**Security Vulnerability**

A security vulnerability is a flaw or weakness in a network or system that makes it possible for an attack to negatively impact the network or system, including:

* enabling unauthorized access to a network or system
* causing the system's or network's performance to decrease
* destroying or changing data stored on a network or system

It's possible that the system is inherently vulnerable.

For example, even when installed and used properly, new software has a vulnerability when it is deployed.

The implementation of a system could be the cause of the vulnerability.

For example, setting up new software

The vulnerability could arise from how a system is run and maintained.

For example, Bad security protocols

**Causes**

Software-flaws in new software, not tested sufficiently before deployment

Hardware - dust

Organization 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 System**

Large companies typically have large and complex computer networks.

Security flaws are more likely to exist in larger systems.

Security flaws are more likely to exist in complicated systems.

Large, complex networks require a great deal of effort and time to thoroughly test.

**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 organization

More services mean:

• More protocols

• More ports

• More connections

The network is therefore more open to attack

**Password Vulnerability**

Enforcing the usage of secure passwords is vital.

It's vital to change passwords regularly.

Additionally, make verify that "abc" actually changed to "abc2."

Since it's easier to remember, the majority of users will use a really weak password if they can.

A 2006 UK survey gave the top 3 passwords as:

123

Password

Liverpool

**Operating Systems**

System vulnerabilities may arise from default settings.

For example, giving every user full access right gives all programs, including malware on the network, full authority.

Network administrators need to specify appropriate permissions in order to secure the network, even in cases where the operating system is flawless.

**Surfing the Internet**

Malware, including spyware and viruses, is widely available on the Internet.

* And, naturally, lots of excellent and really helpful things!

An organization's web browsing policy, firewall, and other security measures are essential for protecting the whole network.

A vital part of the protection is worker training and acceptable use standards.

**Software bugs**

Hackers may be able to take advantage of security holes in newly released software.

Although the quantity of code and complexity in modern software programs make this necessary, the conduct is not malicious.

Software providers release updates and fixes on a regular basis to address vulnerabilities as soon as they are found.

* Among the many benefits of utilizing original 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

**Buffer Overflow Attack**

A continuous block of memory set aside for a particular use, like an array, is called a buffer.

The amount of data a user can write to a buffer might not be capped, hence this could overrun the buffer and travel outside its boundaries.

Unexpected behavior may occur if a program writes more than the buffer's allotted RAM.

The software will try to carry out these commands if the extra data is stored into memory locations designated for program instructions rather than data.

By inserting malicious code into this overflow area, a hacker can cause a program to run their commands instead of the ones the writer intended.

**Repeating Mistakes**

It's critical to take in lessons from previous errors.

Old programming libraries are reused in modern programming code.

It is necessary to make sure that any vulnerabilities found are fixed.

Open Web Application Security Project (OWASP) provides information about known vulnerabilities to assist programmers and system designers in avoiding coding errors.

**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**

You can use software to check for security flaws in your own network.

It will sometimes remove the vulnerability.

* In the upcoming lecture, the vulnerability scanner will be discussed in greater detail.

No matter how good the software is, having staff who is trained in security procedures and can identify and report any risks is still crucial.

**2 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:

• Prioritizing vulnerabilities

• Fixing vulnerabilities

• Reducing the effects of potential breeches

• Monitoring for new/unknown vulnerabilities

**Know and unknow**

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 defense.

**Penetration Testing**

A penetration test mimics a malicious network attack’s movement.

Finding current vulnerabilities as well as those that an attacker might find is the aim.

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**

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.

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 - The server has responded to a service that is using the port by stating that it is listening for messages on this port.

Filtered - If there is no response, there must be filtering on this port, usually done by a firewall.

Closed - We receive a reply indicating that this port is closed to communication.

**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 synchronize (SYN) packet to host

• Host returns a synchronize 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 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.

**TCP Windows and RPC Scans**

On some operating systems, TCP Windows scan may be able to identify open ports.

This is because of an error in the reporting of TCP window size.

Remote procedure call (RPC) ports on Unix systems are found by TCP RPC scans.

They are also able to identify version numbers and related programs.

**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 quick and easy method for password cracking.

A list of dictionary terms is contained in a text document (the dictionary file).

This is included into the software package.

It operates on user accounts within the program that the hacker is targeting.

Simple passwords are typically easy to figure out.

**Brute Force Attack**

Make take long time to work

* Depending on how complicated the password is.

Until the right combination is determined, all potential character combinations are used.

Although software programs handle the work for you, breaking a password this method can still take weeks.

Using cryptographic techniques in combination with strong passwords is the best defense.

**Password Cracking Software**

Many Packages available, popular ones are:

Cain and abel

John the Ripper

Hydra

ElcomSoft

Lastbit