Network Security Tools

General Project Description:

Your task is to learn an application that is useful in network security and create a powerpoint that identifies the specific steps showing how to do something specific using that tool.

Crackers use software tools that are commonly developed by other crackers for their own purposes. Crackers hear about these tools by word of mouth, often in online forums and chat rooms. These software tools often do not have written manuals to guide new users on how they are used. Sometimes they do have brief and incomplete help files, but these usually assume a good deal of pre-knowledge about the subject.

Learning these software tools is a difficult task for those in charge of network security who want to test the vulnerability of their own networks. For your project, do not rely solely on the help file, if one is provided. Spend time exploring the application. Look for Internet sites that might be helpful. Be sure to talk to people, such as network administrators, who may use or know about your application or applications similar to yours. Explore forums on the Internet where you can post questions and seek answers.

Your task in this assignment is two-fold:

1) You must learn how to use one software tool from the proposed list (below). Understand and be able to demonstrate in your project one pre-approved objective for the application.

2) You will prepare a powerpoint presentation that you will upload to our Blackboard course (Digital DropBox). The presentation should include the following required information (the last item below is optional):

- Name of software
- Name of software developer
- Software version
- URL of software download
- Operating System Platform(s) on which the application will run
- Other software which must be installed on the computer for the application to run and the URL for downloading that additional software
- Application category (sniffer, keylogger, remote access, etc)
- Purpose of software (To spoof an IP address, to capture a password, etc) that you are demonstrating. This should be a simple statement, in general terms. A sentence or two is fine.

- Step-by-step directions for your demonstration. You do not need to include installation directions for the application unless there are special issues, features that need to be enabled during installation, etc. In other words, anything that deviates from a default installation needs to be covered in your demonstration. Default installations do not need to be included in the demonstration.

  Reminder: Do not copy/paste information for your PowerPoint slides. Use your own words.

- Optional: Useful charts (such as port numbers), lists (of protocols, types of encryption, etc), or other information helpful to the user for the specific purpose you are demonstrating.

To select an application tool and obtain pre-approval for a tool objective:

1. Review the Application List carefully. Consider all the implications of choosing a particular application tool, including the operating system and any hardware requirements. Once you are assigned an application, there will be no changes. No exceptions.

2. Go to the Application Tool Discussion Board and review previous posts to see if anyone has previously been assigned an application tool of interest to you. Since applications are assigned on a first come first served basis, have a second and third choice in mind if needed. Once an application is approved by one student, it cannot be chosen by another student. (Note: if a student request for an application tool is denied, the application tool becomes available again to any student).

3. Send an email to your instructor that you are submitting a post in the Forum.

4. Go to the Forum to Request Project Approval In the subject of the post, include the name of the application tool you are requesting be assigned to you. Include the version.

5. In the content area of your post, state what objective you will be demonstrating. Be specific. Example 1: Using this tool I will demonstrate how to recover a lost password. Example 2: Using this tool I will demonstrate how to view information in a packet crossing through a network. Example 3: Using this tool I will demonstrate how to locate unadvertised networks.

6. Your instructor will post a reply to your post, indicating that your request is “Approved” or “Denied” or “Question”.
    a. If approved, you may schedule when to present your project (see below for specific directions). You may begin working on your project.
    b. If denied, an explanation for the denial will be provided. You might still be able to construct a project with that tool if you can correct the reason for the denial. Think through an appropriate correction and resubmit your request as a reply post -or- request a different tool in a NEW post.
    c. If the instructor has a question, please answer promptly. A request with a question is pending until the question is resolved.

Application List

Achilles
Achilles is a tool designed for testing the security of web applications. Achilles is a proxy server, which acts as a man-in-the-middle during an HTTP session. A typical HTTP proxy will relay packets to and from a client browser and a web server. Achilles will intercept an HTTP session's data in either direction and give the user the ability to alter the data before transmission. For example, during a normal HTTP SSL connection a typical proxy will relay the session between the server and the client and allow the two end nodes to negotiate SSL. In contrast, when in intercept mode, Achilles will pretend to be the server and negotiate two SSL sessions, one with the client browser and another with the web server. As data is transmitted between the two nodes, Achilles decrypts the data and gives the user the ability to alter and/or log the data in clear text before transmission.

Analyzer
Analyzer is a full configurable network analyzer program for Win32 environment. Analyzer is able to capture packets on all platforms (and link-layer technologies) supported by WinPcap, except for Windows 95.

Arpwatch
Keeps track of ethernet/ip address pairings and can detect certain types of foul play.

ASP
Send certificate-based secure email in just a few lines of ASP code.

Big Brother
Big Brother is designed to let anyone see how their network is doing in near real-time, from any web browser, anywhere.

Blast
A small, quick TCP service stress test tool.

