Topic 6:

Vulnerability Assessment

Topic 6 – Lecture 1:

An overview of vulnerability

Network Security and Cryptography

Vulnerability Assessment Topic 6 - 6.2

Scope and Coverage

This topic will cover:

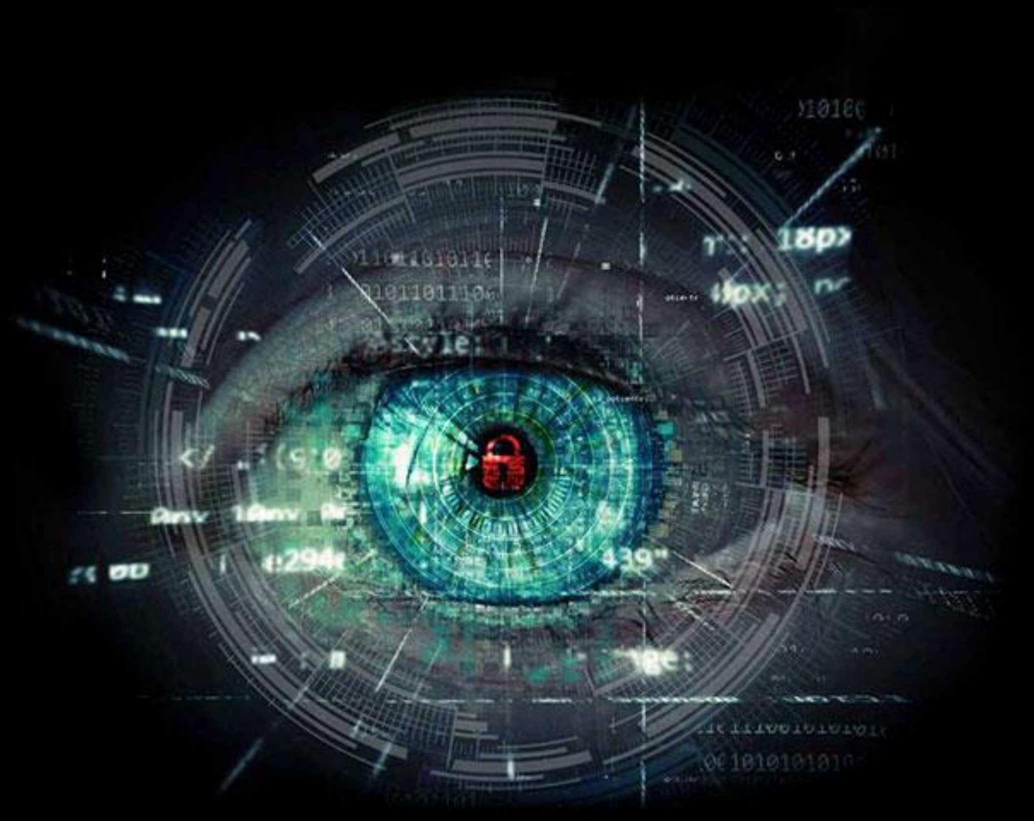
01 Overview of network vulnerability

02 Port scanners

03 Password crackers

Learning Outcomes

By the end of this topic students will be able to:



- Use port scanners to highlight open ports
- Perform password cracking using dictionary and brute-force methods

Security Vulnerability - 1

Vulnerability Assessment Topic 6 - 6.4

- A security vulnerability is a flaw or a weakness in a system or network that allows an attack to harm the system or network in some way, such as:
  - Allowing an unauthorised user to access the system or network
  - Causing a deterioration in the performance of the system or network
  - Damaging or altering the data held by a system or network

Security Vulnerability - 2

- The vulnerability may be inherent in the system
  - E.g. new software includes a vulnerability when it is deployed, even if installed and operated correctly
- The vulnerability may be as a result of the implementation of a system
  - E.g. the configuration of new software
- The vulnerability may be as a result of the operation and management of a system
  - E.g. poor security procedures

Causes

- Software - flaws in new software, not tested sufficiently before deployment
- Hardware – dust
- Organisation procedures – poor password policy, lack of audits
- Personnel – not training staff properly
- Physical environment – no physical access controls, risks from flooding
- Combinations of the above

