Osi and security layers

Reginald Monroe-@02516632 Summary of OSI layers & Security OSI stands for Open Systems Interconnection and it was developed by the Europeans in the 1980’s. OSI is divided into two major fields, an abstract model of networking and a set of defined protocols. The seven layers of the OSI basic reference model are listed and defined below (from bottom to top): 1. The Physical Layer — this layer describes the physical components of the various communications media, it also includes the electrical properties and interpretation of the signals exchanged. Many security breaches can be found at the physical layer, and they deal with the physical security attributes. This could be done a number of ways: * Disrupting a power source. * Changing of interface pins * The cutting of cables * Tampering with a fuse box connected to your network 2. The Data Link Layer — this layer describes a logical organization of data bits transferred through a chosen medium. The data link layer can be breached in several ways, mainly by altering the MAC information, better known as ARP Cache Poisoning. This can be prevented first at the physical layer, and is rarely done in less someone is on the same network as the poisoner. 3. The Network Layer — this layer describes how a series of different data links can transfer data between any two nodes in a network. This is commonly attacked by those users outside of the network, by use of routers. Routers running older software versions are relatively more prone to attack. Password buffer overflow is one of the most common ways to intrusion. 4. The Transport Layer- this describes the quality and nature of the delivery of the data. The transport layer can be breached in many ways. One of the most common way that the transport layer can be breached is port scanning as well as a “ half-open" scan. This is the way attackers gather information about open ports on your system. Most

attackers use NMAP because only an internet connection is needed to begin malicious activities. 5. The Session Layer- this describes data organization sequences that are larger than the packets handled by the lower layers. Most hijacking on the session layer at the start of a TCP session, since most authentication only occurs at the start of TCP, it allows the hacker to gain access to the machine. Proper authentication is the first and most important weapon in the line of defense. 6. The Presentation Layer- this describes the syntax of data being transferred. What makes the presentation layer more succeptible to attack is Unicode vulnerabilities. Protecting against Unicode vulnerabilities is often as simple as applying a recommended patch from a vender. 7. The Application Layer — this describes how real work actually gets done. The most well know and the most vulnerable part of security is done at the application layer with Trojan horse and viruses. Our computer can be best protected by use of antivirus and only downloading trusted applications.