Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Understanding Security Using the OSI Model

This paper is written as a guide for those who do not labor through the wee hours of the morning (yet) studying every new Information Technology (IT) vulnerability. This paper will provide a breakdown of the OSI (Open Source Interconnection) model, and using that model, explain some well-known vulnerabilities. The paper will take each layer of the OSI model (there are seven) and describe a relevant vulnerability with a solution to that problem area. The reader will become more aware of the vulnerabilities that exist in...

Copyright SANS Institute
Author Retains Full Rights

AD

Understanding security using the OSI model.

Author: Glenn Surman
Assignment Version: GSEC Practical Version 1.3
Date: 20 Mar. 2002.

1. Abstract

1.1 This paper is written as a guide for those who do not labour through the wee hours of the morning (yet) studying every new Information Technology (IT) vulnerability. This paper will provide a breakdown of the OSI (Open Source Interconnection) model, and using that model, explain some well-known vulnerabilities. The paper will take each layer of the OSI model (there are seven) and describe a relevant vulnerability with a solution to that problem area. The reader will become more aware of the vulnerabilities that exist in the IT environment. More importantly, the reader will be able to use the OSI model as a guide to simplify the security process.

2. Introduction

2.1 Having an Internet connection at home is becoming as popular as having a Playstation, or a bicycle. In some cases not everyone on the end of that Internet connection is playing nice. That 'Internet connection' is all it takes to exploit a well-known vulnerability and a computer doesn't check for a user's intent when logging them on. The potential attackers' demographic is only limited by basic education and intent. Attackers could very well be school children or aged people with an interest in the area. The audience for malicious use of IT related resources is huge. It is comforting to know that there are many people fighting the battle against attackers and information on how to protect systems is readily available. Good network administrators need to be security conscious in order to protect their organisation's IT assets.

2.2 The task of securing a personal computer can be daunting to the uninitiated, let alone the task of securing a network. IT system administrators need somewhere to start, and that starting point should be understanding the OSI model. The OSI model breaks the network into easily understood components that can be secured individually. Once each component has been secured a cohesive security plan will have been achieved and the risk of attack will be significantly reduced. Firstly though we need to understand the OSI model.

3. What is the OSI model?

3.1 "Short for **O**pen **S**ystem **I**nterconnection, an ISO standard for worldwide communications that defines a networking framework for implementing protocols in seven layers."[1] The parts worth noting here are that the model is an ISO standard that affects the way the IT industry should design computer networking protocols. Some people like to think of protocols as languages and these languages make communications with similar devices possible. If everyone is playing to the same set of rules then it is much easier to make the jigsaw fit together. The OSI model is compartmentalised into

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

seven areas. This makes understanding the communications process easier. So easy in fact that the OSI model is taught in many schools. The problem being that just this knowledge is not always used for the best intentions.

3.2 "Control is passed from one layer to the next. Starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy."[2] What this means is that starting at the top layer information is passed to the lower layer until it reaches the bottom. Once the information reaches the bottom, which just happens to be the physical medium, the information makes its way to the destination. When the information reaches the destination it travels up each layer until it reaches the appropriate level for translation. An e-mail for example, starts at the Application layer or the source and makes its way down the stack, across the wire, up the stack to the destination's Application layer. The Application Layer will be covered soon. For now concentrate on the last part of the reference. Within the source computer control is passed from one layer to the next. Data travels down the source computer's hierarchy and then up the destination computer's hierarchy. Figure 1 illustrates this flow of information, notice there is no way of skipping a layer, and that the process is a mirror with the next computer.

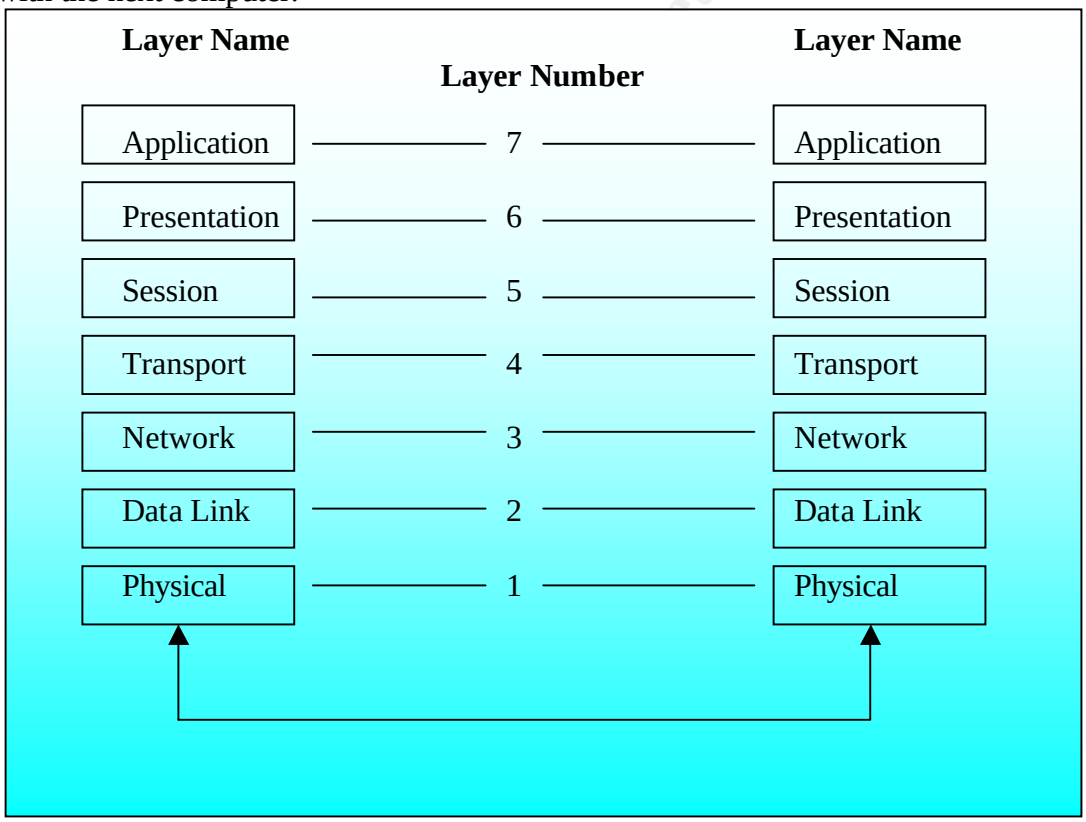

Figure 1 – The OSI Model Illustrated.

