Hacker Highschool
SECURITY AWARENESS FOR TEENS

LESSON 4
SERVICES AND CONNECTIONS

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

Table of Contents

"License for Use" Information....2
Contributors....4
4.0 Introduction....5
4.1 Services....6
4.1.1 HTTP and The Web....6
4.1.2 E-Mail – POP and SMTP....7
4.1.3 IRC....8
4.1.4 FTP....8
4.1.5 Telnet and SSH....10
4.1.6 DNS....10
4.1.7 DHCP....11
4.2 Connections....12
4.2.1 ISPs....12
4.2.2 Plain Old Telephone Service....12
4.2.3 DSL....12
4.2.4 Cable Modems....13
Further Reading....14

Contributors

Chuck Truett, ISECOM

Guiomar Corral, La Salle URL Barcelona

Jaume Abella, La Salle URL Barcelona - ISECOM

Kim Truett, ISECOM

Marta Barceló, ISECOM

Pete Herzog, ISECOM

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

LA SALLE
Enginyeria
Arquitectura
Universitat Ramon Llull

4.0 Introduction

The purpose of this lesson is to give you an understanding of some of the basic services which networks use to provide and exchange information, and to discuss some of the methods in which personal computers and local networks connect with the other networks which make up the Internet.

4.1 Services

You have a computer, and you know that there is useful information on this computer, but not very much. You also know that other people, millions of other people also have computers, and that their computers will also have useful information.

Now, you can assume that these other people, and these other computers may very likely have lots of information on them that would be of interest to you. The only problem is how to access all this useful information that may be on other people's computers.

The computers themselves can communicate with each other, easily, through ports, using the different protocols that have been designed, but that doesn't really help you. You can't understand the streams of binary data that the computers exchange between themselves. You need some way for your computer to interpret the information that it can receive from the other computers in some way that you can use it.

The programs that the computers use to translate the data that they exchange into a form that is useful to you are call *services*. These services allow you to view web pages, exchange e-mail, chat, and interact in remote computers in many other different ways.

Your computer, the *local* computer uses programs called *clients* to interpret the information that you receive. The other computers, the *remote* computers, use programs called *servers* to provide this information to your computer.

4.1.1 HTTP and The Web

When you say, 'the Internet,' what comes to mind for most people is, in fact, the *World Wide Web*. The World Wide Web, or just the Web, is not the Internet. Instead, it is a method of using the Internet to exchange information between computers. The Web uses *http* or *hypertext transfer protocol* and services known as *web browsers* and *web servers* to allow information in the form of *web pages* to be exchanged between local and remote computers.

On the local side, what you see is the *web browser*. Information from the remote computer is sent to your local computer using the http protocol. The web browser interprets that information and displays it on your local computer in the form of web pages.

The *hypertext* part of the http protocol refers to a non-linear method of presenting information. Text is normally read in a linear fashion: word 2 follows word 1; sentence 3 follows sentence 2; paragraph 5 follows paragraph 4. The idea of hypertext allows information to be viewed in a non-linear way. This is the major difference between hypertext and the older, plain text methods of displaying information.

With hypertext, words and ideas can connect, not only with the words that directly surround them, but also with other words, ideas or images. Hypertext is not restricted to the Web. Most full-featured word processors will allow you to create locally stored pages in web or http format. These pages are read using your web browser and act as would any other web page, only they are stored on your local computer, not a remote computer.

On your local computer, you use a client program called a web browser. Contrary to what you might have been lead to believe, there are actually a number of web browsers available for both Windows and Linux. These include Microsoft's Internet Explorer, Netscape Navigator, and the Mozilla Firefox browsers.

You can also create your own web page. The easiest way to do this is to use one of the common word processors, such as OpenOffice, Microsoft Word, or WordPerfect. These programs will allow you to produce simple web pages, combining text, hypertext and images.

Plenty of people have made useful, clever and innovative web pages using these simple tools.

But these pages aren't flashy. Flashy means frames and scripts and animations. It also means spending lots of money on a fancy web page design program. These programs allow you to create many interesting effects on your web page, but they are more complex to use than the word processors that you are probably already familiar with.

Once you have the pages designed, you'll need a computer to put them on, so that other people can view them. This is called *web hosting*.

The hosting computer will be running a web server. It is possible to run one of these servers from your own home, using your own computer, but there are several drawbacks, the primary one of these being *persistence*. Information stored on a web server is only available when that server is powered up, operating properly and has an open connection. So, if you want to run a web server from your own bedroom, you have to leave your computer on all the time; you have to make sure that the web server program is operating properly all the time (this includes troubleshooting hardware problems, controlling viruses, worms and other attacks, and dealing with the inevitable bugs and flaws within the program itself), and you have to keep a connection to the Internet open. This is why most people pay someone else to do all this.

A *web hosting* company will store your web page on their computer. A perfect web hosting company will have multiple, redundant servers and a regular backup policy, so that your service is not lost because of hardware problems, a support staff to keep the server running despite hacker attacks and program bugs, and a number of open connections to the Internet, so that all your have to do is design your web page, upload it to the hosting company's server, hang up the phone, turn off the computer, and go to sleep, and your web page will be available to the entire world.

It's also possible to find organizations that offer free web hosting. Some of these organizations are funded by paid advertising, which means that anyone who wants to view your web page will first have to view someone else's advertisement. But they don't have to buy anything, and you don't have to pay anything.

4.1.2 E-Mail – POP and SMTP

The second most visible aspect of the Internet is probably e-mail. On your computer, you use an e-mail client, which connects to a mail server. When you set up your e-mail account, you are given a unique name in the form of *user@domain*. You are also asked to provide a password to use to retrieve your e-mail.

The *SMTP* protocol, which is used to send e-mail, does not require a password. This may not have been a fault when the protocol was designed, and the Internet was a small world inhabited by like minded people, but now it has become a loophole which allows for unauthorized use of mail servers and various other tricks, such as 'e-mail spoofing', in which someone sends an e-mail that appears to come from another address. However, some mail servers minimize this flaw by implementing an authentication step, in which you must prove your identity before you can send an e-mail.

One important thing to remember is, despite being password protected, e-mail is not a way to send secure information. Most POP clients and servers require that your password be communicated – unencrypted – to your mail server. This doesn't mean than anyone who receives an e-mail from you also receives your password; but it does mean that someone with

the right knowledge and tools can relatively easily 'sniff out' your password. (For ideas on making your e-mail more secure, see **Lesson 9: E-mail Security**.)

4.1.3 IRC

IRC, or *Internet relay chat*, is where the unregulated nature of the Internet is most clearly expressed. On IRC, anyone with anything to say gets a chance to say it.

You may be familiar with the chat rooms used by certain online services. IRC is just like a chat room, only there are no rules, there are no standards, and – quite often – there are no chaperones. You may find exactly what you are looking for on an IRC channel, or you just may find something that you had rather you never knew existed.

All the rules that you've heard about chat rooms are applicable to IRC channels. Don't tell anyone your real name. Don't give out your phone number, your address, or your bank account numbers. But have fun!

Exercises:

Find and join three IRC channels which focus on security topics. How do you join in the public conversation? What do you have to do to have a private conversation with a person?

It is possible to exchange files through IRC. How could you do this? Would you always want to exchange files through IRC? Why or why not?

4.1.4 FTP

FTP stands for *file transfer protocol*. As the name implies, it allows for files to be transferred between a local and a remote computer. While it can be used for private file transfers, it is more commonly associated with free, anonymous ftp servers which offer public access to collections of files.

Anonymous ftp was once the means by which most computer users exchanged files over the Internet. While many anonymous ftp servers are used to distribute files that are available illegally(and are possibly infected with viruses), there are also many which are legally used to distribute programs and files. Servers which offer anonymous ftp services can be found through various means, including Internet search engines.