Brutus
This Windows-only cracker bangs against network services of remote systems trying to guess passwords by using a dictionary and permutations thereof. It supports HTTP, POP3, FTP, SMB, TELNET, IMAP, NTP, and more. No source code is available.

BTScanner
Btscanner allows you to extract as much information as possible from a Bluetooth device without the requirement to pair. It extracts HCI and SDP information, and maintains an open connection to monitor the RSSI and link quality.

Cheops / cheops-ng
Gives a simple interface to many network utilities, maps local or remote networks and identifies OS of machines.

DSniff
This popular and well-engineered suite includes many tools, such as dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy which passively monitor a network for interesting data (passwords, e-mail, files, etc.). arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker due to layer-2 switching. sshmitm and webmitm implement active monkey-in-the-middle attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI. A separately maintained partial Windows port is available.

Ecora NetExplorer
Automatically discover what's connected to your network for an instant inventory of your IT infrastructure. Scan ports to find what is running on each machine and which ports are open to eliminate potential security holes.

Enigma
Encrypting files will guarantee your privacy and keep your documents private.

Ettercap
Ettercap is a terminal-based network sniffer/interceptor/logger for ethernet LANs. It supports active and passive dissection of many protocols (even ciphered ones, like SSH and HTTPS). Data injection in an established connection, and filtering on the fly is also possible, keeping the connection synchronized. Many sniffing modes are implemented. Plugins are supported. It has the ability to check if you are in a switched LAN and to use OS fingerprints (active or passive) to reveal the topology of the LAN.

Evidence Eliminator
This software can be used to protect your PC from investigations.

Foundstone Forensic Toolkit
This tool is a file properties analyzer. Examine the files on a disk drive for unauthorized activity. Lists files by their last access time, search for access times between certain time frames, scan the disk for hidden files, data streams. Dump file and security attributes. Report on audited files. Discover altered ACL's. See if a server reveals too much info via NULL sessions.

FPipe
FPipe is a source port forwarder/redirector. It can create a TCP or UDP stream with a source port of your choice. This is useful for getting past firewalls that allow traffic with source ports of say 23, to connect with internal servers.

Fport
fport reports all open TCP/IP and UDP ports on the machine you run it on and shows what application opened each port. It can be used to quickly identify unknown open ports and their associated applications.

Fragroute
Fragroute intercepts, modifies, and rewrites egress traffic, implementing most of the attacks described in the Secure Networks IDS Evasion paper. It features a simple rule set language to delay, duplicate, drop, fragment, overlap, print, reorder, segment, source-route, or otherwise monkey with all outbound packets destined for a target host, with minimal support for randomized or probabilistic behavior. This tool was written in good faith to aid in the testing of intrusion detection systems, firewalls, and basic TCP/IP stack behavior.

Hfnetchk
This is a Microsoft tool for checking the patch status of all the Windows machines on a network from a central location.

Honeyd
Honeyd is a small daemon that creates virtual hosts on a network. The hosts can be configured to run arbitrary services, and their TCP personality can be adapted so that they appear to be running certain versions of operating systems. Honeyd enables a single host to claim multiple addresses on a LAN for network simulation. It is possible to ping the virtual machines or to traceroute them. Any type of service on the virtual machine can be simulated according to a simple configuration file. It is also possible to proxy services to another machine rather than simulating them. The web page is currently down for legal reasons, but the V. 0.5 tarball is still available.

IpTraf
IP network monitoring software.

John the Ripper
John the Ripper is a fast password cracker, currently available for many flavors of Unix, DOS, Win32, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. It supports several crypt(3) password hash types which are most commonly found on various Unix flavors, as well as Kerberos AFS and Windows NT/2000/XP LM hashes. Several other hash types are added with contributed patches.

Kismet
Kismet is an 802.11b network sniffer and network dissector. It is capable of sniffing using most wireless cards, automatic network IP block detection via UDP, ARP, and DHCP packets, Cisco equipment lists via Cisco Discovery Protocol, weak cryptographic packet logging, and Ethereal and tcpdump compatible packet dump files. It also includes the ability to plot detected networks and estimated network ranges on downloaded maps or user supplied image files. Windows support is currently preliminary.

Knoppix
Internet connection software with utilities for data recovery and system repairs for many different operating systems, including network and security analysis tools for network administrators and more than 900 installed software packages with over 2000 executable user programs & utilities.

NBTScan
NBTscan is a program for scanning IP networks for NetBIOS name information. It sends NetBIOS status query to each address in supplied range and lists received information in human readable form. For each responded host it lists IP address, NetBIOS computer name, logged-in user name and MAC address.

Nemesis
The Nemesis Project is designed to be a command line based, portable human IP stack for UNIX/Linux (and now Windows!). The suite is broken down by protocol and should allow for useful scripting of injected packet streams from simple shell scripts. If you enjoy Nemesis, you might also want to look at hping2. They complement each other well.