3.3 Other OSI model points to note are:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

3.3.1 Each layer can communicate with only the layer above and below it. Looking at Figure 1 it becomes clear that the Physical Layer can communicate with the Data Link layer and the medium itself (notice there is no lower layer for Physical).

3.3.2 Each layer is developed independently. This allows flexibility and allows development in one layer to progress without delays from other layers.

3.3.3 As information passes through each layer relevant information to that layer is attached – this process is commonly known as encapsulation.[3] This encapsulation is how each layer can communicate with its relevant layer at the destination.

3.4 From this overview of the OSI model you should have a basic understanding of the OSI model. It is worth noting that there are independent layers working cohesively (1 through 7 inclusive). The next section covered will look at the first layer of the OSI model.

4. The Physical Layer

4.1 David W. Baker describes in his book *Communications and Networking* that the Physical Layer "[d]efines the physical properties of the network, such as voltage levels, cable types, and interface pins."[4] Exploiting the Physical Layer could suggest some type of physical action, like disrupting a power source, changing of interface pins, or the cutting of cables. Simply tampering with someone's fuse box outside their office can cause a disruption of service. Faulty power is a problem that can be caused accidentally by the power company, or intentionally by your competitor tampering with the fuse box. By installing an Uninterrupted Power Supply (UPS) to your system you can avoid many unrecoverable power associated problems. Add an UPS to your critical system and when power is interrupted your UPS will give you time to perform an orderly shutdown. This is important because abrupt termination of power to any electrical equipment has potential for damage. With regards to your competitor tampering with your fuse box, a lock may deter them.

4.3. A less obvious physical component of networking is Wireless Ethernet. IEEE 802.11 (IEEE standards can be found at http://www.ieee.org) explains the standards for Wireless Ethernet. Replacing wire with radio waves transporting electrical impulses wireless technologies use frequencies and Wireless Ethernet uses 2.4 GHz (Giga Hertz).[5] As Doug Jackson mentions in his paper *AirUTD: Wireless at UT Dallas* this band is the same as used by microwave ovens.[6] If binary is transmitted over a 2.4GHz band, and a leaky microwave oven is also sending 2.4GHz patterns, it is not hard to guess that there is a chance of signal disruption. Any old leaky ovens can cause real wireless problems, and in the worst case scenario – a Denial of Service (DoS).

4.4 Consider a Wireless Ethernet Hub located next to a wall in an office block. The encryption used on the network is guaranteed by the vendor to prevent your information

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

reaching your rivals who are situated in the offices next to yours. The only thing separating you and your competitor is a layer of brick and plaster. Your rival is interested in making your life hard. He/she simply buys a Microwave Omission Analyser for AUS$24.96 (Dick Smith Electronics – http://www.dse.com.au) and searches around garage sales, trash and treasure stores, until a suitably leaky device is found. Once the device is next to your office, plugged in and turned on, all sorts of problems can occur with your network signal, and the source can be hard to detect.

4.5. A possible solution is prevention by design. Walk around with a Microwave Omission Analyser when designing your Wireless network, or at least employ a person who is aware of these problems and take will take your environment into account.

5. The Data Link Layer

5.1 David W. Baker explains the second OSI layer, the Data Link Layer, as the layer that "[t]ransmits and receives packets of information reliably across a uniform physical network."[7] The vulnerabilities with the design of the Data Link Layer exist because the layer was designed to be functional and practical. One can imagine the last thing in the minds of the designers was that someone would one day exploit this technology. In today's security climate it would make sense to have exploits as a consideration, but in the early 80's it was not as big a problem.

5.2 RFC 826 first discussed a protocol called ARP.[8] ARP stands for Address Resolutions Protocol. Now that isn't going to mean a lot until you think, "What is it that we are trying to address?" Network Interface Cards (NIC) exist to give computers the ability to talk to each other. To do this they need to be able to find each other. In order to do this they are assigned a single unique address – known as a MAC Address. Media Access Control (MAC) Addresses are used by ARP. ARP is a protocol that allows a source computer to ask other computers if they know the MAC address of the machine it wants to speak with. Hopefully the destination machine will reply, and say something along the lines of "I know who you are after – that's me!" Of course if no one knows who the source is asking after then the information is sent to a device like a router. [9] So now we see that computers talk to each other, and they use NICs to do this and the way the NICs can find each other is via ARP.

5.3 "ARP converts an IP address to its corresponding physical network address".[10] It needs to be mentioned, in case of terminology confusion, that the physical network address is understood as the MAC Address. Now there is one more item mentioned in the definition and that is IP address. This will be covered in more detail in the next segment (Network Layer).

5.4 The function of ARP, as mentioned by Bob Fleck and Jordan Dimov in *Wireless Access Points and ARP Poisoning*, is:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

… the mapping between IP addresses and MAC hardware addresses on local networks. For example, a host that wants to send a message to IP address 10.0.0.2 on the local network sends a broadcast ARP packet that requests the MAC for that IP. The host that owns the IP 10.0.0.2 returns an ARP reply packet with its MAC address. The requesting host then sends the message, and stores the IP-to-MAC mapping for future packets. [11]

5.4.1 IP (Internet Protocol) Addresses are four octet numbers (octet1.octet2.octet3.octet4) that allow logical addressing. Each number is between 0 and 255 inclusive.[12] For example a computer on a network may have an IP address of 10.17.13.5 and the computer next to it may have an address of 10.17.13.6. Devices like routers make information forwarding decisions using IP addresses. Why send information to Network Z when the destination is on Network A? A router wouldn't send the information to Network Z instead it would forward the information to Network A. This reduces the amount of unnecessary traffic you have on your network.

