







# Chapter 12 - Key Terms

 Term	 Page	 Description
<u>Tor</u>	588	A free tool that enables its users to surf the web anonymously. Tor works by “routing” IP traffic through a free, worldwide network consisting of thousands of Tor relays. It then constantly changes the way it routes traffic to obscure a user’s location from anyone monitoring the network. Tor’s name was created from the acronym for the original software project name, “The Onion Router.”
<u>Tor exit node</u>	588	Basically the last Tor node or the “gateway” where the Tor-encrypted traffic “exits” to the Internet.
<u>peer-to-peer (P2P communication).</u>	586	The distributed architecture that “divides tasks” between participant computing peers. In a P2P network, the peers are equally privileged, which is why it’s called a peer-to-peer network of nodes.
<u>Virtual Private Network (VPN).</u>	589	A type of network used to hide or encode something so that the content is protected from unwanted parties.
<u>remote-access VPN</u>	586	A virtual private network that connects a remote host to a trusted network.
<u>traffic timing attack</u>	589	An attack in which the attacker performs actions more slowly than normal while not exceeding thresholds inside the time windows the detection signatures use to correlate different packets together.
<u>clientless VPN</u>	579	A type of virtual private network that provides remote access services without requiring a host client. Typically, this is based on providing access to a secure network the segment also known as a sandbox.
<u>Secure Shell (SSH).</u>	587	A protocol that encrypts traffic between a client and SSH server and uses public-key cryptography to authenticate the remote computer and permit it to authenticate the user.
<u>resource exhaustion attack</u>	586	An attack that consumes the resources necessary to perform an action.

 Term	 Page	 Description
<u>traffic fragmentation attack</u>	588	A method of avoiding detection by breaking up a single Internet Protocol or IP datagram into multiple smaller-size packets.
<u>protocol misinterpretation attack</u>	586	An attack where protocols are manipulated to confuse security devices from properly evaluating traffic.
<u>traffic substitution &amp; insertion attack</u>	589	A method of substituting the payload data with data in a different format but with the same meaning, with the goal of being ignored due to not being recognized by the security device.
<u>pivoting</u>	586	Attacking other systems on the same network. Also known as island hopping.
<u>site-to-site VPN</u>	587	A virtual private network that connects one or more hosts over a secure connection.