=============Start lecture 7 notes=========================

Q.Distinguish between a false positive and a true negative statistics in terms of virus detection capabilities of Anti-Virus software

• Anti-Virus (AV) Software is not guaranteed to detect threats → detection rates on the Zeus family of trojans can be as low as 40%

• As with other tools AV can have:

➢ True positive → actual virus detected

➢ False positive → benign file detected as virus

➢ True negative → benign file detected as benign

➢ False negative → virus missed!

Q.Describe in detail three methods implemented by anti-virus software to detect malware.

• Three important ones are: 1. Signature-based Detection 2. Malicious Activity Detection 3. Heuristic-based Detection

Q. Distinguish between signature-based, malicious activity based and Heuristic based virus detection techniques.

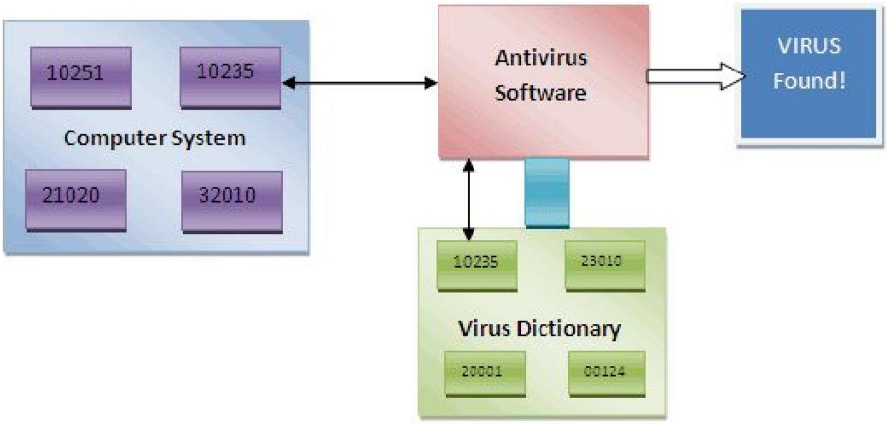
AV Signature Based Detection

Traditionally, antivirus software heavily relied upon signatures to identify malware.

■ Cannot defend against malware unless samples have already been obtained and signatures created.

■ AV scan → checks the contents of a file against a dictionary of virus signatures.

A virus signature is the viral code



AV Malicious Activity Detection

• The suspicious behavior approach does not attempt to identify known viruses, but instead monitors the behavior of all programs.

• If one program tries to write data to an executable program, for example, the antivirus software can flag this suspicious behavior, alert a user and ask what to do.

• The suspicious behavior approach provides protection against zero day viruses that are not yet in the dictionary.

• However, it can also sound a large number of false positives and users may become de-sensitized to the warnings.

AV – Heuristic Detection

Some more sophisticated antivirus software uses heuristic analysis to identify new malware or variants of known malware.

Three methods are used: ▪ File Analysis ▪ File Emulation ▪ Generic Signatures

Q.List three possible actions AV software can take if software is suspected as being malicious.

Three methods are used: ▪ File Analysis ▪ File Emulation ▪ Generic Signatures

Q. Comment on the ability of signature based detection in combating ODE (zero-day-exploits), polymorphic and metamorphic viruses.

Polymorphic and metamorphic viruses → defeat simple signature based detection

And Signature based AV can not guard the Zero-day-exploits

Q. Discuss in detail the three modes of operation of Heuristic virus detection.

File Analysis

▪ File analysis is the process by which antivirus software will analyze the instructions of a program.

▪ Based on the instructions, the software can determine whether or not the program is malicious.

▪ For example, if the file contains instructions to delete important system files, the file might be flagged as a virus.

▪ Can trigger many false positives.

File Emulation

▪ This runs the target file in a virtual system environment, separate from the real system environment.

▪ The antivirus software would then log what actions the file takes in the virtual environment.

▪ If the actions are found to be damaging or malicious, the file may be marked a virus.

Generic Signatures

■ Signature-based detection → it is possible for a user to be infected with new malware for which no signature exists yet.

■ Generic signatures → can identify new viruses or variants of existing viruses by looking for known malicious code (or slight variations of such code) in files.

■ Entire families of viruses can be protected against!

Q. In the context of virus detection what is a sandbox and where does it find use?

Sandboxing is a form of software virtualization that lets programs and processes run in its isolated virtual environment thus protecting the OS from unexpected or malicious activity.

Q. List 5 approaches that will help in eliminating virus threats.

Use real-time protection

Scan e-mail

Scan instant messenger attachments

Schedule virus scans

Use Automatic Updates

Kill Viruses

Q. What roles do firewalls play in computer security?

• Firewalls can block unauthorised programs from getting onto your PC, and also stop them from making outbound connections without your knowledge.

• A Firewall is an important layer in your Defense in Depth approach to protecting your PC.

