Security Risks

Denial Of Service Attacks and effects

A **Denial of Service (DOS)** attack is an active attack, where an attempt is made to force a website/online service to not be able to provide its service.

How will you know you are being DOS'ed?

- Your server/system may have slow/sluggish performance
- users may have an inability to access it

Reason's behind a DOS attack?

Financial

Blackmail

Hacker for hire

Political

You don't agree with the other sides views

Personal

Grudge against a former employer etc

Motivation behind a DOS attack?

Personal

Disgruntled employee
Relationship breakup

What about anti competitive practices?

Can be be financially motivated or personal?

What about just to see if it can be done?

Costs associated with a DOS attack

There will be costs associated with a DOS attack
Some costs would be

1. **Lost revenue** through to **downtime**
2. **Determining the nature** of the attack
3. The payment for **labour to repair and response to the attack**
4. Payment for **labour** to devise and **implement safeguards**
5. **Additional admin** to compensate for loss of network services

Types of DOS

There are various methods by which a Denial Of Service attack can be implemented

1. Physical/Hardware
2. Bandwidth Consumption
3. Resource Starvation
4. Hardware attacks
5. Routing/DNS Attacks

Physical Attacks

The easiest **physical attack** is to actually cut the wires/break the service of a server
This can be through attacking switches/routers or other infrastructure

Bandwidth Consumption

An attacker may be able to flood your server with packets of information

These can be as simple as PING (ICMP echo) requests

This forces the server to respond that it has received the packet

This **consumes the bandwidth available** to the server

Resource Starvation

A server has a finite amount of physical **resources** such as

Backing Storage

Memory

An attack of this type will try to exhaust these resources

What if you are able to continually force a server to create new user accounts or new orders

Or spamming an email server so that it uses all of the available backing storage?

Not all DOS are malicious

A “test email” sent to more than 1.2 million NHS employees caused the entire system to crash on Monday morning (14/11/16)

NHS staff used Twitter to complain about an email that “inadvertently” included everyone on the mailing list of the NHSmail system. As thousands of **replies to all** were sent in response, asking to be removed from the mailing list, many claimed the entire system crashed.

Staff used social media to encourage others to stop replying to the message.

DNS Attacks

When you enter a URL into a browser. This URL is sent to a **DNS server (Domain Name Service)**

The DNS server **resolves** the URL into an IP address

DNS attacks (cont.)

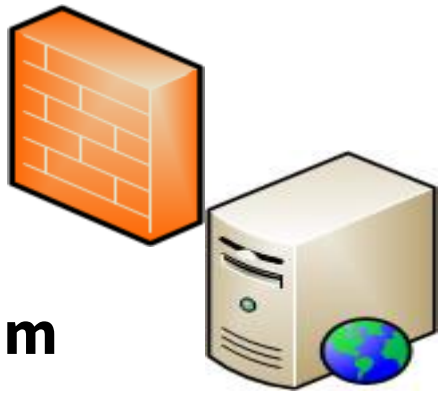
One type of DNS attack would be to cause the DNS servers to route traffic to a target server consuming bandwidth

Another would be to route traffic to a server of the attackers choosing

So the users are denied the access of the server they wanted to

Example DOS Attack

Attacker



Victim

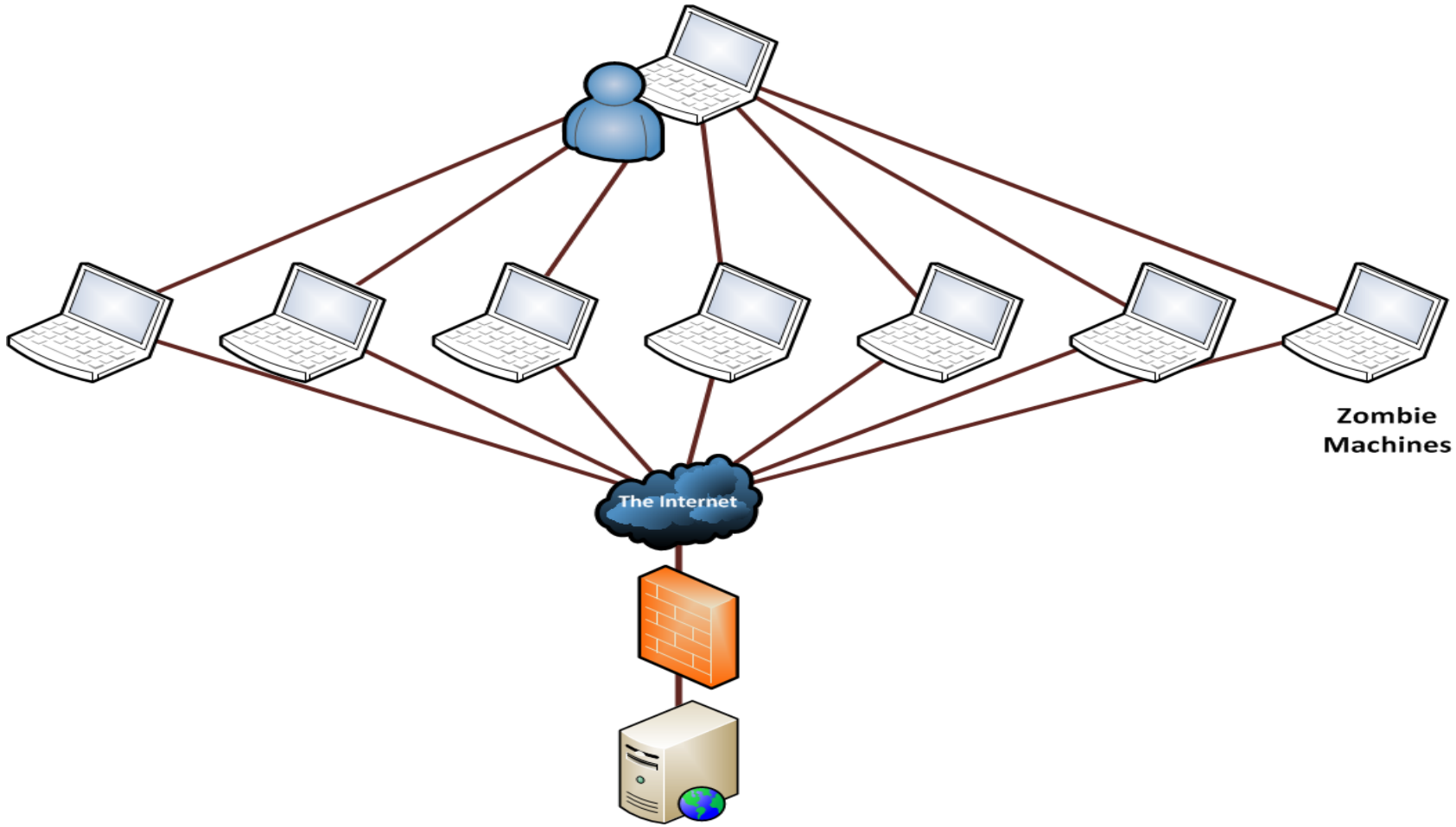
Distributed Denial Of Service (DDOS)

A **Distributed Denial of Service (DDOS)** attack is a type of DOS that uses a network of computers sometimes called a **botnet** or **zombie army**.

The users of the zombies may be unaware

Can be achieved through viruses/trojans

Example DDOS



Passive Attacks

Passive attacks are where an attacker may just monitor a network
Perhaps just intercepting data

Can be very difficult to identify this is occurring

Encryption would be the primary defence against this