5.5 The IP-to-MAC addressing relies on receiving valid MAC information. MAC addressing information resides on OSI model Layer 2. By altering this MAC information you are effectively exploiting the Data Link Layer. This is known as ARP Cache Poisoning.[13]

5.6 ARP Cache Poisoning works like this:

5.6.1 Computer A wants to communicate with Computer Z. To make this illustration easier to understand we will assume both computers are on the same local network.

5.6.2 Computer A has the IP address of Computer Z, but needs to know the MAC address of Computer Z so that the NICs can talk (remember NICs don't really understand IP addressing). Computer A searches through its ARP Cache (a file used to store IP to MAC addressing) and finds that it does not know the MAC Address for Computer Z.

5.6.3 Computer A broadcasts the network asking for the MAC Address of Computer Z. Only Computer Z will reply. This is how computers find each other when they are on the same network segment.

5.6.4 Attackers alter the ARP Cache so that computers associate the wrong MAC Address with the IP. Computer A looks up its ARP Cache to see if it knows what computer belongs to a particular IP address (Computer Z). Computer A has a poisoned ARP Cache so it mistakenly sends the information for Computer Z to the attacker's machine. The attacker's machine then sends the information on to Computer Z and no one is the wiser.[14]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

5.7 Protecting against ARP Cache Poisoning begins with physical security. The attacker normally needs to be on the same physical network for ARP poisoning to be activated in this sense. ARP does not cross router boundaries so it is generally harder for an attacker to activate this attack from outside of your network (dependant on your network infrastructure). The first step to proper physical security is to make sure your staff knows who is sitting next to them, and give them the authority and responsibility of challenging strangers. Organisations can enforce this type of policy and advise their staff to simply approach unknown people in the office with "Hello can I help you?"

5.8 Once your organisation has a solid policy for physical security it would be beneficial to prepare for a break down in that policy. System Administrators should always be asking "What will happen to the network if that policy is not adhered to, and what can I do to minimise the impact of that intrusion?" In the paper *Protecting against the unknown* Mixter Technologies write "…use of static ARP cache entries, especially on routers and switches is recommended, to prevent malicious packet redirection to arbitrary hosts."[15] By making administration of ARP cache entries a manual process an attacker would not be able to take advantage of the ARP vulnerability. If you have a small network then this is a viable option to dynamic ARP cache entries. Take away dynamic ARP cache entering and you increase your overheads. You would need to assess this risk against the risk to your physical security all the while considering the administrative overhead. You could start by statically assigning ARP entries for a small component of your network and assess the overhead in isolation. A quick calculation will tell you if your network is too large for you to administer ARP entries manually.

6. The Network Layer

6.1 It is feasible that in the future you could get into your car, tell it where you wish to go, and drink coffee while it takes you there. The fundamentals of how the car gets you to your destination are basically what the Network Layer offers us today with computer interconnectivity.

6.2 David W. Baker defines the Network Layer as the layer that "[r]outes data through various physical networks while traveling [sic] to a known host."[16] Keeping the flying-car example in mind, the various physical networks would be the paths over the trees, through the tunnel. The 'to a known host' component would be that your car understands what you mean when you say "Work please car".

6.3 The most important part of understanding Layer 3 – Network Layer principles is knowing that routers make decisions based on Layer 3 information. Routers are machines that decide how to send information from one logical network to another. Routers understand the Internet Protocol (IP) and base routing decisions on that information.[17]

6.4 So from the information you have so far we should be able to determine a process. ARP matches a MAC Address to an IP address, and Routers make forwarding decisions based on IP addresses. If an attacker wants to cause problems when they are physically

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

located within the network then they can ARP cache poison, but what if they are outside of the network? They can use routers.

6.5 Routers running older software versions can be relatively easy to attack. One hacker in particular mentions that to hack into a CISCO router you just need a bit of patience and practice.[18] The author mentions that CISCO routers running v4.1 can be easily disabled by simply connecting to port 23 via the proxy server.[19] The attacker will only use the proxy server because that makes tracking them harder. Once asked for a password the attacker simply enters in a large password string, which in the example is about 350 characters of senseless text. There is a chance that the router will reboot, and that is not good for the attacker because they can not attack a machine that is off. If the machine pauses, rather than rebooting, then the vulnerability has surfaced. While the router is working out what this huge password is the attacker can open another session using telnet, through another proxy server, and connect to the paused router using the password 'admin'. The author comments "… the reason for this is because by default, this is the router's password, and while it is temporarily disabled, it will revert to it's [sic] default state."

6.6 To their credit CISCO normally provides quick and accurate solutions to vulnerabilities with their systems. With regard to the vulnerability in para 6.5, CISCO addressed this with:

> **Software Fixes**
>
> A software fix was integrated in IOS/700 version 4.1(2.1). The first regular production release containing this fix was 4.2(1). Cisco will be making the fixed software available to all IOS/700 customers who are presently running 4.1 software, regardless of contract status. Customers under contract may obtain the software through their regular upgrade channels. Customers not under contract should contact the Cisco TAC and reference the URL of this document.
>
> **Workaround**
>
> The vulnerability may be avoided by controlling access to the system console port, and by restricting access to the TELNET facility to trusted hosts.[20]

6.7 The CISCO router password buffer problem illustrates that you should spend some time ensuring that protective measures are employed. Also, you need to minimise access to your hosts. In this case you can update your software to prevent the password buffer overflow. Where possible you need to identify your 'trusted' agents and only give them access via a vulnerable process, in this case TELNET. [21]

6.8 TELNET and passwords are not layer three topics however the objective of this segment was to explain how easy it can be to attack a layer three device – a CISCO router. Even though CISCO release patches to correct vulnerabilities, they may still exist. A business starting out may use this type of router and have not implemented the new

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

software. Responsible network administrators should spend some time reading about vulnerabilities to their equipment and then applying the patches.

