# Worksheet 3 Internet security Answers

**Task 1**

1. Firewalls use ports to determine if traffic using a certain protocol should be allowed through. Complete this table of commonly used network protocols and their port numbers:

|  |  |  |
| --- | --- | --- |
| **Application** | **Protocol** | **Port** |
| File transfer by browser or FTP client | FTP | 20, 21 |
| Virtual terminal text conversation | Telnet | 23 |
| Routing messages between mail servers | SMTP | 25 |
| Domain name system | DNS | 53 |
| Automatic assignment of IP addresses to network devices | BOOTP, DHCP | 67 |
| Retrieving email from a server | POP3 | 110 |
| Secure communication with web server | HTTPS (HTTP over TLS/SSL) | 443 |
| Game | Call of Duty | 28960 |

1. Open [www.t1shopper.com/tools/port-scan](http://www.t1shopper.com/tools/port-scan) in a web browser. Click on the Check All link and then the Scan Ports button. The website will check which of the listed ports in your LAN’s firewall is open to incoming traffic.

List any open ports below and state why they might be open:

|  |  |  |
| --- | --- | --- |
| **Port** | **Use** | **Reason it is open** |
| *80* | *HTTP* | *School hosts a website* |
|  |  |  |
|  |  |  |
|  |  |  |

If none of these ports are open to incoming traffic, why do you think that might be?

On a mobile (cellular) network, the network operator (carrier) blocks incoming traffic through all ports by default;

On a home LAN, the gateway may have a firewall that blocks incoming traffic through all ports by default.

**Task 2**

Select the most appropriate security methods for the given scenarios, explaining the technical reasons for your choices:

|  |  |  |
| --- | --- | --- |
| **Scenario** | **Most appropriate security method(s)** | **Reason** |
| The recipient of an email needs to check that the message contents are unaltered and verify the identity of the sender. | Digital signatureDigital certificate | Recipient’s hash of message matching that encrypted in the digital signature verifies the integrity of the message’s content.Digital certificate sent with encrypted message verifies the identity of the owner of the public key contained in the certificate, who digitally signed the message.CA’s digital signature contained in the certificate verifies certificate’s origin and integrity. |
| A stock market and a broker exchange financial information securely. Data need to be processed very quickly. | Symmetric encryption | This method reduces the encryption and decryption time. Need to pre-share the key securely. |
| Transactions between an eCommerce website and its customers need to be protected.  | Digital certificateHTTPS protocol | Digital certificate verifies the identity of the owner of the website’s public key.CA’s digital signature contained in the certificate verifies certificate’s origin and integrity.HTTPS applies encryption using the website’s public key contained in its certificate. |
| A number of accountants are exchanging financial details about a company. They need to ensure the data is protected but do not work for the same company and have never met. | Asymmetric encryption | The public keys of the accountants can be used to encrypt the data. These keys are available to all (on request) so the system does not require them to have previously shared a key. |

**Task 3**

You are responsible for the network security of a small company with one office. All employees use their own devices in the office.

The owner wants to make new employees aware of the best practices for preventing the intrusion of malicious software into the network.

Write an overview that can be used to educate these new employees. You should explicitly mention:

* Preventing viruses
* Preventing worms

Key points:

* Ensure anti-virus software is installed
* Make sure it is regularly updated
* Regularly update your operating system
* Do not open email attachments that you are not expecting
* Do not click on links in emails that seem suspicious
* Ensure passwords are difficult to guess
* Make sure you have a firewall installed
* Only enable the minimal amount of network access required to complete your work