Tutorial 3 Solutions

Answer 1.

a. If the size of the file is not given then the transfer time = 5Mbps. And if the size of the file given it is 200Bytes/5Mbps.

b. 200Bytes/100bps.

Answer 2.

a. 10 users can be supported because each user requires one tenth of the bandwidth.

b. We know that each user transmits only 10 percent of the time, so for a given user the probability will be: p = 10/100= 0.1

c.

Answer 3.

Network security refers to any activities designed to protect your network. Specifically, these activities protect the usability, reliability, integrity, and safety of your network and data. Effective network security targets a variety of threats and stops them from entering or spreading on your network.

Answer 4.

Network Security Services (NSS) comprises a set of libraries designed to support cross-platform development of security-enabled client and server applications with optional support for hardware TLS/SSL acceleration on the server side and hardware smart cards on the client side. NSS provides a complete open-source implementation of cryptographic libraries supporting Transport Layer Security (TLS) / Secure Sockets Layer (SSL) and S/MIME. Previously tri-licensed under the Mozilla Public License 1.1, the GNU General Public License, and the GNU Lesser General Public License, NSS upgraded to GPL-compatible MPL 2.0 with release 3.14.

Answer 5.



Answer 6.

DDoS stands for “Distributed Denial of Service.” A DDoS attack is a malicious attempt to make an online service unavailable to users, usually by temporarily interrupting or suspending the services of its hosting server.

DDoS attacks can be broadly divided into three types:

1. Volume Based Attacks: Includes UDP floods, ICMP floods, and other spoofed-packet floods. The attack’s goal is to saturate the bandwidth of the attacked site, and magnitude is measured in bits per second (Bps).

2. Protocol Attacks: Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and is measured in Packets per second.

3. Application Layer Attacks: Includes low-and-slow attacks, GET/POST floods, attacks that target Apache, Windows or OpenBSD vulnerabilities and more. Comprised of seemingly legitimate and innocent requests, the goal of these attacks is to crash the web server, and the magnitude is measured in Requests per second.

Answer 7.

The most common blunder people make when the topic of a computer virus arises is to refer to a worm or Trojan horse as a virus. The phrases are used interchangeably, but they are not the same thing.

One common mistake that people make when the topic of a computer virus arises is to refer to a [worm](http://www.webopedia.com/TERM/W/worm.html) or [Trojan horse](http://www.webopedia.com/TERM/T/Trojan_horse.html) as a [virus](http://www.webopedia.com/TERM/V/virus.html). While the words Trojan, worm and virus are often used interchangeably, they are not exactly the same thing. Viruses, worms and Trojan Horses are all malicious [programs](http://www.webopedia.com/TERM/P/program.html) that can cause damage to your [computer](http://www.webopedia.com/TERM/C/computer.html), but there are differences among the three, and knowing those differences can help you better protect your computer from damaging effects.

What Is a Computer Virus?

A [computer](http://www.webopedia.com/TERM/C/computer.html) virus attaches itself to a [program](http://www.webopedia.com/TERM/P/program.html) or [file](http://www.webopedia.com/TERM/F/file.html) enabling it to spread from one computer to another, leaving infections as it travels. Like a human virus, a computer virus can range in severity: some may cause only mildly annoying effects while others can damage your [hardware](http://www.webopedia.com/TERM/H/hardware.html), [software](http://www.webopedia.com/TERM/S/software.html) or [files](http://www.webopedia.com/TERM/F/file.html). Almost all viruses are attached to an executable, which means the virus may exist on your computer but it actually cannot infect your computer unless you run or open the malicious program.

It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going. Because a virus is spread by human action people will unknowingly continue the spread of a computer virus by sharing infecting files or sending [emails](http://www.webopedia.com/TERM/E/e_mail.html) with viruses as [attachments](http://www.webopedia.com/TERM/A/attachment.html) in the email.

Fast Facts: Attaches to an executable file, requires human action to spread.

What Is a Worm?

A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action. A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.

The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book, and the manifest continues on down the line.

Due to the copying nature of a worm and its capability to travel across networks the end result in most cases is that the worm consumes too much [system memory](http://www.webopedia.com/TERM/S/system.html) (or [network](http://www.webopedia.com/TERM/N/network.html) bandwidth), causing Web [servers](http://www.webopedia.com/TERM/S/server.html), network servers and individual computers to stop responding. In recent worm attacks such as the much-talked-about Blaster Worm, the worm has been designed to tunnel into your system and allow malicious users to control your computer remotely.

Fast Facts: Can replicate itself on system, does not require human action to spread.

What Is a Trojan horse?

A Trojan Horse is full of as much trickery as the mythological Trojan Horse it was named after. The Trojan Horse, at first glance will appear to be useful [software](http://www.webopedia.com/TERM/S/software.html) but will actually do damage once installed or run on your computer.  Those on the receiving end of a Trojan Horse are usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source.