7. The Transport Layer

7.1 A definition for the Transport Layer is:

> In the Open Systems Interconnection (OSI) communications model, the Transport layer ensures the reliable arrival of messages and provides error checking mechanisms and data flow controls. The Transport layer provides services for both "connection-mode" transmissions and for "connectionless-mode" transmissions.[22]

7.2 One way the Transport Layer ensures that there is reliability and error checking is through the Transport Control Protocol (TCP). You may have heard of TCP/IP, this is the TCP protocol working over the Internet Protocol (IP). Another protocol used at Layer 4 is UDP (User Datagram Protocol). TCP and UDP are individually described as:

7.2.1 TCP, written in 1980 within RFC 761 by Information Sciences Institute University of Southern California. TCP was originally produced for the United States Department of Defence. The original document found in the reference above describes TCP as: "The Transmission Control Protocol (TCP) is intended for use as a highly reliable host-to-host protocol between hosts in packet-switched computer communication networks, and especially in interconnected systems of such networks."[23] Highly reliable host-to-host communications would be file transfers, where loss of data would be unacceptable.

7.2.2 "UDP (User Datagram Protocol) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol)." [24] The type of information that can be transmitted using UDP where reliability is not as important as file transfers would be video streaming. If a single packet was lost during a video streaming session then that packet probably would not be critical to the stream. In this case accuracy is traded for speed.

7.3 TCP was designed to get data from one place to another, and once there, ensure it is in good order. UDP was never designed to be that sure about itself. It offers only a limited amount of service, as the above reference states. You can see that both protocols were intended to help organisations share data they just have different levels of reliability and speed.

7.4 No surprise that not everyone uses TCP and UDP the way the original designers planned. An attacker will gather information about a system using TCP and UDP. The ways in which TCP and UDP are used to infiltrate, deny services, or scan networks are too varied and many for the scope of this paper. We will concentrate on TCP

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

fundamentals. In light of that you will need to know a little about the TCP Process. Laura Chappell details in her paper *Inside the TCP Handshake* "The handshake process is based on three steps."[25] Figure 2 illustrates the TCP handshake:

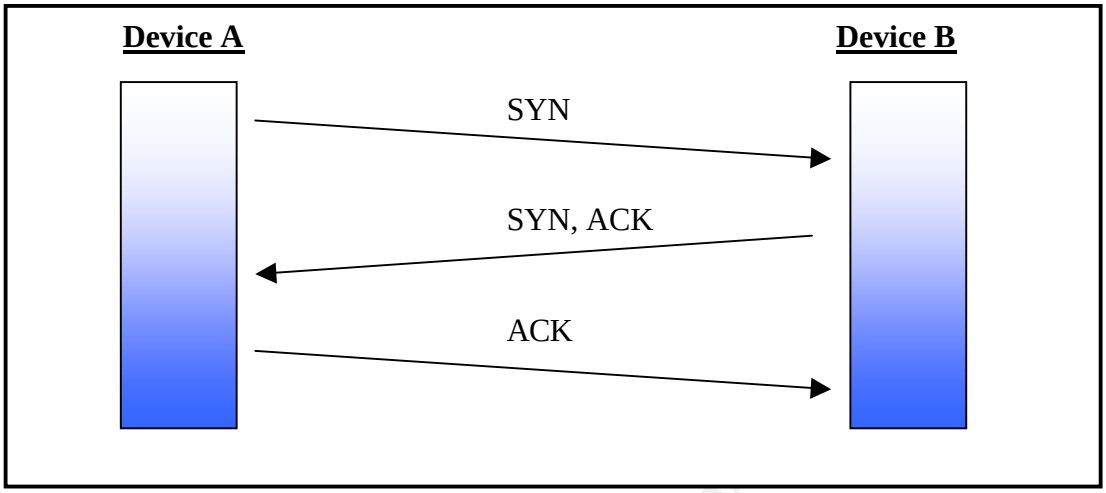

Figure 2 – TCP Handshake process

When Device A wants to talk, using TCP, to Device B, it sends a SYN (please Synchronise with me). Device B will send back the SYN and an ACK (in reply I want to also Synchronise, and I'm Acknowledging your request now). Once that has passed successfully the original device will send back an ACK (I Acknowledge that you got my request and that you are ok to talk). During this setup a port will be designated allowing the connection to exist at the logical level.[26] Port level discussion could be reserved for the 'Session Layer', however determining a port's status is achieved by the direct use of TCP, a Layer 4 (Transport Layer) protocol and because of that it is correct to mention it here.

7.5 Port scanning is often an attacker's first probe of your network. Lawrence Teo writes "Another sneakier, 'stealthier' kind of port scan is called the 'half-open' SYN scan. In this scan, the port scanner connects to the port but shuts down the connection right before a full connection occurs (hence the name 'half-open'). Since a full connection never happened, the operating system of the target machine usually does not log the scan"[27] He continues by writing "…the three-way handshake is never completed—the port scanner judges whether the port is open by the response given by the target machine." This is how attackers gather information about open ports on your system.

7.6 The port scanner that many attackers use by choice is NMAP. Considering only an Internet connection is needed to begin malicious activities it should be noted that NMAP can be obtained for free at http://www.insecure.org/[28] Any individual, or organisation, interested in network security, or in our case Layer 4 vulnerabilities and securities should be familiar with a product like NMAP. Understanding how these tools work will lead to better protection against attackers.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

7.7 Another way to reduce the risk is to implement a Firewall. Peter Norton says "A firewall is software running on the gateway server (or the access point for your network) that protects the resources inside your network against intrusion from outside the network."[29] It only makes sense to have a Firewall that, rather than accepting the half-open SYN state, will recognise and drop the packets. Linux uses processing called Iptables or Ipchains, depending on the version of Linux you use. Proper implementation of this technology is effective firewalling. If your system has connectivity to the internet then you will need to investigate and implement a firewall of some kind. If you do not it is similar to leaving the front door of your house open at night – living in a not so nice neighbourhood.