Complex Systems

- Computer networks in large businesses are usually large and also complex
- A larger system is more likely to have security holes
- A complex system is more likely to have security holes
- Complete testing of large, complex networks is very difficult and extremely time consuming

Common Components

- Modern networks will use common components:
  - Software used by many others (sometimes open-source)
  - Hardware used by many others
  - Operating systems used by many others
- Attackers will have access to these components and be familiar with any security flaws they have
- The Internet rapidly spreads the knowledge of these flaws and increases the likelihood of them being quickly exploited

Many Services

- A typical modern network will provide numerous services to an organisation
- More services means:
  - More protocols
  - More ports
  - More connections
- The network is therefore more open to attack

Password Vulnerability

- Vital to enforce the use of strong passwords
- Vital to regularly change passwords
  - And ensure this is a real change not ‘abc1’ changed to ‘abc2’
- Most users will use a really weak password if they can as it is easier to remember
  - A 2006 UK survey gave the top 3 passwords as:
    - 123
    - Password
    - Liverpool

Operating Systems (OS)

- Default settings can leave system open to attack
  - E.g. granting full access rights to any user – this gives every program, including any malware on the network, full administration privileges
- Even where an OS has no inherent flaws the network administrator must set suitable permissions in order to protect the network

Surfing the Internet

- The Internet is awash with viruses, spyware and other malware
  - And, of course, a lot of very useful and high quality content!
- The web browsing policy of an organisation, plus its firewall etc. is vital in protecting the whole network
- Acceptable use policies and staff training form a vital part of the protection

Software Bugs

- New software may contain security flaws that can be exploited by a hacker
- This is not a malicious act but the complexity and amount of code in modern software applications make this inevitable
- Updates and regular patches are issued by software providers to fix these vulnerabilities as they are discovered
  - One of the many reasons for using genuine software

User Input

- Programs that allow user input must check that input to prevent malicious code inclusion
- Common attacks on systems are:
  - SQL Injection attacks
  - Buffer Overflow attacks
  - (See Private Study Exercises for more on these)
- Human error is the biggest threat to security:
  - May be malicious or not
  - Includes designers, programmers and users

Repeating Mistakes

- It is important to learn from past mistakes
- Modern programming code reuses old programming libraries
- Must ensure that any vulnerabilities that have been discovered are removed
- The Open Web Application Security Project (OWASP) publishes known vulnerabilities to help system designers and programmers from repeating past mistakes

Prevention

- Vulnerabilities have been found in every operating system
  - Hence the updates and patches that appear and should be installed
- The best prevention is sound security practices:
  - System maintenance
  - Firewalls and anti-virus
  - Staff training
  - Access controls
  - Audits

Testing Your Own Security

- Software is available to test your own network for security vulnerabilities

- In some instance it will remove the vulnerability
  - The vulnerability scanner will be covered in more detail in the next lecture

- No matter how good the software is it is still important to have trained staff who follow sound security practices and report any potential threats

Break

Daffodil International University

Topic 6:

Vulnerability Assessment

Topic 6 – Lecture 2:

