconnaissance

Scanning

Gaining Access

Maintaining Access

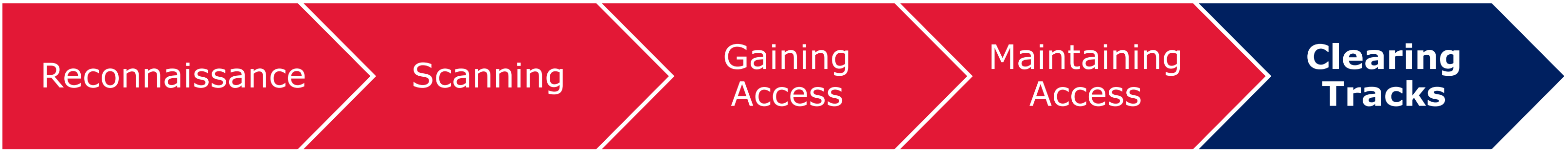
Clearing Tracks

- Now that attacker has access, the plan is to KEEP it

- Attackers who choose to remain undetected may remove evidence of hack and install backdoor, rootkit or Trojan on system so that they can come back later

- Use covert channels to exfiltrate data

- More in later topics


Reconnaissance

Scanning

Gaining Access

Maintaining Access

Clearing Tracks

Attackers always cover their tracks to destroy evidence

Intentions

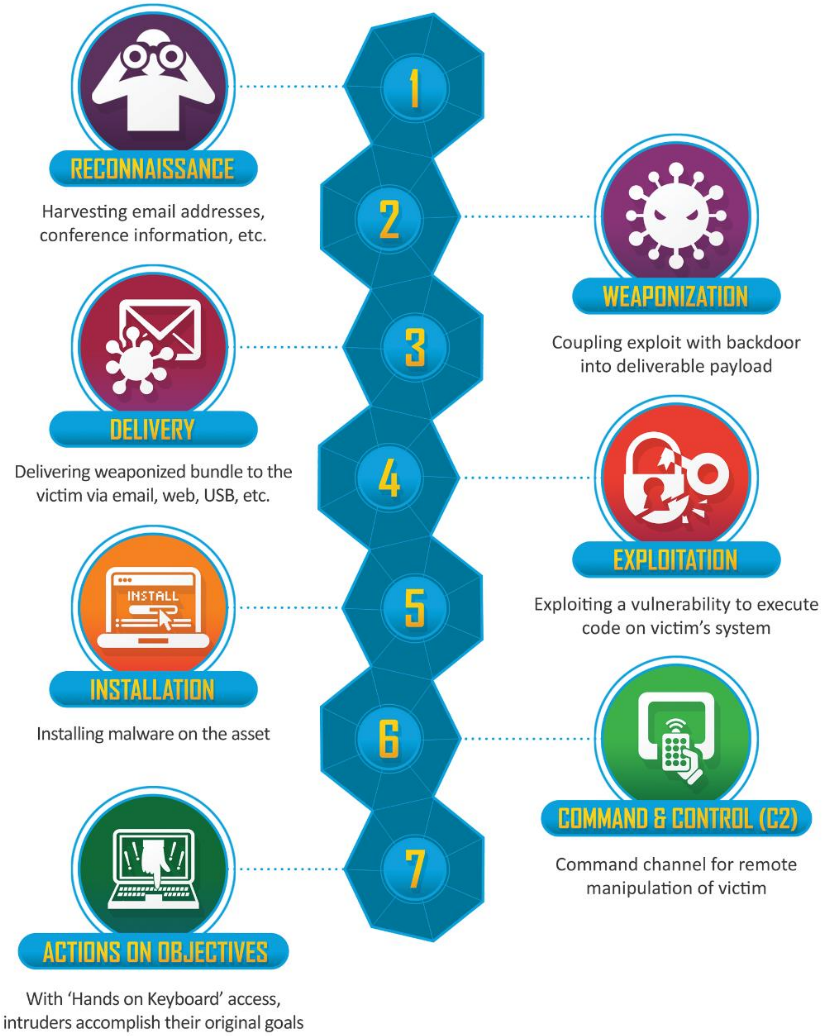
- Keeping target unaware, remaining uncaught, reusing same exploit in future, destroying incriminating evidence

Methods

- Remove traces of activity by overwriting or tampering with audit logs
- Delete files, file systems, metadata
- Reset system to purge volatile memory

Cyber Kill Chain

- Every cyber attack goes through number of steps to achieve objective
- Objective: stopping attacker at early point in chain



1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Ethical Hacking

- Thinking like hacker is great way to beat one
- Ethical hackers will anticipate techniques that attackers may use, and be able to secure systems in anticipation of these attacks
- Also referred to as pen(etration) testing

Ethical Hacking

Organisations recruit ethical hackers

- To counter hackers and information breaches
- To counter against terrorism and security breaches
- To build resilient systems
- To test organisations own security

Ethical hackers answer these questions

- What can intruder find on system?
- What can intruder do with this knowledge?
- Would intruder get caught?
- Is organisation’s environment safe?
- If not, how would we make it safe and at what cost?
- Are security measures in line with industry practises?

Lecture Summary and Week Ahead

- Attack vector terminology
- Risk/threat etc. terminology
- Dimensions of security (CIA triangle, non-repudiation)
- Important concepts (attack surface, defence in depth)
- Basic security principles (implicit deny, least privilege)
- Phases of hack/attack

- Labs: Introduction, Basic Information Gathering

- Next week: Network Security