7.8 Lawrence Teo also comments on overcoming TCP vulnerabilities at the boundary by writing:

> "The good news is that such port scans are detectable using special tools. Solar Designer has developed such a tool called scanlogd, which is a daemon that runs in a background and listens on the network interface for port scans."[30]

7.9 Protecting against the myriad ways the TCP process is used against an organisation can seem daunting. However, once you have a fair understanding of the TCP handshake process you can then enhance that knowledge base relatively quickly. For example, this type of printout is what you can expect from a standard Firewall. This printout has been taken from an active firewall. You are looking at a genuine printout, except the xx marks exist to hide the identity of the machines.

```
20020313T021400 tcp 10.27.xx.xx:1663 -> 203.111.xx.xx:58396
20020313T021439 tcp 10.27.xx.xx:1668 -> 203.111.xx.xx:110
20020313T021624 tcp 10.27.xx.xx:1674 -> 203.111.xx.xx:8396
20020313T021700 tcp 10.27.xx.xx:1677 -> 203.111.xx.xx:8080
20020313T021830 tcp 10.27.xx.xx:1683 -> 203.111.xx.xx:443
```

Using the book *Network Intrusion Detection, An Analyst's Handbook*[31] as a guide to understanding TCP behaviour assists us here. It helps us determine the following characteristics about the first line of the printout:

20020313T021400	- indicates the time of the log
tcp	- the type of protocol used
10.27.xx.xx	- the source host ip address(xx.xx to hide the identity)
:1663	- source port
-->	- indicating direction of traffic flow
203.111.xx.xx	- the destination ip address
:58396	- the destination port.

The printout exists because a firewall was in place, and that firewall was not only monitoring inwards traffic, but also outwards traffic. The firewall acknowledged that a host was trying to establish a link outside the network. The interesting thing is that the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

source, within the network, is trying to connect to multiple ports at the destination. It appears that the source is scanning the destination. If your Firewall rules only allow certain connections you can set the software to alert you. Note that there is normally some administrative overhead attached to alerts. Once alerted you can scrutinise the log to find what happened on your network. As you can see, you do not need to know everything about TCP/IP to understand a basic log entry. You do though need to spend time on deciding what traffic can pass freely and what traffic should be halted.

This illustration existed because a user did not download the latest anti-virus pattern file. As a result a Trojan was placed on the user's computer. The user's computer then acted as a scanner for another site. The evidence of that can be seen by the same destination address with different ports trying to be reached. One could only guess what the intention of the Trojan was. It could have been to implant the destination with itself, or to prepare for an attack, or simply gather information. Information on Trojans will be covered in segment 10.

7.10 One thing to be aware of is the trade off between security and convenience. As Peter Norton mentions:

> The firewall is another example of the tradeoff between convenience and safety…. While it may be safer to block the ports used for World Wide Web traffic, many users need Web access today to do their jobs, and blocking those ports would be too inconvenient to be implemented.[32]

8. The Session Layer

8.1 Whatis.com (http://whatis.techtarget.com/) describes the Session Layer (Layer 5): "In the Open Systems Interconnection (OSI) communications model, the Session layer (sometimes called the "port layer") manages the setting up and taking down of the association between two communicating end points that is called a *connection*. A connection is maintained while the two end points are communicating back and forth in a conversation or *session* of some duration."[33]

8.2 Internet Security Systems (http://www.iss.net/) write "TCP session hijacking is when a hacker takes over a TCP session between two machines. Since most authentication only occurs at the start of a TCP session, this allows the hacker to gain access to a machine."[34] From this we notice that authentication is occurring to allow a session's establishment. A realistic question would be "Ok, I understand that an attacker could do that…but why?"

> A hacker can also be "inline" between B and C using a sniffing program to watch the conversation. This is known as a "man-in-the-middle attack".
> A common component of such an attack is to execute a denial-of-service (DoS) attack against one end-point to stop it from responding. This attack can be either against the machine to force it to crash, or against the network connection to force heavy packet loss.[35]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

8.3 It makes sense that an attacker would spend some of their time hiding their real identity, and for very good reasons. In the Session Layer a very important component exists in an attempt to prevent unwanted connections and that is authentication. We have already mentioned that basic authentication is instigated at the beginning of the TCP session. If the session is hijacked after that authentication then the destination will 'trust' the hijacked session.[36] Attackers are using already compiled programs like 'hunt' (http://lin.fsid.cvut.cz/~kra/index.html) to make the process easier.[37] It seems necessary then that we look at ways of strengthening the Session Layer. That is, strengthening the authentication process.

8.4 Richard Duncan explains accepted methods of authentication in his paper *An Overview of Different Authentication Methods and Protocols*[38]. He comments "Authentication is the first and most important line of defense [sic] in a system of trusted and open networks." Duncan also mentions that three well-known types of layer five protection are: SSL, Secure Socket Layer; SSH, Secure Shell; Kerberos; and IPSEC.[39]

8.4.1 SSL was developed by Netscape to be used with web connections or more specifically the Hyper Text Transfer Protocol (HTTP). "The client and server authenticate through the use of public keys and the use of security certificates from trusted sources"[40] A client sends a 'hello' message and protocol versions, session id, cipher suit, compression methods, and random values are sent to create a secure connection. Once a successful exchange has taken place the session is considered secure and it proceeds.[41] SSLeay is a free implementation of SSL.[42]

8.4.2 "SSH … is a protocol that lets you log in and execute commands on another machine over a network, as well as transfer files."[43] SSH uses a public/private key authentication system, namely RSA. When a client connects to a server the client has the server's public key and encrypts a random message with that public key. Only the server, which holds the private key, can decrypt the message. The server then sends back the message encrypted which the client understands as having been decrypted and encrypted again correctly. This process can only be done with the correct keys. There are versions of SSH available for most operating systems so the scope for use is favourable.[44]

8.4.3 Kerberos was developed to provide secure authentication over an insecure network, for example the Internet. Kerberos is based on a trusted third party principle. The client and the server look for authentication information from this third party. The client contacts a Kerberos server and establishes an encrypted authentication. The server achnowledges the client as a valid requestor and issues a ticket. This ticket acts as authentication to other servers on the network that are privy to the Kerberos process. Problems with this type of security are if at any stage the server hosting the tickets is vulnerable, the whole secure process is.[45]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

8.4.4 IPsec (IP Security) is another protocol based authentication method. The staff at Webopedia.com describes it like this:

> Short for ***IP Sec**urity*, a set of protocols developed to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks.
>
> IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (*payload*) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet.[46] IPsec can only tunnel IP traffic, so it is not useful for networks that use IPX, NetBEUI or AppleTalk protocols.[47]