NetCat
A simple Unix utility which reads and writes data across network connections, using TCP or UDP protocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and exploration tool, since it can create almost any kind of connection you would need and has several interesting built-in capabilities.

Network Stumbler
Netstumbler is the best known Windows tool for finding open wireless access points ("wardriving"). A WinCE version for PDAs called Ministumbler is also distributed. The tool is currently free, but Windows-only and no source code is provided. The author reserves the right to change this license agreement as he sees fit, without notice.

NGrep
ngrep strives to provide most of GNU grep's common features, applying them to the network layer. ngrep is a pcap-aware tool that will allow you to specify extended regular or hexadecimal expressions to match against data payloads of packets. It currently recognizes TCP, UDP and ICMP across Ethernet, PPP, SLIP, FDDI, Token Ring and null interfaces, and understands bpf filter logic in the same fashion as more common packet sniffing tools, such as tcpdump and snoop.

Nikto
Nikto is a web server scanner which looks for over 2000 potentially dangerous files/CGIs and problems on over 200 servers.

NTLast
Security log analyzer. Identify and track who has gained access to your system, then document the details---Enhanced audit/tracking features, such as reading saved files. Includes raw time output for Excel analysis and many more additional features for Webmasters.

NTop
Ntop shows network usage. In interactive mode, it displays the network status on the user's terminal. In Web mode, it acts as a Web server, creating an HTML dump of the network status. It sports a NetFlow/sFlow emitter/collector, an HTTP-based client interface for creating ntop-centric monitoring applications, and RRD for persistently storing traffic statistics.

Pstools
A suite of free command-line tools for managing Windows systems (process listings, command execution, etc)

puTTY
Ssh (Secure Shell) is a program for logging into or executing commands on a remote machine. It provides secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel. It is intended as a

replacement for rlogin, rsh and rcp, and can be used to provide rdist and rsync with a secure communication channel.

Redfang
Redfang v2.5 is an enhanced version from @Stake of the original Redfang application that finds non-discoverable Bluetooth devices by brute-forcing the last six bytes of the device's Bluetooth address and doing a read_remote_name().

SafeGuard Easy
Full Hard Disk Encryption to protect 100% of your system and data.

Sam Spade
SamSpade provides a consistent GUI and implementation for many handy network query tasks. It was designed with tracking down spammers but can be useful for many other network exploration, administration, and security tasks. It includes tools such as ping, nslookup, whois, dig, traceroute, finger, raw HTTP web browser, DNS zone transfer, SMTP relay check, website search, and more.

Sniphere
Sniphere is an another network wiretapping program for Windows using winpcap. Nevertheless, Sniphere is a pretty handy program with a lot of possibilities which most of free sniffers do not have.

SPIKE Proxy
Spike Proxy is an open source HTTP proxy for finding security flaws in web sites. It is part of the Spike Application Testing Suite and supports automated SQL injection detection, web site crawling, login form brute forcing, overflow detection, and directory traversal detection.

SSID Sniff
A tool to use when looking to discover access points and save captured traffic. Comes with a configured script and supports Cisco Aironet and random prism2 based cards.

SuperScan
A connect-based TCP port scanner, pinger and hostname resolver. No source code is provided. It can handle ping scans and port scans using specified IP ranges. It can also connect to any discovered open port using user-specified "helper" applications (e.g. Telnet, Web browser, FTP).

UserDump
UserDump is UserInfo with a twist. It combines LookupAccountSID and LookupAccountName with UserInfo's NetGetUserInfo calls, resulting in a SID Walker that can dump every user in a domain in a single command line.

WEPCrack
WEPCrack was the first of the WEP encryption cracking utilities. WEPCrack is an open-source tool used to break 802.11 WEP keys. Also available for Linux.

Whisker/Libwhisker
Whisker is a scanner which allows you to test HTTP servers for many known security holes, particularly the presence of dangerous CGIs. Libwhisker is a perl library (used by Whisker) which allows for the creation of custom HTTP scanners.

wIDS
wIDS is a wireless IDS. It detects the jamming of management frames and could be used as a wireless honeypot. Data frames can also be decrypted on the fly and re-injected onto another device.

WIDZ
WIDZ is a proof of concept IDS system for 802.11 wireless networks. It guards access points (AP's) and monitors local frequencies for malicious activity. It detects scans, association floods, and bogus/Rogue AP's. It can also be integrated with SNORT or RealSecure.

Winfingerprint
A Win32 Host/Network Enumeration Scanner

Zx Sniffer
Shows network traffic like ICMP, IGMP, UDP and TCP. Intercepts and decodes passwords of POP3, FTP, ICQ, Basic Proxy and Web Authorization.