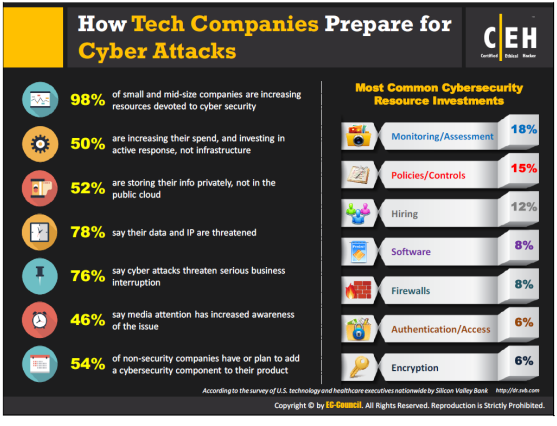
Scanning Networks

Module 03

Ethical Hacking and Countermeasures v9

Module 03: Scanning Networks

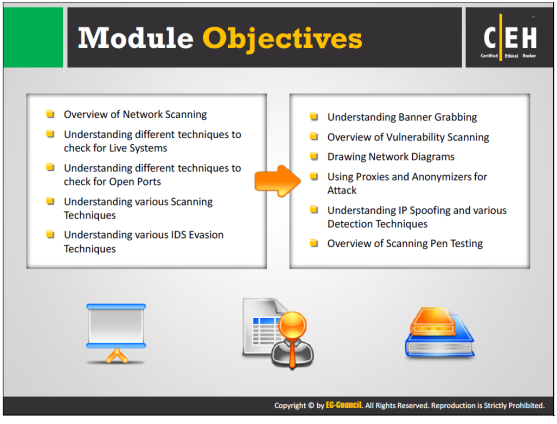
Exam 312-50



With no doubt, hackers are becoming more powerful, educated, and mission driven. They are increasingly discovering and implementing new attack vectors to exploit and tools to attack their target organizations, thereby making it difficult for security professionals to defend their organizations.

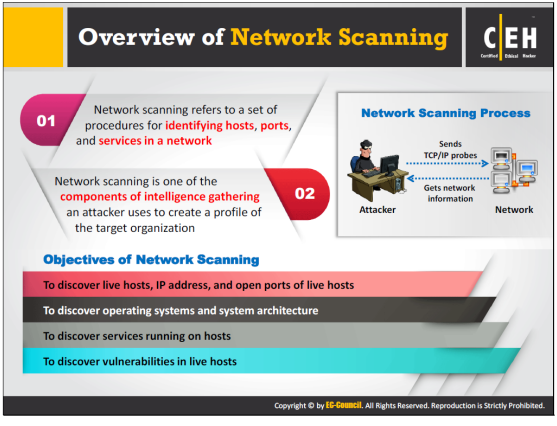
Media are playing a key role in making organizations aware of cyber attacks around the world. According to a survey conducted by Silicon Valley Bank in 2014, 76% of tech companies say cyber attacks threaten serious business interruption. Because of such threats, 98% of small and midsize companies are increasing resources devoted to cyber security. Organizations are investing more money on defense strategies rather than infrastructure: monitoring/ assessment accounts for 18% of these investments, while policies/controls account for 15%.

Source: http://dr.svb.com



After identifying the target system and performing the initial reconnaissance, as discussed in the Footprinting and Reconnaissance module, attackers begin to search for an entry point into the target system. You should note that the scanning itself is not the actual intrusion, but rather an extended form of reconnaissance in which the attacker learns more about his/her target, including information about operating systems, services, and any configuration lapses. The information gleaned from this reconnaissance helps the attacker select strategies for the attack on the target system or network.

This module starts with an overview of network scanning, and provides an insight into various techniques to check for live systems and open ports. It goes on to discuss various scanning techniques, and ends with an overview of pen-testing steps that an ethical hacker should follow to perform the security assessment of the target.



As already discussed, footprinting is the first phase of hacking, in which the attacker gains primary information about a potential target. He/she then uses this information in the scanning phase in order to gather much more detailed information about the target.

Scanning is the process of gathering additional detailed information about the target using highly complex and aggressive reconnaissance techniques. It is one of the most important phases of intelligence gathering for an attacker. In the process of scanning, the attacker tries to gather information, including the specific IP addresses that can be accessed over the network, the target's operating systems and system architecture, and the services running on each computer.

The purpose of scanning is to discover exploitable communications channels, probe as many listeners as possible, and keep track of the ones that are responsive or useful to an attacker's particular needs. In the scanning phase of an attack, the attacker tries to find various ways to intrude into a target system. The attacker also tries to discover more about the target system, including whether or not there are any configuration lapses in the target system. The attacker then uses the information gleaned during the scan to develop an attack strategy.

Types of Scanning

- **Port scanning** – Lists the open ports and services. Port scanning is the process of checking the services running on the target computer by sending a sequence of messages in an attempt to break in. Port scanning involves connecting to or probing TCP and UDP ports on the target system to determine if the services are running or are in a

listening state. The listening state provides information about the operating system and the application currently in use. Sometimes, active services that are listening may allow unauthorized user access to misconfigure systems or running software with vulnerabilities.