8.5 The first line of defence with authentication is password protection. Passwords are a form of authentication and thus deserve mention with this layer.[48] Building strong passwords is a tradeoff with convenience. If you make your password policy too difficult users may be inclined to write the password down on a piece of paper and put it in a drawer. If your password policy is too relaxed users will choose inappropriate passwords such as: their birthday, their first or last name, the word password, or their telephone number. Peter Norton mentions password complexity in the book *Network Security Fundamentals.*[49] He explains to passwords should include letters, numbers and punctuation. Alternate ways to get users to remember complex passwords are to join two words with punctuation (ie blue$%public4). Other ways are to use the first letter of a sentence, with numbers and punctuation included (ie I remember walking down 3rd street in New York would be IRWD3SINY!). Peter Norton also mentions dropping vowels in words and replacing them with numbers is also effective.[50] Either way ensure you let your users know that there is a password policy and give them easy to understand guidelines on how to change passwords. To test the integrity of your passwords you can use tools for NT passwords found at http://www.l0phtcrack.com/ The use of l0phtcrack is wide spread and the tool is easy to use so there is it will not be covered in depth in this paper.

8.6 You would be correct if you deducted that authentication methods, other than passwords, can be difficult to master. However there are many professionals who can assist with this type of security implementation. If your data is valuable enough, this type of protection is a must. As an introduction it might be worthwhile remembering that authentication methods can be carried out at the Session Layer of the OSI model and securing this can be done using SSL, SSH, Kerberos and IPsec.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

9. Presentation Layer

9.1 "The presentation layer ensures that the communications passing through are in the appropriate form for the recipient. For example, a presentation layer program may format a file transfer request in binary code to ensure a successful file transfer."[51] From that information it can be determined that the Presentation Layer ensures the format of information is acceptable to the Application Layer and the Session Layer. For example ASCII and Binary interpretations are presented to applications. This means the 'passing' of that data is a Presentation Layer function.[52] Another type of code that is offered by the Presentation Layer is Unicode.[53]

9.2 The definition of Unicode as offered HostingWorks.com (http://hostingworks.com) is:

> "A 16-bit character set standard, designed and maintained by the non-profit consortium Unicode Inc.
>
> Originally Unicode was designed to be universal, unique, and uniform, i.e., the code was to cover all major modern written languages (universal), each character was to have exactly one encoding (unique), and each character was to be represented by a fixed width in bits (uniform)."[54]

9.3 Andrew Brannan addresses Unicode vulnerabilities in his paper *Unicode Vulnerability – How & Why?* He mentions that Microsoft IIS once accepted (there is a patch now to prevent this) Unicode where normal keyboard commands would be rejected. Microsoft IIS searches through each and every URL to ensure the request does not contain the characters '../'.[55] Specifically the command ../ is used by programs to run the remaining information in the parent directory. Attackers like this because by design systems do not grant permissions to the parent directory. Brannan specifically illustrates with the following:

> If the "/" character is encoded in Unicode as "%c0%af", the URL will pass the security check, as it does not contain any "../" patterns. Instead the security check only sees "..%c0%af", which it does not recognize as a malicious pattern.[56]

This flaw allows savvy users to enter your web server and using Unicode access directories that they would otherwise be restricted from. The reason is that IIS interprets both plain and Unicode commands, however, only the plain commands are compared with the denial list.[57]

9.4 Protecting against Unicode vulnerabilities can be as simple as applying the recommended patches from the vendor. This further illustrates that IT security is not a fix, but an ongoing dedication. Andrew Brannan comments "However, this vulnerability can be easily defeated if a careful system administrator takes a few simple steps, such as moving the web folder root off of the logical drive that holds the system executables."[58]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

This effectively takes away the attackers access to the 'crown jewels' of your operating system. So in part it is the vendor's responsibility to provide you, the IT consumer, with reasonably secure products, but you can meet them halfway.

10. The Application Layer

10.1 "Layer 7 of the Open Systems Interconnection (OSI) networking model, which defines standards for interaction at the user or application program level; for example, formatting electronic mail messages, reading and writing files, and file transfer. It is the highest layer of the protocol stack."[59] The interesting component here is that there is user and application interaction. The most common use of IT resources would have to be e-mail.

10.2 Considering that formatting electronic mail messages is part of Layer 7 it would make sense then that malicious use of this technology would be considered a Layer 7 threat or vulnerability. The greatest threat to have wide circulation must be the e-mail Trojan (short for Trojan Horse).

10.3 "Trojan horse is a destructive program that masquerades as a benign application. Unlike a viruses [sic], Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer."[60] For example, Whack-A-Mole is an interesting Trojan in that the malicious software is placed onto the victims' machine under the guise of a great little cartoon type game. You install the game, play it, however in the background the program has loaded a Trojan. [61] Just so that you know what you are up against, an incomplete list of known Trojans and the ports they use can be found at http://www.nccn.net/~ncpcug/trojans.htm

10.4 Protecting your assets from Trojans and Viruses is serious business. The people at Trend Micro (www.antivirus.com) are a profit organisation with revenue in 2001 at US$259 million.[62] There are various vendors you can obtain anti-virus (read anti-Trojan also) software from. Your needs and budget will dictate who you rely on. Keeping your license (if any) updated and listening to industry watch-keepers will allow you to be confident in your anti-virus software. The important thing to remember is that Trojans, and Viruses for that matter, are created daily. Because your anti-virus software is working today, does not mean it will protect you tomorrow. If is possible that as you are reading this paragraph someone is creating a new Trojan. A positive step in the right direction for defending your network is keeping your anti-virus software up to date, and ensuring those updates permeate your host network.