Managing Vulnerability, Port Scanners & Password Cracking

Network Security and Cryptography

http://www.freepowerpointtemplates-design.com

Vulnerability Management

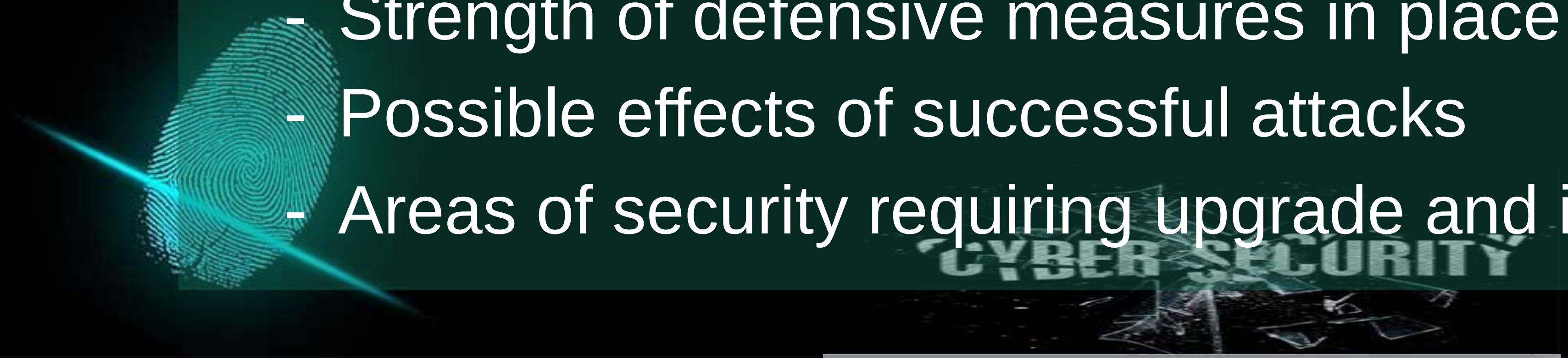
- All networks will contain vulnerabilities
- Therefore managing these vulnerabilities and the risks associated with them is a key task of network management
- Managing vulnerability includes:
  - Prioritising vulnerabilities
  - Fixing vulnerabilities
  - Reducing the effects of potential breeches
  - Monitoring for new/unknown vulnerabilities

Known and Unknown

- Known vulnerabilities in software, operating systems and networks are well documented
- Tools (***vulnerability scanners***) are available to test for know vulnerabilities (***penetration testing***)
- Networks will also have unknown vulnerabilities that have not yet been discovered
- The implementation of sound security policies and the use of best practice is the best defence

Penetration Testing

- A penetration test mimics the actions of a malicious attack on a network
- The aim is to discover the vulnerabilities that exist and that could be discovered by an attacker
- Provides information on:
  - Threats to the system
  - Strength of defensive measures in place
  - Possible effects of successful attacks
  - Areas of security requiring upgrade and investment



Vulnerability Scanner

Vulnerability Assessment Topic 6 - 6.23

- A vulnerability scanner can be used in a penetration test
- It is software that tests a system or network for weaknesses
- Different types are available
- Each type focuses on a particular area of potential weakness
- Can only discover known vulnerabilities

Vulnerability Scanners

- Types are available for scanning:
  - Ports
  - Networks
  - Databases
  - Web applications
  - Individual computers
- We will take a closer look at Port Scanners

Port Scanners

- Software that probes for open ports
- Used by network administrators to test the network
- Used by attackers to look for vulnerabilities
- The TCP/IP protocol suite has services being supplied by a host through a port
- There are 65536 different port numbers available
- Most services use only a very limited number of ports

Port Status

- A port scan will generally give one of three results:
  - *Open* – there is a service using the port and the host has replied with a message that it is listening for communications on this port
  - ***Filtered*** – no reply is received meaning that there is some filtering occurring on this port, typically via a firewall
  - ***Closed*** – a reply is received stating that communication is denied on this port