- **Network scanning** – Lists IP addresses. Network scanning is a procedure for identifying active hosts on a network, either to attack them or as a network security assessment.
- **Vulnerability scanning** – Shows the presence of known weaknesses. Vulnerability scanning is a method used to check whether a system is exploitable by identifying its vulnerabilities. A vulnerability scanner consists of a scanning engine and a catalog. The catalog consists of a list of common files with known vulnerabilities and common exploits for a range of servers. A vulnerability scanner may look for backup files or directory traversal exploits, for example. The scanning engine maintains logic for reading the exploit list, transferring the request to the Web server and analyzing the requests to ensure the safety of the server. These tools generally target vulnerabilities that secure host configurations can fix easily, updated security patches, and a clean Web document.

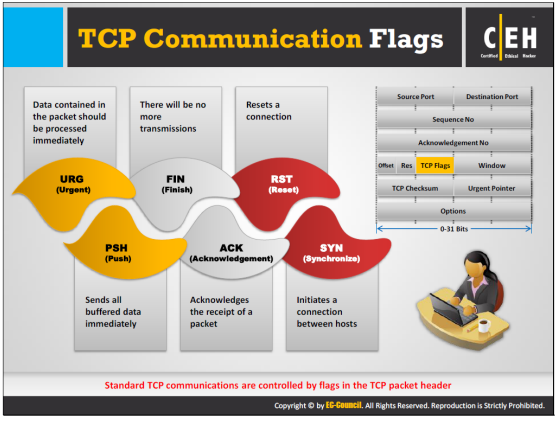
The access points that a thief who wants to break into a house looks for are the doors and windows. These are usually the house's points of vulnerability, as they are easily accessible. When it comes to computer systems and networks, ports are the doors and windows of the system that an intruder uses to gain access. A general rule for computer systems is that the more open ports there are on a system, the more vulnerable the system. There are cases, however, in which a system has fewer ports open than another machine, but the open ports present a much higher level of vulnerability.

Objectives of Network Scanning

The more information there is at hand about a target organization, the greater the chances are of knowing a network's security loopholes and consequently, for gaining unauthorized access to it.

Below are some objectives for scanning a network:

- Discover the network's live hosts, IP addresses, and open ports of live. Using open ports, the attacker will determine the best means of entry into the system.
- Discover the operating system and system architecture of the target. This is also known as fingerprinting. From the operating system's vulnerabilities, an attacker will formulate an attack strategy.
- Discover the services running/listening on the target system. Doing so gives the attacker an indication of vulnerabilities (based on the service) exploitation for gaining access to the target system.
- Identify specific applications or versions of a particular service.
- Identify vulnerabilities in any of the network systems. This helps an attacker to compromise the target system or network through various exploits.



TCP header contains various flags that control the transmission of data across a TCP connection. There are six TCP control flags that manage the connection between hosts and give instructions to the system. Four of these flags govern the establishment, maintenance, and termination of a connection: SYN, ACK, FIN, and RST. The other two flags provide instructions to the system: PSH and URG. The size of each flag is 1 bit. As there are six flags in the TCP Flags section, the size of this section is 6 bits. When a flag value is set to "1," that flag is turned on.

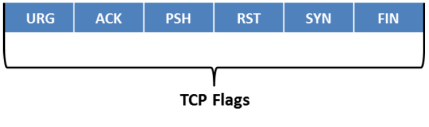


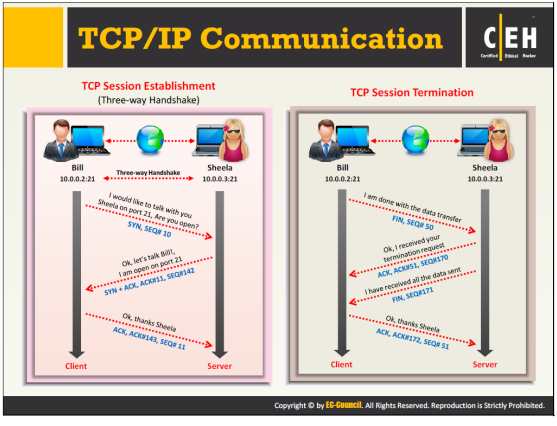
FIGURE 3.1: TCP Communication Flags

The following are the TCP communication flags:

- Synchronize alias "SYN": Notifies transmission of a new sequence number. These flags generally represent establishment of a connection (3-way handshake) between two hosts and terminating the connection.

- Acknowledgement alias "ACK": Confirms receipt of transmission, and identifies next expected sequence number. When the system successfully receives a packet, it sets the value of its flag to "1," implying that the receiver should pay attention to it.
- Push alias "PSH": When its flag is to "1," it indicates that the sender has raised the push operation to the receiver; which means the remote system should inform the receiving application about the buffered data coming from the sender. The system raises the PSH flag at the time of start and end of data transfer, and sets it on the last segment of a file to prevent buffer deadlocks.
- Urgent alias "URG": Instructs the system to process the data contained in packets as soon as possible. When the system sets the flag to "1," the remote system gives priority to the urgent data and processes it first, stopping all the other data processing.
- Finish alias "FIN": Its flag is set to "1" to announce that it will not send more transmissions to remote system, and terminates the connection established by the SYN flag.
- Reset alias "RST": When there is an error in the current connection, its flag is set to "1," and it aborts the connection in response to the error. Attackers make use of this to scan hosts in search of open ports.

SYN scanning mainly deals with three of the flags: SYN, ACK, and RST. You can use these three flags for gathering illegal information from servers during the enumeration process.



TCP is connection-oriented, which prioritizes connection establishment before data transfer between applications. This connection between protocols is possible through the process of the three-way handshake.