10.5 Anti-virus software detects a host of application layer exploits. We have already mentioned Trojans, but add to that Viruses and Worms and the list becomes more critical. Having established that a Trojan is installed pretending to be a harmless piece of software, it is time to segregate a Virus from a Worm. A Virus will attach itself to a data file or a program, where a Worm is self-propagating. A Worm wriggles its way into your computer network and then it can find other computers connected to yours and wriggle its way into them.[63] The security you have and the imagination of its inventor limit a

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Worm's actions. In the book *Underground: tales of hacking, madness and obsession on the electronic front*ier,[64] Suelette Dreyfus describes the chaos caused by an Australian designed worm which took over NASA's computer network in October 1989. If any network administrator is hesitating about obtaining a healthy virus scanner, and keeping that scanner up to date, then they should read this book. If one Worm can bring NASA to its knees then it is possible that one Worm can take a small company to a premature end of trading. Virus protection will help prevent this ill-fated outcome.

11. Summary

11.1 Understanding the OSI model helps the network administrator understand IT security. The topic is varied and growing each day. Threats facing an organisation range from a misdirected backhoe, to the sinister attacker carefully constructing a Trojan to open ports on your web server. There is no doubt that computer resources are under attack and those resources are not free.

11.2 By looking at the layers we can understand our networks' strengths and weaknesses. We may have purchased an excellent virus protection software kit, but our encryption methods are dated. Knowing that a particular layer is weak allows us to understand that our system is vulnerable and we can distribute resources, and seek specialist assistance if required.

11.3 The most critical thing you should take from this paper is that for every layer there are attacks being created, or attacks awaiting activation as a result of poor defence. Defending your system against attacks is not a one off thing – it is an ongoing process irrespective of the layer.

11.4 Understanding the OSI model gives us a better appreciation of the threats that our networks may encounter. By understanding the compartmentalised nature of the OSI model we begin to understand the compartmentalised, yet over arching approach we need to take. It is only when we can see our networks as individual components that we can adequately secure these levels. If we can break the network into manageable components, and the OSI model helps us do that, then we can divide the risk. Dividing the risk into more manageable components gives us a better chance at addressing vulnerabilities and therefore protecting our assets.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References

[1] "OSI" http://www.webopedia.com/TERM/O/OSI.html (15 Mar. 2002).

[2] "OSI" http://www.webopedia.com/TERM/O/OSI.html (15 Mar. 2002).

[3] Baker, David W. "Communications and Networking" *Using Java 1.1, Third Edition* http://docs.rinet.ru:8083/UJ11/ch23.htm (01 Mar. 2002).

[4] Baker, David W. "Communications and Networking" *Using Java 1.1, Third Edition* http://docs.rinet.ru:8083/UJ11/ch23.htm (01 Mar. 2002).

[5] "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the2.4 GHz Band" *Supplement to IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements.* http://standards.ieee.org/reading/ieee/std/lanman/802.11b-1999.pdf (15 Mar. 2002).

[6] Jackson, Doug. **"**AirUTD: Wireless at UT Dallas**"** http://webapps.utdallas.edu/irutd/index.asp (01 Mar. 2002).

[7] Baker, David W. "Communications and Networking" *Using Java 1.1, Third Edition* http://docs.rinet.ru:8083/UJ11/ch23.htm (01 Mar. 2002).

[8] "ARP" http://compnetworking.about.com/library/glossary/bldef-arp.htm (01 Mar. 2002).

[9] "ARP" http://compnetworking.about.com/library/glossary/bldef-arp.htm (01 Mar. 2002).

[10] "ARP" http://compnetworking.about.com/library/glossary/bldef-arp.htm (01 Mar. 2002).

[11] Fleck, Bob and Dimov, Jordan. "Wireless Access Points and ARP Poisoning: Wireless vulnerabilities that expose the wired network" http://www.cigitallabs.com/resources/papers/download/arppoison.pdf (02 Mar. 2002).

[12] Osterloh, Heather. "ITCP/IP Addressing and the protocol suite" *CCNA 2.0 Prep Kit 640-507 Routing and Switching* Indianapolis, Indiana, USA: Que, 2000. (Ch6)

[13] Fleck, Bob and Dimov, Jordan. "Wireless Access Points and ARP Poisoning: Wireless vulnerabilities that expose the wired network" http://www.cigitallabs.com/resources/papers/download/arppoison.pdf (02 Mar. 2002).

[14] Fleck, Bob and Dimov, Jordan. "Wireless Access Points and ARP Poisoning: Wireless vulnerabilities that expose the wired network" http://www.cigitallabs.com/resources/papers/download/arppoison.pdf (02 Mar. 2002).

[15] Minter Technologies. "Protecting against the unknown" http://mixter.warrior2k.com/protecting.html (02 Mar. 2002).

[16] Baker, David W. "Communications and Networking" *Using Java 1.1, Third Edition* http://docs.rinet.ru:8083/UJ11/ch23.htm (01 Mar. 2002).

[17] "Router" http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212924,00.html (15 Mar. 2002).

[18] "Exploiting Cisco Systems(Even From Windows!" http://blacksun.box.sk/cisco.txt (20 Mar. 2002).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

[19] "Exploiting Cisco Systems(Even From Windows!" http://blacksun.box.sk/cisco.txt (20 Mar. 2002).

[20] "Cisco Security Advisory: 7xx Router Password Buffer Overflow" http://www.cisco.com/warp/public/770/pwbuf-pub.shtml (20 Mar. 2002).

[21] Cisco Security Advisory: 7xx Router Password Buffer Overflow" http://www.cisco.com/warp/public/770/pwbuf-pub.shtml (20 Mar. 2002).

[22] "Transport Layer" http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213212,00.html (20 Mar. 2002).

[23] "DOD STANDARD TRANSMISSION CONTROL PROTOCOL" http://www.rfc.net/rfc761.txt (10 Mar. 2002).

[24] "Internet Protocol" http://searchwebmanagement.techtarget.com/sDefinition/0,,sid27_gci214157,00.html (08 Mar. 2002).

[25] Chappell, Laura. "Inside the TCP Handshake." http://www.nwconnection.com/2000_03/pdf30/hand30.pdf (20 Mar. 2002)

[26] Northcutt, Stephen, and Novak, Judy "Network Intrusion Detection An Analyst's Handbook" Second Edition. Indianapolis, Indiana USA: New Riders, 2000. (Ch 2, p26)

[27] Teo, Lawrence. "Network Probes Explained: Understanding Port Scans and Ping Sweeps" http://www.linuxjournal.com/article.php?sid=4234 (20 Mar. 2002).