When a Trojan is activated on your computer, the results can vary. Some Trojans are designed to be more annoying than malicious (like changing your [desktop](http://www.webopedia.com/TERM/D/desktop.html), adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on your system. Trojans are also known to create a back door on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

Fast Facts: Appears useful but damages system, requires human action to run, do not self-replicate.

Answer 8.

Criminals have long employed the tactic of masking their true identity, from disguises to aliases to caller-id blocking. It should come as no surprise then, that criminals who conduct their nefarious activities on networks and computers should employ such techniques. IP spoofing is one of the most common forms of on-line camouflage. In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by “spoofing” the IP address of that machine. In this article, we will examine the concepts of IP spoofing: why it is possible, how it works, what it is used for and how to defend against it.

History

The concept of IP spoofing was initially discussed in academic circles in the 1980's. While known about for sometime, it was primarily theoretical until Robert Morris, whose son wrote the first Internet Worm, discovered a security weakness in the TCP protocol known as sequence prediction. Stephen Bellovin discussed the problem in-depth in Security Problems in the TCP/IP Protocol Suite, a paper that addressed design problems with the TCP/IP protocol suite. Another infamous attack, Kevin Mitnick's Christmas Day crack of Tsutomu Shimomura's machine, employed the IP spoofing and TCP sequence prediction techniques. While the popularity of such cracks has decreased due to the demise of the services they exploited, spoofing can still be used and needs to be addressed by all security administrators.

Answer 9.

This example illustrates how a botnet is created and used for malicious gain

1. A hacker purchases or builds a Trojan and/or exploit kit and uses it to start infecting users' computers, whose payload is a malicious application—the *bot*.
2. The *bot* on the infected PC logs into a particular command-and-control (C&C) server. (This allows the bot master to keep logs of how many bots are active and online.)
3. The bot master may then use the bots to gather keystrokes or use form grabbing to steal online credentials and may rent out the botnet as DDoS and/or spam as a service or sell the credentials online for a profit.
4. Depending on the quality and capability of the bots the value is increased or decreased.

Answer 10.

* [Cleartext](http://en.wikipedia.org/wiki/Cleartext)  is readable data transmitted or stored “*in the clear*” (i.e. unencrypted)
* [Plaintext](http://en.wikipedia.org/wiki/Plaintext) is the input to an encryption algorithm
* [Ciphertext](http://en.wikipedia.org/wiki/Ciphertext) is the unreadable output of an encryption algorithm
* [Plaintext](http://en.wikipedia.org/wiki/Plain_text) means its text that hasn’t been formatted (i.e., a plain text file)
* And clear text… well, this is just text that is easy to comprehend (added to be thorough)

* Something that is cleartext may be in plain text, could be used as plaintext, but definitely isn’t cipher text.
* Something that is plaintext should be in plain text, could be clear text, and will become ciphertext.
* Something that is ciphertext should be in plain text, could be used as plaintext, but definitely isn’t clear text.

To non-security folks, this makes about as much sense as “*key encryption keys”* and “*ticket granting tickets”*(They’re real, look them up!), but the distinction comes down to when you are describing the text in question.  Let’s use the scenario of storing credentials in a database, which is where I came across during our security reports.

If you store a password in a database, you would store it as either cleartext or ciphertext, usually in plain text, meaning the password is either encrypted or unencrypted, usually without formatting. Since while just sitting in a database it isn’t an input to an encryption algorithm, it is not plaintext.

Now you can correctly say something like “The clear text password was queried from the database and used as plain text by the encryption method to produce cipher text, protecting our proprietary clear text formula.”

One last important distinction to understand is that plaintext is not necessarily readable, as you could take the ciphertext from one algorithm, feed it to another (i.e., plaintext), and produce more ciphertext.

Answer 11.

Trudy can pretend to be Bob to Alice (and vice‐versa) and partially or completely modify the message(s) being sent from Bob to Alice. For example, she can easily change the phrase “Alice, I owe you $1000” to “Alice, I owe you $10,000”. Furthermore, Trudy can even drop the packets that are being sent by Bob to Alice (and vise‐versa), even if the packets from Bob to Alice are encrypted.

Answer 12.

A nonce is an arbitrary number used only once in a cryptographic communication, in the spirit of a nonce word. They are often random or pseudo-random numbers. Many nonces also include a timestamp to ensure exact timeliness, though this requires clock synchronization between organizations. The addition of a client nonce ("cnonce") helps to improve the security in some ways as implemented in digest access authentication. To ensure that a nonce is used only once, it should be time-variant (including a suitably fine-grained timestamp in its value), or generated with enough random bits to ensure a probabilistically insignificant chance of repeating a previously generated value. Some authors define pseudo-randomness (or unpredictability) as a requirement for a nonce.