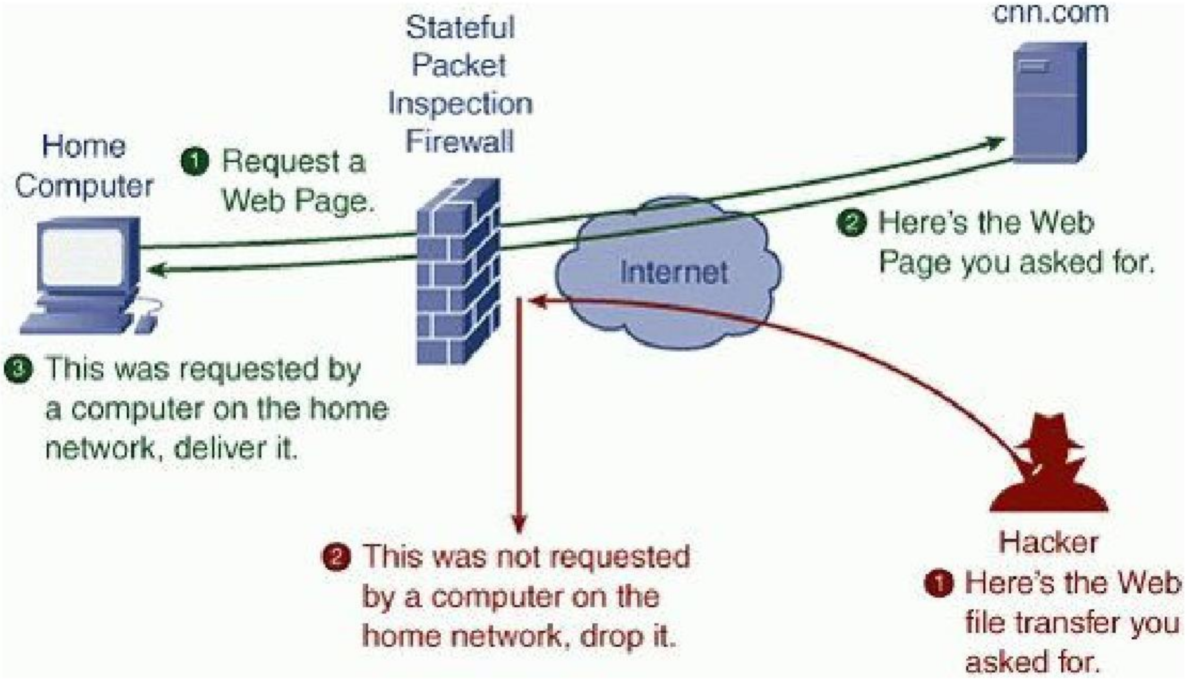
• You can also download a third party Firewall such as McAfee Personal Firewall, Norton Personal Firewall or ZoneAlarm.

• All firewalls work in a similar manner. When a program tries to access the Internet, either outbound or inbound, you receive a warning.

• If the firewall recognises the program, it tells you whether it's safe or dangerous.

• You then tell the firewall to let the program access the Internet if it is safe. • Firewalls remember your decisions for future operations if configured to do so.

Q.Draw a block diagram illustrating the operation of a personal firewall.


Stateful Packet Inspection Firewall
cnn.com
Home Computer
❶ Request a Web Page.
❷ Here's the Web Page you asked for.
Internet
❸ This was requested by a computer on the home network, deliver it.
❷ This was not requested by a computer on the home network, drop it.
Hacker
❶ Here's the Web file transfer you asked for.

Q.Name and describe the three modes of operation in firewall. Q.Distinguish between packet filter and stateful inspection modes of operation in a firewall.

• Packet filtering - a simple method, packet filtering entails analysing small packets or chunks of data through a series of filters/rules. (Susceptible to IP Spoofing)

• Proxy service - all of the data entering or leaving the network is first sent to the Proxy server. It hides the true network addresses.

• Stateful inspection - this method looks at parts of packets to see if they match specific characteristics that are allowable. It tracks all of the network connections and distinguishes which are valid packets for different types of connections.

Q.Name and describe four firewall analysis mechanism.

Firewall analysis is based on four mechanism:

1. Address, 2. Port, 3. Protocol, 4. Application.

• Address - Every computer or network gateway on the Internet has an IP (Internet Protocol) address, such as 126.1.228.4. They also have names corresponding to those addresses, known commonly as 'domain names,' like mail.yahoo.com.

• Protocol - Certain types of data conform to different communication standards or protocols. For example, the HTTP (Hyper Text Transfer Protocol)

- Port - Firewalls can block or restrict transmission based on a port or series of ports. More common ports closed off are Telnet(23) and FTP(21)

Q.What additional services can a firewall offer to clients in addition to traffic filtering?

These days Firewalls also have a wide range of additional services to offer their clients:

- Data Encryption – encrypt all data being sent.

- Pop-up Ad Blocking

- Logging/Reporting – Modern firewalls can report in detail what packets came from where, when, and provide analysis as to their purposes.

- Hiding your Presence – Some Firewalls will try to hide your presence to the outside world.

- Email Virus Protection