[28] McClure, Stuart, Joel Scrambray, and George Kurtz. Hacking Exposed. Third Edition. Berkeley, California USA: Osborne/McGraw-Hill, 2001. (Ch2, p42).

[29] Norton, Peter and Stockman, Mike. "Network Security Fundamentals" First Edition. Indianapolics, Indiana, USA: SAMS, 2000.(Ch1, p15)

[30] Teo, Lawrence. "Network Probes Explained: Understanding Port Scans and Ping Sweeps" http://www.linuxjournal.com/article.php?sid=4234 (20 Mar. 2002).

[31] Northcutt, Stephen, and Novak, Judy "Network Intrusion Detection An Analyst's Handbook" Second Edition. Indianapolis, Indiana USA: New Riders, 2000.

[32] Norton, Peter and Stockman, Mike. "Network Security Fundamentals" First Edition. Indianapolics, Indiana, USA: SAMS, 2000. (Pt1, Ch1, p15)

[33] "Session Layer" http://whatis.techtarget.com/definition/0,289893,sid9_gci212967,00.html (20 Mar. 2002).

[34] "Session Hijacking" http://www.networkice.com/Advice/Exploits/TCP/session_hijacking/default.htm (20 Mar. 2002).

[35] "Session Hijacking" http://www.networkice.com/Advice/Exploits/TCP/session_hijacking/default.htm (20 Mar. 2002).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

[36] "Session Hijacking" http://www.networkice.com/Advice/Exploits/TCP/session_hijacking/default.htm (20 Mar. 2002).

[37] McClure, Stuart, Joel Scrambray, and George Kurtz. Hacking Exposed. Third Edition. Berkeley, California USA: Osborne/McGraw-Hill, 2001 (Ch14, p555).

[38] Duncan, Richard. "Authentication" http://rr.sans.org/authentic.overview.php (20 Mar. 2002).

[39] Duncan, Richard. "Authentication" http://rr.sans.org/authentic.overview.php (20 Mar. 2002).

[40] Norton, Peter and Stockman, Mike. "Network Security Fundamentals" First Edition. Indianapolics, Indiana, USA: SAMS, 2000. (Pt2 Ch5 p88)

[41] Duncan, Richard. "Authentication" http://rr.sans.org/authentic.overview.php (20 Mar. 2002).

[42] Norton, Peter and Stockman, Mike. "Network Security Fundamentals" First Edition. Indianapolics, Indiana, USA: SAMS, 2000. (Pt2 Ch5 p88)

[43] Norton, Peter and Stockman, Mike. "Network Security Fundamentals" First Edition. Indianapolics, Indiana, USA: SAMS, 2000. (Pt2 Ch5 p86)

[44] Norton, Peter and Stockman, Mike. "Network Security Fundamentals" First Edition. Indianapolics, Indiana, USA: SAMS, 2000. (Pt2 Ch5 p86, 87)

[45] Norton, Peter and Stockman, Mike. "Network Security Fundamentals" First Edition. Indianapolics, Indiana, USA: SAMS, 2000. (Pt2 Ch6, p107)

[46] "IPSEC" http://www.webopedia.com/TERM/I/Ipsec.html (20 Mar. 2002).

[47] Norton, Peter and Stockman, Mike. "Network Security Fundamentals" First Edition. Indianapolics, Indiana, USA: SAMS, 2000. (Pt2 Ch4, p63)

[48] Norton, Peter and Stockman, Mike. "Network Security Fundamentals" First Edition. Indianapolics, Indiana, USA: SAMS, 2000. (Pt2 Ch6, p95)

[49] Norton, Peter and Stockman, Mike. "Network Security Fundamentals" First Edition. Indianapolics, Indiana, USA: SAMS, 2000. (Pt2 Ch6, p97,98)

[50] Norton, Peter and Stockman, Mike. "Network Security Fundamentals" First Edition. Indianapolics, Indiana, USA: SAMS, 2000. (Pt2 Ch6, p97)

[51] "Presentation Layer" http://whatis.techtarget.com/definition/0,289893,sid9_gc212824,00.html (20 Mar. 2002).

[52] "Presentation Layer" http://whatis.techtarget.com/definition/0,289893,sid9_gc212824,00.html (20 Mar. 2002).

[53] "ISO" http://courses.cs.vt.edu/~cs4254/fall01/slides/iso_6.pdf (20 Mar. 2002).

[54] "Unicode" http://hostingworks.com/support/dict.phtml?foldoc=Unicode (20 Mar. 2002).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

[55] Brannan, Andrew. "Unicode Vulnerability – How & Why" http://rr.sans.org/threats/unicode.php (20 Mar. 2002).

[56] Brannan, Andrew. "Unicode Vulnerability – How & Why" http://rr.sans.org/threats/unicode.php (20 Mar. 2002).

[57] Brannan, Andrew. "Unicode Vulnerability – How & Why" http://rr.sans.org/threats/unicode.php (20 Mar. 2002).

[58] Brannan, Andrew. "Unicode Vulnerability – How & Why" http://rr.sans.org/threats/unicode.php (20 Mar. 2002).

[59] "Application Layer" http://www.computeruser.com/resources/dictionary/noframes/nf.definition.html?bG9va3VwPTEyMDU= (20 Mar. 2002).

[60] "What is a trojan?" http://www.astonsoft.com/whatstrojan.htm (20 Mar. 2002).

[61] McClure, Stuart, Joel Scrambray, and George Kurtz. Hacking Exposed. Third Edition. Berkeley, California USA: Osborne/McGraw-Hill, 2001 (Ch14, p579).

[62] "Company Profile" http://www.antivirus.com/corporate/company_profile/ (20 Mar. 2002).

[63] Dreyfus, Suelette. Underground: tales of hacking, madness & obsession on the electronic frontier. Kew, Victoria Australia: Mandarin, 1997. (Ch1, p10)

[64] Dreyfus, Suelette. Underground: tales of hacking, madness & obsession on the electronic frontier. Kew, Victoria Australia: Mandarin, 1997. (Ch1)

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 5th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced