Hacker Highschool
SECURITY AWARENESS FOR TEENS

COMPLETE TABLE OF CONTENTS AND GLOSSARY

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

Lesson 1: Being a Hacker

Lesson 2: Basic Commands in Linux and Windows

Lesson 3: Ports and Protocols

Lesson 7: Attack Analysis

Lesson 8: Digital Forensics

Lesson 9: Email Security

Lesson 10: Web Security

Lesson 11: Passwords

Lesson 12: Legalities and Ethics

Glossary

Find more computer term definitions at www.webopedia.com, which provided many of the definitions reproduced here.

Anonymous FTP – A method by which computer files are made available for downloading by the general public

awk – A programming language designed for working with strings.

backdoors – An undocumented way of gaining access to a program, online service or an entire computer system.

Baud – bits per second, used to describe the rate at which computers exchange information.

BIOS – basic input/output system. The built-in software that determines what a computer can do without accessing programs from a disk. On PCs, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions. The BIOS is typically placed in a ROM chip that comes with the computer.

blog (weblogs) – Web page that serves as a publicly accessible personal journal for an individual.

Boolean logic – Boolean logic is a form of algebra in which all values are reduced to either TRUE or FALSE. Boolean logic is especially important for computer science because it fits nicely with the binary numbering system, in which each bit has a value of either 1 or 0. Another way of looking at it is that each bit has a value of either TRUE or FALSE.

Boot sector – The first sector of the hard disk where the master boot records resides, which is a small program that is executed when a computer boots up.

cache – Pronounced cash, a special high-speed storage mechanism. It can be either a reserved section of main memory or an independent high-speed storage device. Two types of caching are commonly used in personal computers: memory caching and disk caching.

Client – a program on a local computer that is used to exchange data with a remote computer, see server.

cluster / allocation unit – A group of disk sectors. The operating system assigns a unique number to each cluster and then keeps track of files according to which clusters they use

cookies – A message given to a Web browser by a Web server. The browser stores the message in a text file. The message is then sent back to the server each time the browser requests a page from the server.

CRC – Cyclical redundancy check.

cyclical redundancy check (CRC) – a common technique for detecting data transmission errors. Transmitted messages are divided into predetermined lengths that are divided by a fixed divisor. According to the calculation, the remainder number is appended onto and sent with the message. When the message is received, the computer recalculates the remainder and compares it to the transmitted remainder. If the numbers do not match, an error is detected.

DHCP – Dynamic Host Configuration Protocol.

Digital Subscriber Line (DSL) – A technology that allows the simultaneous transmission of voice and high-speed data using traditional telephone lines.

DNS – Domain Name Server.

Domain Name Server (DNS) – A service that translates domain names into IP addresses.

domain names – A name that identifies one or more IP addresses. For example, the domain name microsoft.com represents about a dozen IP addresses. Domain names are used in URLs to identify particular Web pages. For example, in the URL http://www.pcwebopedia.com/index.html, the domain name is pcwebopedia.com.

Every domain name has a suffix that indicates which top level domain (TLD) it belongs to. There are only a limited number of such domains. For example:

.gov - Government agencies

.edu - Educational institutions

.org - Organizations (nonprofit)

.com - Commercial Business

.net - Network organizations

Because the Internet is based on IP addresses, not domain names, every Web server requires a Domain Name System (DNS) server to translate domain names into IP addresses.

DSL – Digital Subscriber Line.

Dynamic Host Configuration Protocol (DHCP) – A protocol used to allow for the dynamic configuration of networks.

E-mail – A service with allows for the transmission of simple messages across networks.

ethereal – a packet sniffer that records traffic on your computer.

ethernet – A local-area network (LAN) architecture developed by Xerox Corporation in cooperation with DEC and Intel in 1976. It is one of the most widely implemented LAN standards.

file signature – Small 6-byte signature at the start of the file which identifies what kind of file it is.

file transfer protocol (FTP) – Used to allow local computers to download files from remote computers.

filtered (ports) – ports for which a firewall examines the header of a packet that is directed to that port and determines whether or not to let it through (see open ports).

firewall – A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

forums – An online discussion group. Online services and bulletin board services (BBS's) provide a variety of forums, in which participants with common interests can exchange open messages

FTP – File transfer protocol.

GCHQ – Government Communications Headquarters, is an intelligence and security organization in the UK.

grep – Short for global-regular-expression-print, a UNIX utility that allows the user to search one or more files for a specific string of text and outputs all the lines that contain the string. The user also has the option to replace the string with another.

HIDS – a host based intrusion detection. An intrusion detection system.

honeypot – An Internet-attached server that acts as a decoy, luring in potential hackers in order to study their activities and monitor how they are able to break into a system.

http – hypertext transfer protocol

hub – A common connection point for devices in a network. Hubs are commonly used to connect segments of a LAN.

Hypertext – a method of organizing and presenting data that allows the user to easily move between related items.

hypertext transfer protocol (http) – The underlying protocol used by the World Wide Web, HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

IANA – Internet Assigned Numbers Authority.

ICMP – Internet Control Message Protocol.

IM – Instant messaging.

Instant messaging (IM) – a type of communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet, analogous to a telephone conversation but using text-based, not voice-based, communication.

interfaces – A boundary across which two independent systems meet and act on or communicate with each other.

Internet Assigned Numbers Authority (IANA) – An organization working under the auspices of the Internet Architecture Board (IAB) that is responsible for assigning new Internet-wide IP addresses.

Internet Control Message Protocol (ICMP) – An extension to the Internet Protocol (IP) defined by RFC 792. ICMP supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

internet protocol (IP) – IP specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

Internet Relay Chat (IRC) – A service which allows for real-time, text-based communication between Internet users.

Internet Service Provider (ISP) – A company which provides users with access to the Internet

IP – Internet protocol.

IP address – An identifier for a computer in the internet or on a TCP/IP network. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 61.160.10.240 could be an IP address.

ipconfig – Tool to display information on the active interfaces on a computer.

IRC – Internet Relay Chat.

ISP – Internet Service Provider, a company which provides users with access to the Internet

logicbombs – code designed to execute when a specific activity occurs on a network or computer.

loopback – when a computer refers to itself. Loopback address is a special IP number (127.0.0.1) that is designated for the software loopback interface of a machine. The loopback interface has no hardware associated with it, and it is not physically connected to a network.

MAC – Media access control .

MD5 hash – An algorithm used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

media access control (MAC) – A hardware address that uniquely identifies each node of a network.

Modem – Modulator/Demodulator, a device which translates digital signals into analog signals, and analog signals back into digital signals, allowing computers to communicate with each other through analog telephone lines.

MS-DOS (Microsoft Disk Operating System) – MS-DOS is an Operating System. Mainly it allows the communication between users and PC hardware, and it also manages available resources, such as memory and CPU usage.

netstat – command which displays the status of a network.

network intrusion detection (NIDS) – Intrusion detection system in which the individual packets flowing through a network are analyzed.

newsgroups – Same as forum, an on-line discussion group.

NIDS – Network intrusion detection.

nmap – a program which conducts a probe of your computer for open ports.

NSA – The National Security Agency is the United States' cryptologic organization. It coordinates, directs, and performs highly specialized activities to protect US information systems and produce foreign intelligence information.

open (ports) – ports for which all packets that is directed to that port are allowed through (see filtered ports).

operating system – The underlying program that runs on a computer. Every general-purpose computer must have an operating system to run other programs. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers. Some Operating Systems are Windows, Linux and UNIX.

P2P – Peer-to-peer.

packet sniffer – A program and/or device that monitors data traveling over a network.

packets – A piece of a message transmitted over a packet-switching network.

password cracking – the process of attempting to determine an unknown password.

peer-to-peer (P2P) – a type of network in which each workstation has equivalent capabilities and responsibilities.

ping – A utility to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply.

Plain Old Telephone Service (POTS) – Used to describe basic, old-fashioned telephone service.

POP – Post Office Protocol, a protocol used to retrieve e-mail from a mail server. Most e-mail applications (sometimes called an e-mail client) use the POP protocol, although some can use the newer IMAP (Internet Message Access Protocol).

ports – An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

POTS – Plain old telephone service.

ppp – Point-to-Point Protocol, a method of connecting a computer to the Internet. PPP is more stable than the older SLIP protocol and provides error checking features.

privileged access – A privilege to use computer information in some manner. For example, a user might be granted read access to a file, meaning that the user can read the file but cannot modify or delete it. Most operating systems have several different types of access privileges that can be granted or denied to specific users or groups of users.

protocol – An agreed-upon format for transmitting data between two devices.

RAM (Random Access Memory) – a type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes.

rootkits – malware that creates a method to retain access to a machine.

router – A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect. Routers use headers and forwarding tables to determine the best path for forwarding the packets, and they use protocols such as ICMP to communicate with each other and configure the best route between any two hosts.

routing table – In internet working, the process of moving a packet of data from source to destination. Routing is usually performed by a dedicated device called a router.

sandbox – A security measure in the Java development environment. The sandbox is a set of rules that are used when creating an applet that prevents certain functions when the applet is sent as part of a Web page.

script kiddie – A person who runs hacking tools without knowing how or why they work.

sectors – The smallest unit that can be accessed on a disk.

Secure Shell – A protocol designed as a more secure replacement for telnet.

Server – A program on a remote computer that is used to provide data to a local computer, see client.

Services - Network services allow local computers to exchange information with remote computers.

SMTP – Simple Mail Transfer Protocol, a protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP

social engineering – The act of obtaining or attempting to obtain otherwise secure data by conning an individual into revealing secure information.

spyware – Any software that covertly gathers user information through the user's Internet connection without his or her knowledge

SSH – Secure Shell, a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

switch – In networks, a device that filters and forwards packets between LAN segments.

TCP – Transmission Control Protocol. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

TCP/IP – Transmission Control Protocol/Internet Protocol. The suite of communications protocols used to connect hosts on the Internet.

tcpdump – a packet sniffer that records traffic on your computer.

Telnet – a protocol that allows a local user to connect to a remote computer and access its resources.

timebombs – code designed to execute at a specific time on a network or computer, for example when the expiration date is reached on a trial software.

topologies – The shape of a local-area network (LAN) or other communications system.

tracert – A utility that traces a packet from your computer to an Internet host, showing how many hops the packet requires to reach the host and how long each hop takes.

tracks – A ring on a disk where data can be written. A typical floppy disk has 80 (double-density) or 160 (high-density) tracks. For hard disks, each platter is divided into tracks, and a single track location that cuts through all platters (and both sides of each platter) is called a cylinder. Hard disks have many thousands of cylinders.

trojans – A destructive program that masquerades as a benign application. Unlike viruses, Trojans do not replicate themselves but they can be just as destructive.

Web Browser – a program that allows users to connect to web servers and view the pages stored on them.

Web Server – A computer where web pages are kept to be accessed by other computers.

weblogs (blogs) – Web page that serves as a publicly accessible personal journal for an individual.

Whois – An Internet utility that returns information about a domain name or IP address.

World Wide Web (www)– A service for the transmission and presentation of hypertext.

worms – A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.

zine – Small, often free magazine, usually produced by hobbyists and amateur journalists.