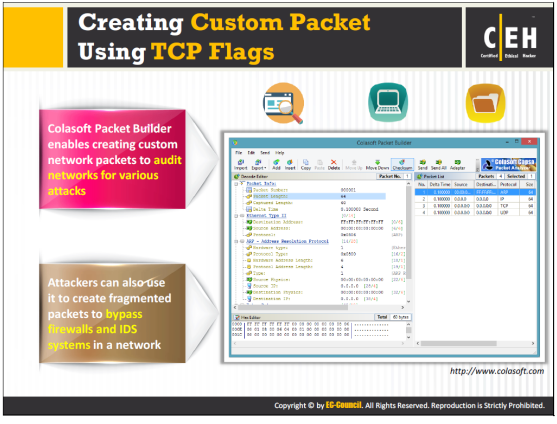
TCP Session initiates using a three-way handshake mechanism:

- To launch a TCP connection, the source (10.0.0.2: 21) sends a SYN packet to the destination (10.0.0.3:21).
- The destination, on receiving the SYN packet, responds by sending a SYN/ACK packet back to the source.
- The ACK packet confirms the arrival of the first SYN packet to the source.
- To conclude, the source sends an ACK packet for the ACK/SYN packet sent by the destination.
- This triggers an "OPEN" connection, allowing communication between the source and the destination, until one of them issues a "FIN" or "RST" packet to close the connection.

The TCP protocol maintains stateful connections for all connection-oriented protocols throughout the Internet, and works the same as an ordinary telephone communication, in which one picks up a telephone receiver, hears a dial tone, and dials a number that triggers ringing at the other end, until a person picks up the receiver and says, “Hello.”

The system terminates the established TCP Session as follows:

After completing all the data transfers through established TCP connection, the sender sends the connection termination request to the receiver by sending a FIN or RST packet. On receiving the connection termination request, the receiver acknowledges the termination requests by sending ACK packet to the sender; then the system will terminate the established connection.



Colasoft Packet Builder is a tool that allows an attacker to create custom network packets and helps security professionals to assess the network. The attacker can select a TCP packet from the provided templates and change the parameters in the decoder editor, hexadecimal editor, or ASCII editor to create a packet. In addition to building packets, Colasoft Packet Builder also supports saving packets to packet files and sending packets to the network.

There are three views in the Packet Builder: Packet List, Decode Editor, and Hex Editor.

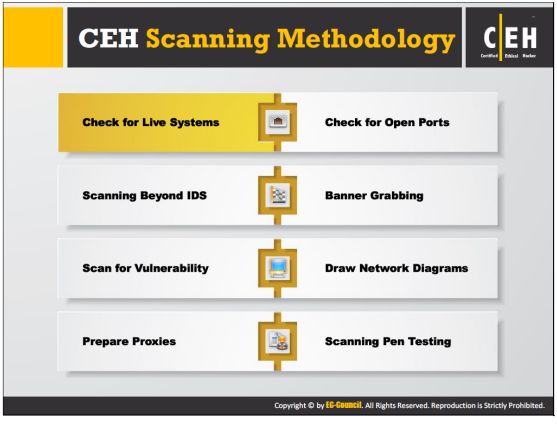
- The Packet List displays all constructed packets. When you select one or more packets in Packet List, the first highlighted packet displays in both Decode Editor and Hex Editor for editing.
- In the Hex Editor, the data of the packet are represented as hexadecimal values and ASCII characters; nonprintable characters are represented by a dot (".") in the ASCII section. You can edit either the hexadecimal values or the ASCII characters.
- Decode editor allows the attacker to edit packets without remembering value length, byte order, and offsets. You can select a field and change value in the edit box.

For creating a packet, you can use the add or insert packet command in the Edit menu or on the Toolbar to create a new packet.

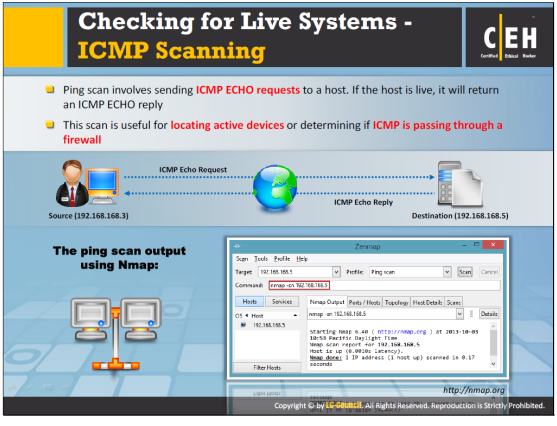
The attacker can send a constructed packet to wire directly, and control how Colasoft Packet Builder sends the packets, specifying, for example, the interval between every packet, loop times, and the delay time between loops.

This packet builder audits networks and checks network protection against attacks and intruders. Attackers may use this packet builder to create fragmented packets to bypass network firewalls and IDS systems. They can also create packets and flood the victim with a very large number of packets, which could result in denial-of-service attacks.

Source: *http://www.colasoft.com*



The first step in scanning networks is to check for live systems. This section highlights how to check for live systems with the help of ICMP scanning, how to ping a system, and various ping sweep tools.



ICMP Scanning

Attackers send ICMP packets to the system to gather all necessary information about it, in a process known as ICMP scanning. Because ICMP does not have a port abstraction, this is not the same as port scanning. However, it is useful to determine what hosts in a network are running by pinging them all (NMAP uses the -P option to ICMP-scan in parallel, which can happen quickly). The user can also increase the number of pings in parallel using the -L option. It can also be helpful to tweak the ping timeout value using the -T option.

ICMP Query

The UNIX tool ICMPquery or ICMPush requests the system time (to learn the system time zone) by sending an ICMP type 13 message (TIMESTAMP). The netmask on a particular system can also be determined using ICMP type 17 messages (ADDRESS MARK REQUEST). After finding the netmask of a network card, a user can determine all the subnets in use. Then, the user can target only one particular subnet and avoid hitting the broadcast addresses.

ICMPquery has both a timestamp and address mask request option:

```
icmp query <-query-> [-B] [-f fromhost] [-d delay] [-T time] target
```

Where,

<query> is one of:

-t: icmp timestamp request (default)

-m: icmp address mask request

-d: delay to sleep between packets is in microseconds

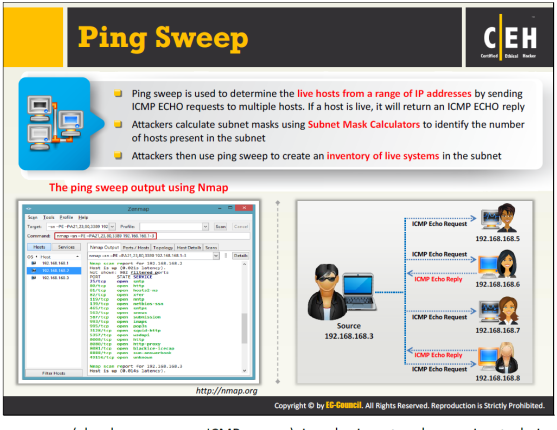
-T - specifies the number of seconds to wait for a host to respond. The default is 5. A **target** is a list of hostnames or addresses.

Ping Scan Output Using Nmap

Source: http://nmap.org

Nmap helps to perform ping scan, also known as host discovery. Ping scan works by sending ICMP ECHO requests to a network host. If the host is live, it will return an ICMP ECHO reply. Using this tool, one can locate live hosts on a network or determine if ICMP is passing through a firewall.

The screenshot shown in the slide below displays the results of a ping scan using Zenmap, the official cross-platform GUI for the Nmap Security Scanner.



A ping sweep (also known as an ICMP sweep) is a basic network scanning technique to determine which range of IP addresses map to live hosts (computers). Although a single ping will tell the user whether one specified host computer exists on the network, a ping sweep consists of ICMP ECHO requests sent to multiple hosts.

If a specified host is active, it will return an ICMP ECHO reply. Ping sweeps are among the oldest and slowest methods used to scan a network. This utility, distributed across almost all platforms, acts like a roll call for systems; a system that is active on the network answers the ping query that another system sends out.

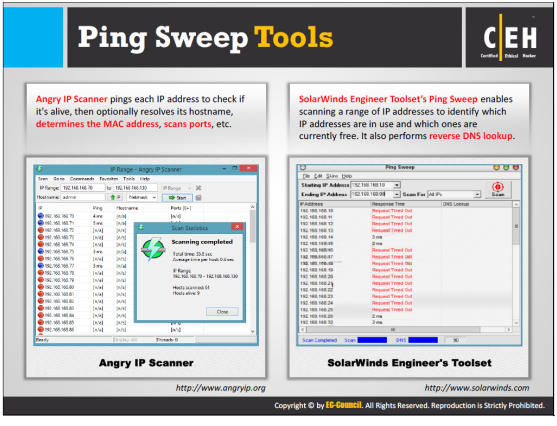
To understand pings better, one should be able to understand the TCP/IP packet. When a system pings, it sends a single packet across the network to a specific IP address. This packet contains 64 bytes (56 data bytes and 8 bytes of protocol header information). The sender then waits or listens for a return packet from the target system. If the connections are good and the target computer is "alive," a good return packet is expected. However, if there is a disruption in the communication, this will not be the case. Ping also details the amount of time it takes for a packet to make the complete trip called the round-trip time. Ping also helps for resolving host names. In this case, if the packet bounces back when sent to the IP address, but not when sent to the name, then the system is unable to resolve the name to the specific IP address.

Ping Sweep Output Using Nmap

Source: *http://nmap.org*

Nmap helps to perform a ping sweep that determines live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts. Live hosts send an ICMP ECHO reply. A ping sweep helps an attacker to create an inventory of live systems in the subnet.

The screenshot shown in the slide below displays the results of a ping sweep using Zenmap, the official cross-platform GUI of the Nmap Security Scanner.



Given below are ping sweep tools that help to determine live hosts on the target network by sending multiple ICMP ECHO requests to multiple hosts on the network at a time.

Angry IP Scanner

Source: *http://www.angryip.org*

Angry IP scanner is an IP address and port scanner. It can scan IP addresses in any range as well as any of their ports. It pings each IP address to check if it is alive, then optionally resolves its hostname, determines the MAC address, scans ports, and so on. The amount of gathered data about each host extends with plugins. Angry IP scanner has additional features, such as NetBIOS information (computer name, workgroup name, and currently logged in Windows user), favorite IP address ranges, web server detection, and customizable openers. The tool allows the user to save the Scanning results to CSV, TXT, XML, or IP-Port list files. To increase scanning speed, it uses a multithreaded approach: a separate scanning thread created for each scanned IP address.

SolarWinds Engineer's Toolset

Source: *http://www.solarwinds.com*

The SolarWinds Engineer's Toolset is a collection of network management tools that allows one to monitor and troubleshoot the network.