Most anonymous ftp servers now allow you to access their files using the ftp protocol through a web browser.

Exercises:

Both Windows and Linux come with a basic, command line ftp client; to access it, open a command prompt or terminal window and type:

```
ftp
```

At the `ftp>` prompt, you can type `help`, to get a list of available commands.

```
ftp> help
Commands may be abbreviated.  Commands are:
!               delete          literal         prompt          send
?               debug           ls              put             status
append          dir             mdelete         pwd             trace
ascii           disconnect      mdir            quit            type
```

```
bell            get             mget            quote           user
binary          glob            mkdir           recv            verbose
bye             hash            mls             remotehelp
cd              help            mput            rename
close           lcd             open            rmdir
```

Some important commands are:

```
ftp> open <domain.name>
```

Which connects you to the ftp server named *domain.name*.

```
ftp> ls
```

or

```
ftp> dir
```

Which lists the contents of the remote working directory.

```
ftp> cd <newdir>
```

Which changes the remote working directory to a directory named *newdir*.

```
ftp> get <filename>
```

Which downloads a file named *filename* from the remote computer to the local computer.

```
ftp> mget <file1> <file2> <file3>
```

Which downloads files named *file1*, *file2*, and *file3* from the remote computer to the local computer.

```
ftp> close
```

Which disconnects you from the remote ftp server.

```
ftp> quit
```

Which shuts down your local ftp client.

To connect to an anonymous ftp service, you must first open your local ftp client:

```
ftp
```

Use the open command to connect to the server. The command

```
ftp> open <anon.server>
```

connects your ftp client with the anonymous ftp server named *anon.server*.

When the remote ftp server makes its connection, it will identify itself to your local client, then ask for a user name.

```
Connected to anon.server.
220 ProFTPD Server (Welcome . . . )
User (anon.server:(none)):
```

For most anonymous ftp servers, you should enter in the word *anonymous* as the user name. The remote ftp server will acknowledge that you are connecting as an anonymous user, and will give you instructions on what to use as a password.

```
331 Anonymous login ok, send your complete email address as your
password.
```

```
Password:
```

In most cases, the remote server does not check the validity of the email address entered as a password, so it will not stop you from accessing the server if you enter an invalid address. However, this is considered to be a breach of etiquette. After you have entered a password, the remote server will send a welcome message to your local computer.

230-

Welcome to ftp.anon.server, the public ftp server of anon.server. We

hope you find what you're looking for.

If you have any problems or questions, please send email to

ftpadmin@anon.server

Thanks!

230 Anonymous access granted, restrictions apply.

From here, you can use the ls, dir, cd and get commands to download files from the remote server to your local computer.

Using these examples, see if you can download a file from an anonymous ftp server. Use your web browser and a search engine to find an anonymous ftp server which has a copy of *Alice in Wonderland*, then, using the command line ftp client – not your web browser – try to download the file.

4.1.5 Telnet and SSH

Telnet allows a local user to send a wide variety of commands to a remote computer. This allows the local user to instruct the remote computer to perform functions and return data to the local computer, almost as if you were sitting at a keyboard in front of the remote computer. *SSH,* or *secure shell* is intended as a secure replacement for telnet.

Again, both Windows and Linux come with a basic, command line telnet client; to access it, open a command prompt or terminal window and type: telnet.

To access a telnet server, you will need to have an account and password set up for you by the administrator of the server, because the telnet program allows you to perform a large number of actions, some of which could severely compromise the remote computer.

Telnet was used in the past to allow computer administrators to remotely control servers and to provide user support from a distance.

Telnet can also be used for a number of other tasks, such as sending and receiving email and viewing the source code for web pages (although telnet does fall under the heading of the most difficult way to do these things). Telnet can be used to do many things that are illegal and immoral, but there are also legitimate reasons for using it. You can use telnet to check your email, and view, not just the subject line, but the first few lines of an email, which will allow you to decide whether or not to delete the email without downloading the entire message.

