Chapter 12 - Key Topics

Description	Element	Page	Summary
Understanding the challenges that encryption introduces to security monitoring	Paragraph	500	Threat actors can use encryption for obfuscation and evasion. Historically, even governments have tried to regulate the use and exportation of encryption technologies. A good example is the Wassenaar Arrangement, which is a multinational agreement with the goal of regulating the export of technologies like encryption.
Understanding the challenges that NAT introduces to security monitoring	Paragraph	501	NAT can present a challenge when you're performing security monitoring and analyzing logs, NetFlow, and other data, because device IP addresses can be seen in the logs as the "translated" IP address versus the "real" IP address. In the case of Port Address Translation (PAT), this could become even more problematic because many different hosts can be translated to a single address, making the correlation almost impossible to achieve.

Description	Element	Page	Summary
Security Monitoring & Tor	Section	504	The use of Tor also makes security monitoring and incident response more difficult because it's hard to attribute and trace back the traffic to the user. Different types of malware are known to use Tor to cover their tracks. This "onion routing" is accomplished by encrypting the application layer of a communication protocol stack that's nested just like the layers of an onion. The Tor client encrypts the data multiple times and sends it through a network or circuit that includes randomly selected Tor relays. Each of the relays decrypts a layer of the onion to reveal only the next relay so that the remaining encrypted data can be routed on to it. A Tor exit node is basically the last Tor node or the gateway where the Tor encrypted traffic exits to the Internet.
Understanding the challenges that peer-to-peer communication introduces to security monitoring	Summary	505	Peer-to-peer (P2P) communication involves a 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. P2P participant computers or nodes reserve a chunk of their resources (such as CPU, memory, disk storage, and network bandwidth) so that other peers or participants can access those resources. This is all done without the need of a centralized server. From a security perspective, P2P systems introduce unique challenges. Malware has used P2P networks to communicate and also spread to victims. Many "free" or stolen music and movie files usually come with the surprise of malware.

Description	Element	Page	Summary
Key encryption & tunneling concepts	List	508	A VPN is used to hide or encode something so the content is protected from unwanted parties. Encryption traffic can be used to bypass detection, such as by an intrusion prevention system (IPS). The two forms of remote-access VPNs are client based & clientless. A site-to-site VPN connects two or more networks. SSH connects a host to an SSH server & uses public-key cryptography to authenticate the remote computer to permit it to authenticate the user. File encryption technology protects files from unauthorized users.
Key resource exhaustion concepts	List	509	Resource exhaustion refers to consuming the resources necessary to perform an action. Attackers use resource exhaustion to bypass access control & security detection capabilities. A common example is sending a ton of traffic to an IPS. Resource exhaustion can be used to render logging unusable. Throttling is a method to prevent resource exhaustion by limiting the number of processes that can be used at one time.
Key traffic fragmentation concepts	List	510	Traffic fragmentation attacks modify the TCP/IP traffic in a way that is unexpected by security detection devices; the goal is to consume the detection functions. Using TCP segmentation and reordering attacks is one way to modify traffic to bypass detection. Causing fragments to overlap by modifying IP headers is another type of traffic fragmentation attack. Proxies & inline security devices can help prevent traffic fragmentation attacks.

Description	Element	Page	Summary
Key protocol misinterpretation concepts	List	511	Protocols can be manipulated to confuse security devices from properly evaluating traffic. TCP checksum & time-to-live protocols can be manipulated to first look like one thing & later to look like something else, with the goal of tricking the security defenses.
Understanding traffic substitution and insertion concepts	List	512	Traffic timing attacks occur when the attacker evades detection by performing his or her actions more slowly than normal while not exceeding thresholds inside the time windows the detection signatures use to correlate different packets together. A traffic substitution and insertion attack substitutes the payload with data that is in a different format but has the same meaning. Some methods to accomplish a traffic substitution and insertion attack include exchanging spaces with tabs, using Unicode instead of ASCII, and abusing case sensitive communication. Security products can stop this type of attack by being able to adapt to format changes, properly processing extended characters, and providing Unicode de-obfuscation.

Description	Element	Page	Summary
Understanding pivoting (lateral movement)	List	516	**Pivoting** - Pivoting in terms of cyber attacks (also known as island hopping) means to attack other systems on the same network with the goal of gaining accessing to that system. Best practice is to have networks segmented and to control access between each segment. A common goal for a pivot attack is to escalate the attacker’s privileges. This is commonly accomplished by jumping from one system to another system with greater network privileges. Defending against pivoting can be accomplished by providing proper access control, network segmentation, DNS security, reputation security, and proper patch management. NetFlow is a great sensor-based tool for detecting unauthorized pivoting occurring within the network.
Untitled			