Tool categories in SolarWinds Engineer's Toolset:

- Intuitive Web Console

- Toolkit Administrator
- Configuration Management
- Diagnostics
- General/Other
- IPAM/DNS/DHCP
- Log Management
- Network Discovery
- Network Monitoring
- Security
- SNMP

Network Discovery category in SolarWinds Engineer's Toolset includes a Ping Sweep utility that enables one to scan a range of IP addresses to display which addresses are in use or not in use, and perform reverse DNS lookups.

Described below are a few more ping sweep tools that help to determine live hosts on the target network:

Colasoft Ping Tool

Source: *http://www.colasoft.com*

Colasoft Ping Tool supports ping multiple IP addresses simultaneously and lists comparative responding times in a graphic chart. Colasoft Ping Tool displays the operation and statistic results of ping in three windows:

- **Graphic window**: reveals every single ping command in a graphic way (*X*-axis shows real ping time, *Y*-axis shows ping response time).
- **Ping Summary**: provides basic information such as IP address, locations, packets received/sent/lost, as well as response time of all required IP addresses or domain names.
- **Ping details**: displays all the detailed information of ping execution.

Visual Ping Tester – Standard

Source: *http://www.pingtester.net*

PingTester stores a list of IP addresses and network test commands to increase working efficiency. It performs ping and traceroute test, "ping sweep" subnets or interval ping all the hosts on a list continuously; Saves the individual ping records to a .txt or Excel file and generate

statistics reports which group by specified time interval to know the network connection status of each period. The IP Scanner function can scan a group of IPs to find the IP in use.

Ping Scanner Pro

Source: http://www.digilextechnologies.com

Ping Scanner Pro is a network troubleshooting tool with various features such as IP Scan, IP MultiScan, Traceroute, MAC Address, DNS Lookup, Whois, Subnet Calculator, Finger, Throughput test, NT Users, Windows Network, Network statistics, and so on.

OpUtils

Source: http://www.manageengine.com

Ping Scan utility of OpUtils software sweeps an entire range of IP Addresses to check their availability. The tool uses the basic PING function as a base to perform the sweep.

PingInfoView

Source: http://www.nirsoft.net

PingInfoView is a utility that allows you to ping multiple host names and IP addresses. It automatically pings to all hosts every number of seconds specified and displays the number of successful and failed pings, as well as average ping time. One can save the ping result into text/html/xml file format, or copy it to the clipboard.

Advanced IP Scanner

Source: http://www.radmin.com

Advanced IP Scanner is a network scanner for Windows.

Features:

- Scans multiple IP addresses simultaneously
- Scans ports of network computers and finds HTTP, HTTPS, FTP, and shared folders
- Scans the network (including Wi-Fi) to provide information about all connected devices, including computers' names and MAC addresses
- Allows the waking of any machine, or group of machines, remotely (Wake-On-LAN)
- Shuts down any remote machine, or group of machines, running Windows
- Allows the running of quick commands (ping, tracert, telnet, and SSH) on a remote computer

Ping Sweep

Source: http://www.whatsupgold.com

Ping Sweep Tool is an integrated component of the WhatsUp Gold Engineer's Toolkit.

Features:

- Pings a range of IP addresses to find out which addresses are active/inactive, and to resolve their domain name

- Configure settings such as ping timeout, packet time to live, and the delay between pings

Network Ping

Source: http://www.greenline-soft.com

Network Ping is the network diagnostic utility that allows visual monitoring of computers/devices activity on the network. The notification feature helps to identify the machines ping reply status change by sending emails. This program has custom settings for range of endpoint IP Address (ping timeout, whether to send emails, when to send email notifications, etc.).

Ping Monitor

Source: http://www.niliand.com

Ping Monitor is a host-monitoring tool based on ICMP echo requests (ping).

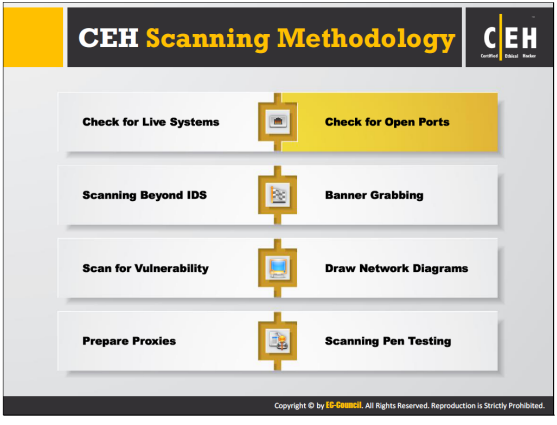
Features:

- Constant monitoring of host or server availability
- Multithreading and several hostnames/IPs to ping simultaneously
- Supports Windows Service mode
- Automatically saves tracert result if a host goes down

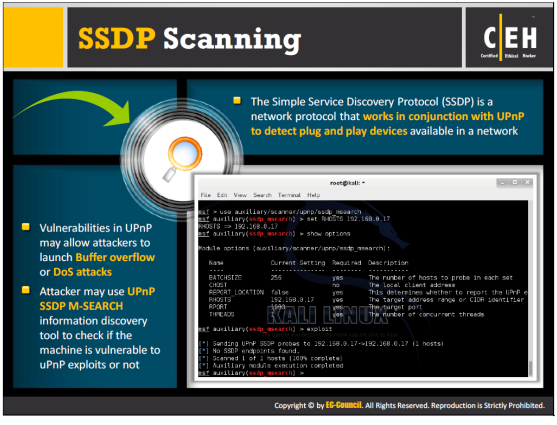
Pinkie

Source: http://www.ipuptime.net

Pinkie is a suite of network troubleshooting tools. Pinkie's PingSweep allows users to sweep an entire subnet or block of addresses for live hosts.

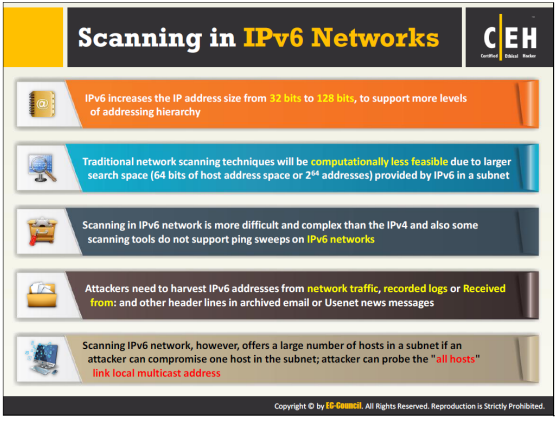


Once the attackers detect live systems in the target network, they try to find open ports in the detected live systems. The next step in the network scanning process involves checking the open ports in live systems. Sometimes users unknowingly keep open unnecessary ports on their systems. Attacker takes advantages of such open ports to launch attacks. This section describes the tools and techniques used by an attacker to do so.

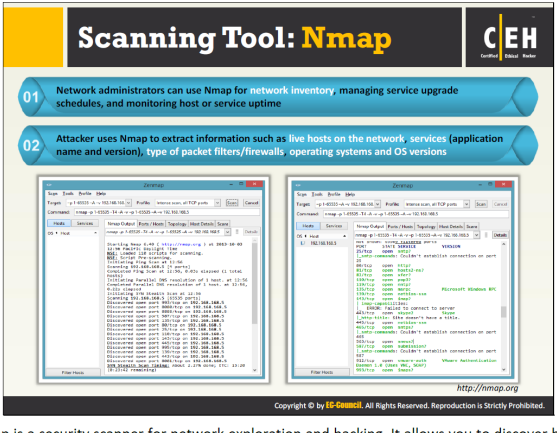


SSDP (Simple Service Discovery Protocol) is a network protocol that generally communicates with machines when querying them with routable IPv4 or IPv6 multicast addresses. The SSDP service controls communication for the Universal Plug and Play feature (uPnP). It generally works when the machine is not firewalled; however, it can sometimes work through a firewall. The SSDP service will respond to the query sent over IPv4 or IPv6 broadcast addresses. This response includes information about the Universal Plug and Play feature (uPnP) associated with it. Attacker uses SSDP scanning to detect UPnP vulnerabilities that may allow him/her to launch buffer overflow or DoS attacks.

The attacker may use the UPnP SSDP M-SEARCH information discovery tool to check whether the machine is vulnerable to uPnP exploits. The UPnP SSDP M-SEARCH information discovery tool gleans information from UPnP-enabled systems as shown in the slide.



IPv6 increases the size of IP address space from 32 bits to 128 bits to support more levels of addressing hierarchy. Traditional network scanning techniques are computationally less feasible because of larger search space (64 bits of host address space, or 2^{64} addresses) provided by IPv6 in a subnet. Scanning an IPv6 network is more difficult and complex than IPv4, and some scanning tools do not support ping sweeps on IPv6 networks. Attackers need to harvest IPv6 addresses from network traffic, recorded logs, or "Received from" and other header lines in archived email or Usenet news messages to identify IPv6 addresses for subsequent port scanning. Scanning an IPv6 network, however, offers a large number of hosts in a subnet; if an attacker can compromise one subnet host, he can probe the "all hosts" link local multicast address, if hosts numbers are sequential, or use any regular scheme. An attacker needs to analyze 2^{64} addresses to check if a particular open service is running on a host in that subnet. At a conservative rate of one probe per second, such a scan would take some 5 billion years to complete.

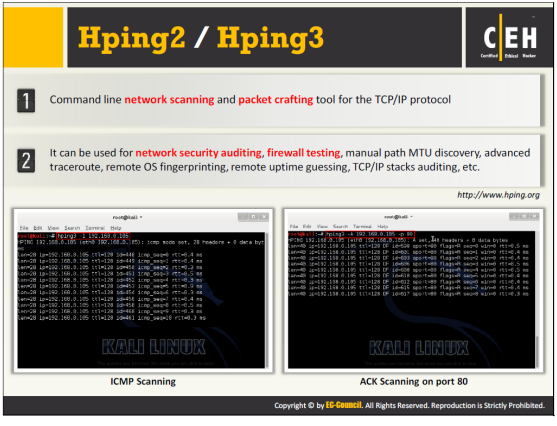


Nmap is a security scanner for network exploration and hacking. It allows you to discover hosts and services on a computer network, thus creating a "map" of the network. It sends specially crafted packets to the target host and then analyzes the responses to accomplish its goal. Either a network administrator or an attacker can use this tool for their particular needs. Network administrators can use Nmap for network inventory, managing service upgrade schedules, and monitoring host or service uptime. Attackers use Nmap to extract information such as live hosts on the network, services (application name and version), type of packet filters/firewalls, operating systems, and OS versions. Nmap includes a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

Some of the features of Nmap include:

- It scans huge networks of literally hundreds of thousands of machines.
- It supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. Nmap includes many port scanning mechanisms (TCP and UDP), OS detection, version detection, ping sweeps, and so on.

Source: http://nmap.org



HPing2/HPing3 is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols. It performs network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, and other functions.