4.1.6 DNS

When you want to call a friend on the phone, you need to know the correct phone number; when you want to connect to a remote computer, you also need to know its number. You

may remember from previous lessons that, for computers on the Internet, this number is called the *IP address.*

As numbers, these IP addresses are very easily managed by computers, but as humans, we prefer to use what are called *domain names.* For example, to connect to the Hacker Highschool web page, we type 'www.hackerhighschool.org' into the address bar of a web browser. However, the web browser can't use this name to connect to the server that hosts the Hacker Highschool web page – it must use the IP address. This means that your local computer must have some means of translating domain names into IP addresses. If there were only hundreds, or even thousands of computers on the Internet, then it might be possible for you to have a simple table stored on your computer to use to look up these addresses, but, not only are there are millions of computers on the Internet, the correlations between domain names and IP addresses can change daily.

For this reason, *DNS* or *Domain Name Service* is used to translate domain names into IP addresses. When you type the domain name *www.domainname.com* into your web browser, your web browser contacts the DNS server chosen by your ISP. If that DNS server has *www.domainname.com* in its database, then it will return the IP address to your computer, allowing you to connect.

If your DNS server doesn't have *www.domainname.com* in its database, then it will send a request to another DNS server, and it will keep sending requests to other DNS servers until it finds the correct IP address, or it establishes that the domain name is invalid.

Exercises:

To learn more about DNS:

Open an MS-DOS window and identify the IP address of your computer. What command have you used? What IP address do you have?

Identify the IP address of your DNS server. What command have you used? What is the IP address of the DNS server.

Ping *www.isecom.org*. Do you receive an affirmative answer? What IP address answers the ping?

Can you direct your computer to use a different DNS server? If so, change the configuration of your computer so that it uses a different DNS server. Ping *www.isecom.org* again. Do you receive the same response? Why?

4.1.7 DHCP

DHCP or *Dynamic Host configuration Protocol* allows for IP addresses to be dynamically allocated within a network. The network is given a block of IP addresses for its use. When a computer joins the network, it is assigned an IP address. When a computer leaves, its IP address becomes available for use by another computer.

This is useful for large networks of computers, since it is not necessary for each computer to have an individually assigned, static IP address. Instead, you use a *DHCP server.* When a new computer connects to the network, the first thing that it does is request an IP address from the DHCP server. Once it has been assigned an IP address, the computer then has access to all the services of the network.

4.2 Connections

Most computers connect to the Internet through a modem. Modems translate the digital signals produced by computers into analog signals that can be transmitted across commonly available telephone lines. Modem speeds are measured in *baud* or *bits per second*. Higher baud rates are better, since they allow for faster transmission of data, but you must also consider what you are planning to do. There are certain applications – such as telnetting into MUDs – for which a twenty year old 300 baud modem would still be acceptable (provided your typing speed wasn't so good), while high bandwidth applications such as streaming video can often strain even the most powerful cable modems.

4.2.1 ISPs

You don't just call up the Internet. You need to access a server that will connect your computer to the Internet. The server does all the heavy work, like being on all the time. The server is run by an *ISP* or *Internet Service Provider*.

An ISP has a point-of-presence on the Internet that is constant, and it has servers that run the services you are going to use. Now, you can run these services on your own. For example, you can run a mail server on your local computer, but it will require you to have your computer powered up and connected to a network all the time, just waiting for those brief moments when information has to be exchanged. An ISP, however, consolidates the efforts of a large number of users, so the mail server is working all the time, instead of sitting around, doing nothing. Additionally, an ISP's computers are going to use a high speed connection to connect to a NAP or Network Access Point. These NAPs then interconnect with each other through ultra-high speed connections called *backbones*. This is the Internet.

