Class 3: Information security basics v2

Note Title

[Start by discussing origin or nature of the CNS test.]

Definitions you need to know are in red.

packet – all traffic on the internet is sent in chunks called packets, typically 500–1000 bytes in size. The header contains information about the packet; the payload is the remaining data (e.g. video, web page)

IP – internet protocol – the protocol that defines how (essentially all) traffic on the internet is transmitted. Uses numeric addresses for source and destination
e.g. 64.123.6.2

Activity: what's the IP address of your computer?
what's the IP address of facebook.com?

Hint: use a search engine, or the terminal command "ping facebook.com"

[Wireshark demo: see amount of traffic (much more than you might expect), plus source and destination IP addresses and TCP port numbers)

port number – each packet has a port number which tells the receiving computer which programs should be given the data. Some are standard, e.g. port 80 is for web traffic and would be delivered to a browser. Others can be used by any program e.g. 57289.

Packets hop between many machines, called **routers**, between source and destination.

Activity: How many hops between your machine and
a) www.dickinson.edu ?
b) www.google.com ?
Hint: use terminal command "traceroute www.dickinson.edu"

spyware – software that collects or records information about computer users (without them knowing about it) and typically sends the information back to the spyware authors.

root – the identity of a user who has permission to do essentially anything on a given computer.

bothet – [fill in yourself for homework]

DNS – the service that translates computer names like "www.dickinson.edu" into numeric IP addresses like "57.204.32.63".

[discussion: see Wikipedia page on root name servers. discuss location & redundancy of these servers. Note the US-centric distribution, and involvement of the US military].

flood attack / denial of service attack – degrade or eliminate the ability of a given computer to do its job, by sending it many requests or a lot of data

Note: doesn't destroy or steal data, just denies service.

Examples:
- SYN flood (send part of a web request)
- HTTP flood (send a full web request)
- DNS amplification (send requests to many DNS servers, as if they came from the target. Target then gets hit by many responses.)

spoofing – faking the origin of a packet

malware – a generic term for any software that does something bad to a computer, without the user's knowledge.

firewall - software or hardware that blocks certain types of packets (for example, based on the port number).

demo: - ssh from mac to another lab machine (ask for IP address or use name e.g. tone12203.fas.lcl) ← ip via ifconfig if necessary
- now ssh to laptop, show packets arriving via wireshark ← get IP via ipconfig
- can't turn on windows firewall via group policy, but show how to construct a rule that would block it.

- weakness of firewall: can only block traffic that can be described, but malicious traffic could be disguised as innocent traffic (e.g. botnet commands disguised as web traffic).