HPing2/HPing3 has a Traceroute mode, and enables you to send files between covert channels. It has the ability to send custom TCP/IP packets and display target replies, as does a ping program with ICMP replies. It handles fragmentation, arbitrary packets' body and size, and uses them to transfer encapsulated files under supported protocols. It supports idle host scanning. IP spoofing and network/host scanning can be used to perform an anonymous probe for services.

An attacker studies the behavior of an idle host to gain information about the target, such as the services that the host offers, the ports supporting the services, and the operating system of the target. This type of scan is a predecessor to either heavier probing or outright attacks.

Features:

The following are some features of HPing2/HPing3:

- Determines whether the host is up even when the host blocks ICMP packets
- Advanced port scanning and test net performance using different protocols, packet sizes, TOS, and fragmentation
- Manual path MTU discovery

- Firewalk-like usage allows discovery of open ports behind firewalls
- Remote OS fingerprinting
- TCP/IP stack auditing

ICMP Scanning

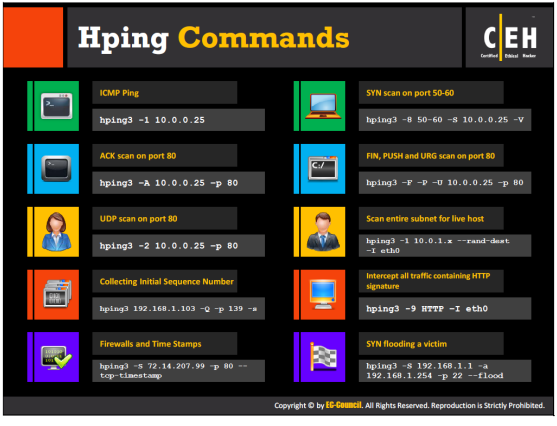
A ping sweep or Internet Control Message Protocol (ICMP) scanning is a process of sending an ICMP request or ping to all hosts on the network to determine which one is up.

Operating system, router, switch, internet-protocol-based devices use this protocol via the ping command to Echo request and Echo response as a connectivity tester between different hosts.

ACK Scanning on Port 80

You can use this scan technique to probe for the existence of a firewall and its rule sets. Simple packet filtering allows you to establish connection (packets with the ACK bit set), whereas a sophisticated stateful firewall does not allow you to establish a connection.

Source: *http://www.hping.org*



Below are various Hping commands:

- **ICMP ping**

  `Ex. hping3 -1 10.0.0.25`

  Hping performs an ICMP ping scan by specifying the argument -1 in the command line. You may use either --icmp of -1 argument in the command line. By issuing the above command, hping sends ICMP-echo request to 10.0.0.25 and receives ICMP-reply, the same as with a ping utility.

- **ACK scan on port 80**

  `Ex. hping3 -A 10.0.0.25 -p 80`

  Hping can be configured to perform an ACK scan by specifying the argument -A in the command line. Here, you are setting ACK flag in the probe packets and performing the scan. You perform this scan when a host does not respond to a ping request.

  By issuing this command, Hping checks if a host is alive on a network. If it finds alive host and an open port, it returns an RST response.

- **UDP scan on port 80**

  `Ex. hping3 -2 10.0.0.25 -p 80`

Hping uses TCP as its default protocol. Using the argument -2 in the command line specifies that Hping operate in UDP mode. You may use either --udp of -2 argument in the command line.

By issuing the above command, Hping sends UDP packets to port 80 on the host (10.0.0.25). It returns an ICMP port unreachable message if it finds the port closed, and does not respond with a message if the port is open.

- **Collecting Initial Sequence Number**

```
Ex. hping3 192.168.1.103 -Q -p 139 -s
```

By using the argument -Q in the command line, Hping collects all the tcp sequence numbers generated by the target host (192.168.1.103).

- **Firewalls and Time Stamps**

```
Ex. hping3 -S 72.14.207.99 -p 80 --tcp-timestamp
```

Many firewalls drop those TCP packets that do not have TCP Timestamp option set. By adding the --tcp-timestamp argument in the command line, you can enable TCP timestamp option in Hping and try to guess the timestamp update frequency and uptime of the target host (72.14.207.99).

- **SYN scan on port 50-60**

```
Ex. hping3 -8 50-60 -S 10.0.0.25 -V
```

By using the argument -8 (or) --scan in the command, you are operating Hping in scan mode in order to scan a range of ports on the target host. Adding the argument -S allows you to perform a SYN scan.

Therefore, the above command performs a SYN scan on ports 50-60 on the target host.

- **FIN, PUSH and URG scan on port 80**

```
Ex. hping3 -F -P -U 10.0.0.25 -p 80
```

By adding the arguments –F, -P, and –U in the command, you are setting FIN, PUSH, and URG packets in the probe packets. By issuing this command, you are performing FIN, PUSH, and URG scans on port 80 on the target host (10.0.0.25). If port 80 is open on the target, you will not receive a response. If the port is closed, Hping returns an RST response.

- **Scan entire subnet for live host**

```
Ex. hping3 -1 10.0.1.x --rand-dest -I eth0
```

By issuing this command, Hping performs an ICMP ping scan on the entire subnet 10.0.1.x; in other words, it sends ICMP-echo request randomly (--rand-dest) to all the hosts from 10.0.1.0 – 10.0.1.255 that are connected to the interface eth0. The hosts whose ports are open will respond with an ICMP-reply. In this case, you haven't set a port, so Hping sends packets to port 0 on all IP addresses by default.