Port Scan Types

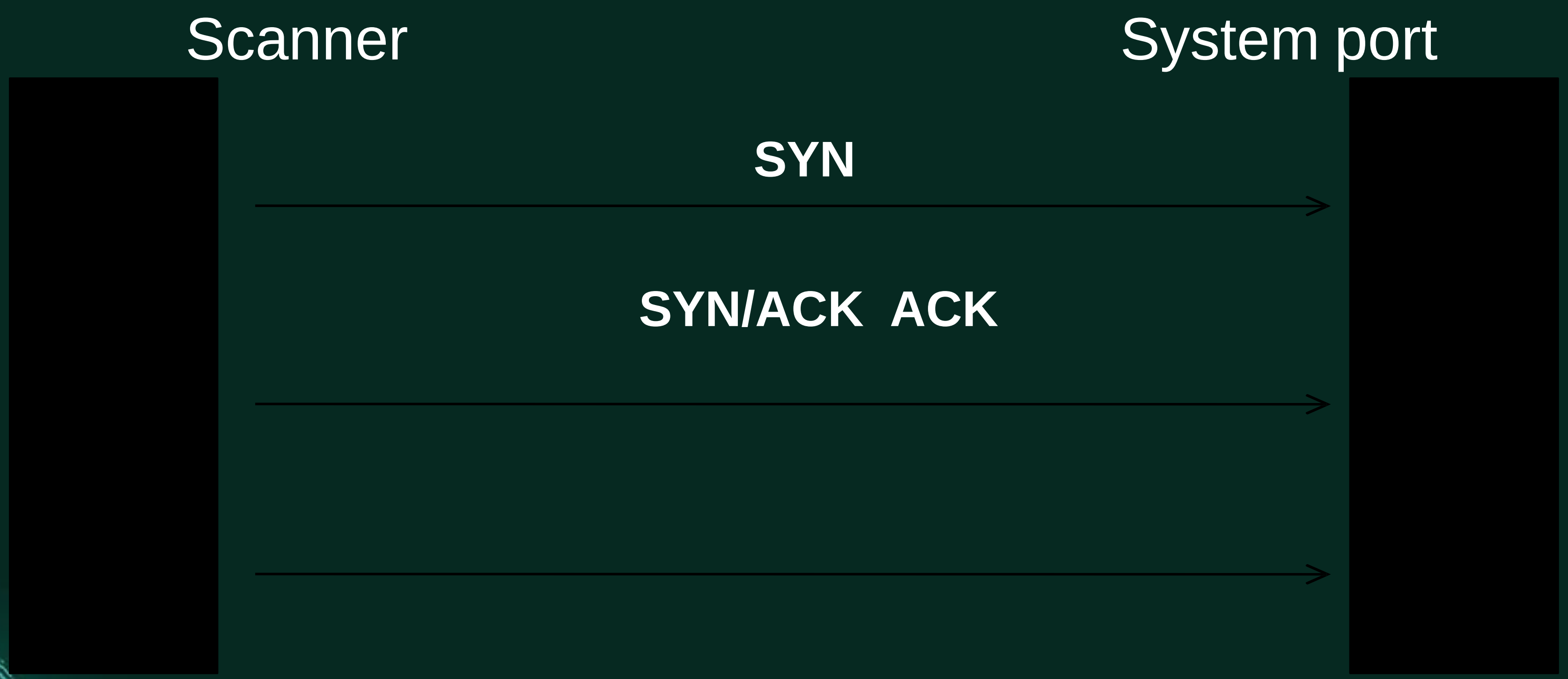
- There are several types of scan, including:
  - TCP connect scan
  - TCP SYN scan
  - TCP FIN scan
  - TCP Xmas Tree scan
  - TCP Null scan
  - TCP ACK scan
  - TCP Windows scan
  - TCP RPC scan
  - UDP scan

TCP Connect Scan

- Connects to the target port and performs the TCP three-way handshake
  - Sends a synchronise (SYN) packet to host
  - Host returns a synchronise acknowledgement (SYN/ACK)
  - Sends an acknowledgement (ACK) to host
  - SYN and ACK are indicated by a bit in the TCP header
- This scan is easily detected by the target system

TCP Three-Way Handshake

Vulnerability Assessment Topic 6 - 6.29



TCP SYN Scan

- A full TCP connection is not made
- Also known as a half-open scanning
  - SYN packet sent to host port
  - Either SYN/ACK or RST/ACK (reset/acknowledgement) received
  - This tells the scanner whether it is open or closed
  - RST/ACK sent to port so full connection is never made
- May not be detected by host

TCP FIN scan

- A FIN packet is sent to the port
- This means no more data from sender
- The targeted host should send back a reset RST packet for all closed hosts
- Usually only works on Unix based hosts

TCP Xmas Tree and Null scans

- ***Xmas Tree*** sends FIN, URG and PSH packets to the target port
  - Finished, urgent and push buffered data to receiving application
- The target system should send RST for all closed ports
- ***Null*** turns off all flags in the packet to the target system
- This should return RST for all closed ports

TCP ACK Scan

- Used to map the rulesets associated with firewalls
- By sending an ACK packet the aim is to determine the type of firewall.
- A simple packet filter firewall will only allow established connections (with the ACK bit set)
- More complex stateful firewalls use more complex rules with advanced packet filtering

(We look at firewalls in more detail later in the course)