4.2.2 Plain Old Telephone Service

POTS, or *plain old telephone service*, is still the most widely used method of accessing the Internet. Its primary disadvantage is its low speed, but in many cases this is made up for by its wide availability. Most national Internet service providers have a large number of local access numbers, and almost everyone still has a phone with a land line. In theory, if you had an acoustic modem and a pocket full of change, you could connect from almost any public pay phone. Not that you would really want to do that.

POTS is slow. The fastest telephone modems are rated at a speed of 56,600 baud. That, however, as they explain in the small print, is a lie. Power constraints limit the actual download speed to about 53,000 baud and the effective rate is usually much lower. This doesn't compare very well with DSL or cable modems.

That said, telephone service is widely available, and POTS based ISPs are relatively cheap (and sometimes free). You wouldn't want to trade pirated movies over POTS, because it's immoral, illegal and ties up your phone line all night and maybe into the afternoon, but you could certainly send friendly, text based e-mails to Granny. And if you used telnet, you could even do it with a dusty DOS based machine that you pulled out of the basement.

4.2.3 DSL

DSL or *digital subscriber line*, is a method of sending large amounts of information over the wires that already exist for the POTS. Its main advantage over POTS is that it is much faster than analog modems, and it provides a permanent connection. In addition, it allows you to make and receive regular telephone calls while you are connected to the Internet. Its main

disadvantage is that its availability is limited by your proximity to the telephone company's switching equipment – if you live too far down the line; you're out of luck.

Exercises:

Using a web search engine, find two companies that supply DSL access. What other services do these companies provide (telephone service, tv service . . .)?

4.2.4 Cable Modems

Cable modems do not use the traditional telephone lines to connect to the Internet. Instead they make use of the optical fiber lines that are used by cable companies to transmit digital cable signals. Like DSL, cable modems allow you to make and receive regular telephone calls while you are connected to the Internet, and they provide a permanent connection, but cable modems are generally faster than DSL.

Cable modems have two basic flaws. The first is that cable modem access is a shared resource, so your connection speeds will be decreased when there are other users in close geographic proximity. The second is that cable modem access is only available in areas where cable companies have installed the necessary fiber optic wiring.

Exercises:

Using a web search engine, find two companies that provide Internet access through cable modems. What other services do these companies provide (telephone service, tv service . . .)?

Further Reading

How E-mail Works: http://computer.howstuffworks.com/email.htm

An IRC FAQ: http://www.irchelp.org/irchelp/new2irc.html

A Basic FTP FAQ (old, but extensive): http://www.faqs.org/faqs/ftp-list/faq/

Another FTP FAQ (also old): http://www.ibiblio.org/pub/Linux/docs/faqs/FTP-FAQ

An Overview of SMTP (with a link to RFC 821, which details the protocol):
http://www.freesoft.org/CIE/Topics/94.htm

And a complementary Overview of POP3 (with a link to RFC 1725):
http://www.freesoft.org/CIE/Topics/95.htm

An Overview of Telnet: http://www.dmine.com/bbscorner/telover.htm

Retrieving Mail with Telnet:
http://wiki.linuxquestions.org/wiki/Retrieving_mail_manually_using_telnet

SSH – a more secure alternative to Telnet: http://www.openssh.com/

Basic DNS Information:
http://hotwired.lycos.com/webmonkey/webmonkey/geektalk/97/03/index4a.html

More Detailed DNS Information:
http://www.microsoft.com/technet/itsolutions/network/deploy/confeat/domain.mspx

A collection of DNS commands, tests and lookups: http://www.dnsstuff.com/

A detailed DHCP FAQ: http://www.dhcp-handbook.com/dhcp_faq.html

A long article on DCHP, with information on NAT and routers:
http://hotwired.lycos.com/webmonkey/00/39/index3a.html?tw=backend

An Overview of Cable Modems: http://electronics.howstuffworks.com/cable-modem.htm