**[3413ICT Network Security](C:\\Documents and Settings\\s995689\\Local Settings\\Temp\\Courses_2013\\Courses_2003\\6216INT_03\\6216inthome.html)**

**Workshop 6A**

1. What are the typical phases of operation of a virus or worm?

Virus: Enters an infected machine through file sharing, downloading files, etc. A user must run the virus on the computer. One the file is run the computer becomes infected and a virus begins infecting other processes and applications on the computer.  
  
Worm: propagates over the network. One a computer is infected it continues to propagate infecting other machines.

1. Explain the role of compression in the operation of a virus.

When a virus infects other files and processes they can be detected because the increased file size can be detected. First compressing the file, and then infecting the compressed file makes the virus more difficult to detect.

1. What is the role of encryption in the operation of a virus?

A polymorphic virus is able to change its signature making it difficult to detect, remove, and quarantine. A virus can achieve this by encrypting itself to avoid detection.

1. The Morris worm used three separate attack vectors. What were they and how did they work?

It attempted to log on to a remote host as a legitimate user. In this method, the worm first attempted to crack the local password file and then used the discovered passwords and corresponding user IDs. The assumption was that many users would use the same password on different systems. To obtain the passwords, the worm ran a password-cracking program that tried

a. Each user’s account name and simple permutations of it

b. A list of 432 built-in passwords that Morris thought to be likely candidates. All the words in the local system dictionary

2. It exploited a bug in the UNIX finger protocol, which reports the whereabouts of a remote user.

3. It exploited a trapdoor in the debug option of the remote process that receives and sends mail.

1. What is a digital immune system?

A digital immune system is a rapid response system that was designed to detect and learn from malware. When new malware is released the immune system captures it, analyse it, learns how to shield from it, removes it, and then passes information about it to the client so the malware can be detected before it is allowed to run elsewhere

1. How does behaviour-blocking anti-virus software work?

Behaviour based anti-virus software integrates itself with the operating system of a host computer and monitors programs behaviour in real time for malicious actions. The software blocks potentially malicious actions before they have a chance to affect the system.

1. Name at least two widely used antivirus softwares.

Norton, AVG, Kaspersky, Panda, Avast!, McAfee

1. What is the most common way for a virus to spread?

E-mail, Instant Messaging, File Sharing, Remote Execution Capability, Remote file access capability

1. What is the primary way by which virus scanners work?

A virus scanner works by detecting malicious signatures.

1. What other way can a virus scanner work?

Newer virus scanners (3rd and 4th gen) can identify viruses by actions and often provide access control.

1. What is a DoS attack? Give an example and explain how it works.

DoS (Denial of Service) attack is an attack that prevents or impairs authorized users of from access to a network, system, and application by exhausting the available resources. An example would be a bunch of botnet zombies accessing the same page at the same time from multiple threads in order to overwhelm a web server with a large number of requests.

1. Explain what Spyware is.

A tiny program that is often downloaded without the users consent or knowledge that can collect information about sites that were visited or log keystrokes.

1. Briefly explain the following:
   1. Trojan horse  
      An application masquerades itself as something it is not. For example: a torrent file is named after a newly released computer game. However the file is not actually a game but a virus.
   2. Buffer overflow attack  
      attempting to store more data than available in a variable causing the variable to overflow. This can lead to gaining root access permissions or modifying the values of other variables. Commonly caused by inexperienced programmers or code that has not been properly reviewed.