TCP Windows & RPC Scans

- ***TCP Windows*** scan may be able to detect open ports on some operating systems
- This is due to an anomaly in the way TCP window size is reported
- ***TCP RPC*** scans detect remote procedure call (RPC) ports on Unix systems
- They can also detect associated programs and version numbers

UDP Scans

- Sends a UDP packet to the target port
- If it receives a “ICMP port unreachable” message the port is closed
- If the message is not received it may be assumed that the port is open
- UDP scans are slow
- Results are unreliable as no message may be received for other reasons

Password Cracking

- Cracking a password can enable an attacker to gain access to:
  - A network
  - A computer
  - Individual files
- Does not necessarily require intelligent techniques
  - May involve reading the note the user has kept, sometimes stuck on the monitor!

Dictionary Attack

- A simple and fast way to crack a password
- A text file contains a set of dictionary words (the dictionary file)
- This is loaded into the software package
- It runs against user accounts in the application the hacker is attacking
- Most passwords are simple and easy to crack

Brute Force Attack

- May take a long time to work
  - Depends upon password complexity
- All possible combinations of characters are used until the correct combination is found
- Software packages do the work for you but it can still take weeks to crack a password this way
- Best defence is to use cryptographic methods allied to strong passwords

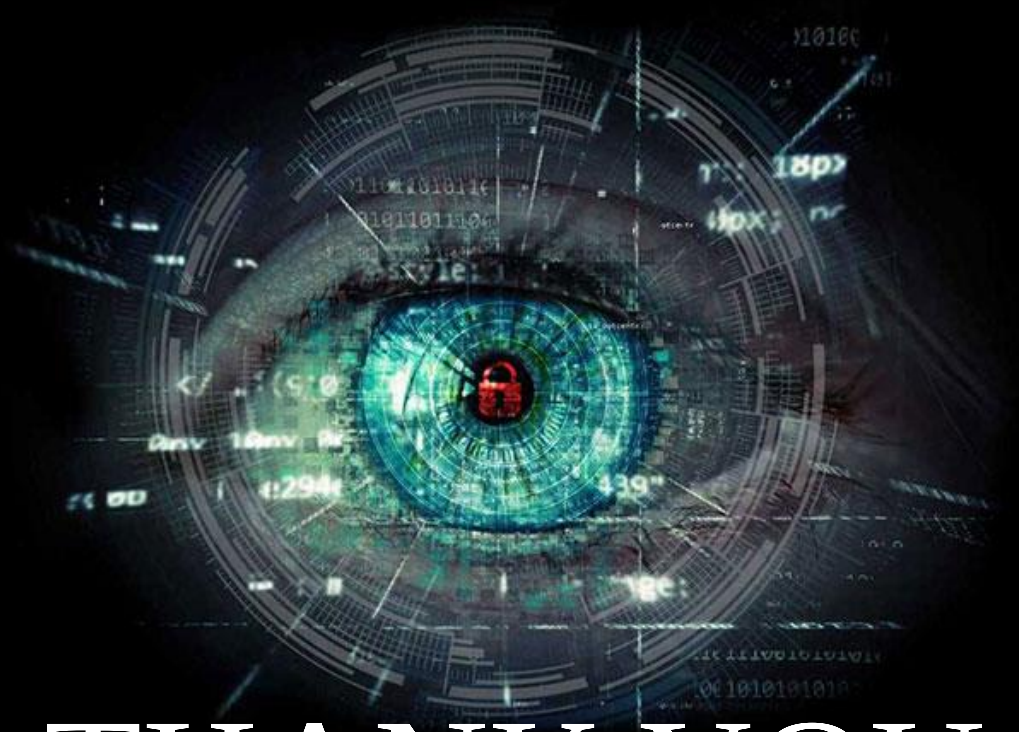
Password Cracking Software

- Many packages available, popular ones are:
  - Cain and Abel
  - John the Ripper
  - Hydra
  - ElcomSoft
  - Lastbit

References

- Scambrey, J., McClure, S. and Kurtz, J. (2001). *Hacking Exposed: Network Security Secrets & Solutions*. 2nd Edition. McGraw Hill.

- The Open Web Application Security Project (OWASP) website: https://www.owasp.org/index.php/Main_Page



THANK YOU
Any Question?

Topic6 – Vulnerability Assessment