- **Intercept all traffic containing HTTP signature**

  `Ex. hping3 -9 HTTP -I eth0`

  The argument -9 will set the Hping in listen mode. So, by issuing the command -9 HTTP, Hping starts listening on port 0 (of all the devices connected in the network to interface eth0), intercepts all the packets containing HTTP signature and dump from signature end to the packet's end.

  For example, on issuing the command `hping2 -9 HTTP`, if Hping reads a packet that contains data 234-09sdflkjs45-HTTPhello_world, it will display the result as hello_world.

- **SYN flooding a victim**

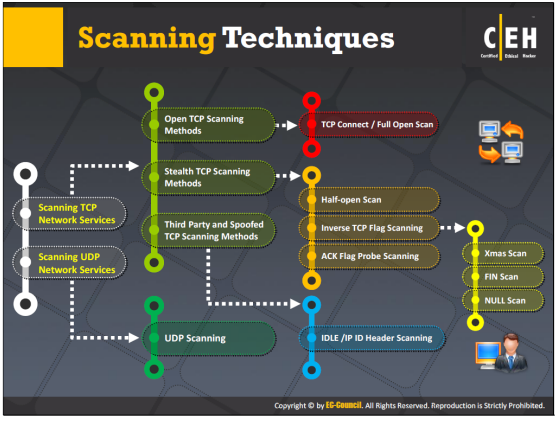
  `Ex. hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood`

  The attacker employs TCP SYN flooding techniques by using spoofed IP addresses to perform DoS attack.

The following table lists the various scanning methods and their respective Hping commands:

Scan	Commands
ICMP ping	`hping3 -1 10.0.0.25`
ACK scan on port 80	`hping3 -A 10.0.0.25 -p 80`
UDP scan on port 80	`hping3 -2 10.0.0.25 -p 80`
Collecting initial sequence number	`hping3 192.168.1.103 -Q -p 139 -s`
Firewalls and time stamps	`hping3 -S 72.14.207.99 -p 80 --tcp-timestamp`
SYN scan on port 50-60	`hping3 -8 50-56 -S 10.0.0.25 -V`
FIN, PUSH and URG scan on port 80	`hping3 -F -P -U 10.0.0.25 -p 80`
Scan entire subnet for live host	`hping3 -1 10.0.1.x --rand-dest -I eth0`
Intercept all traffic containing HTTP signature	`hping3 -9 HTTP -I eth0`
SYN flooding a victim	`hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood`

TABLE 3.1: Hping command and its respective function



Scanning is the process of gathering information about systems that are "alive" and responding on the network.

Port scanning techniques help to identify the open ports on a targeted server or host. Administrators often use port scanning techniques to verify security policies of their networks, whereas attackers use them to identify running services on a host with the intent of compromising the network.

Scanning techniques are further split into two categories as shown in the slide, according to the type of protocol used for communication at the transport layer of the network.

The following is the list of important reserved ports:

Name	Port/Protocol	Description
echo	7/tcp	
echo	7/udp	
discard	9/tcp	sink null
discard	9/udp	sink null
systat	11/tcp	Users
daytime	13/tcp	

daytime	13/udp	
netstat	15/tcp	
qotd	17/tcp	Quote
chargen	19/tcp	ttytst source
chargen	19/udp	ttytst source
ftp-data	20/tcp	ftp data transfer
ftp	21/tcp	ftp command
ssh	22/tcp	Secure Shell
telnet	23/tcp	
smtp	25/tcp	Mail
time	37/tcp	Timeserver
time	37/udp	Timeserver
rlp	39/udp	resource location
nicname	43/tcp	who is
domain	53/tcp	domain name server
domain	53/udp	domain name server
sql*net	66/tcp	Oracle SQL*net
sql*net	66/udp	Oracle SQL*net
bootps	67/tcp	bootp server
bootps	67/udp	bootp server
bootpc	68/tcp	bootp client
bootpc	68/udp	bootp client
tftp	69/tcp	Trivial File Transfer
tftp	69/udp	Trivial File Transfer
gopher	70/tcp	gopher server
finger	79/tcp	Finger
www-http	80/tcp	WWW
www-http	80/udp	WWW
kerberos	88/tcp	Kerberos

kerberos	88/udp	Kerberos
pop2	109/tcp	PostOffice V.2
Pop3	110/tcp	PostOffice V.3
sunrpc	111/tcp	RPC 4.0 portmapper
sunrpc	111/udp	RPC 4.0 portmapper
auth/ident	113/tcp	Authentication Service
auth	113/udp	Authentication Service
audionews	114/tcp	Audio News Multicast
audionews	114/udp	Audio News Multicast
nntp	119/tcp	Usenet Network News Transfer
nntp	119/udp	Usenet Network News Transfer
ntp	123/tcp	Network Time Protocol
Name	Port/Protocol	Description
ntp	123/udp	Network Time Protocol
netbios-ns	137/tcp	NETBIOS Name Service
netbios-ns	137/udp	NETBIOS Name Service
netbios-dgm	138/tcp	NETBIOS Datagram Service
netbios-dgm	138/udp	NETBIOS Datagram Service
netbios-ssn	139/tcp	NETBIOS Session Service
netbios-ssn	139/udp	NETBIOS Session Service
imap	143/tcp	Internet Message Access Protocol
imap	143/udp	Internet Message Access Protocol
sql-net	150/tcp	SQL-NET
sql-net	150/udp	SQL-NET
sqlsrv	156/tcp	SQL Service
sqlsrv	156/udp	SQL Service
snmp	161/tcp	
snmp	161/udp	

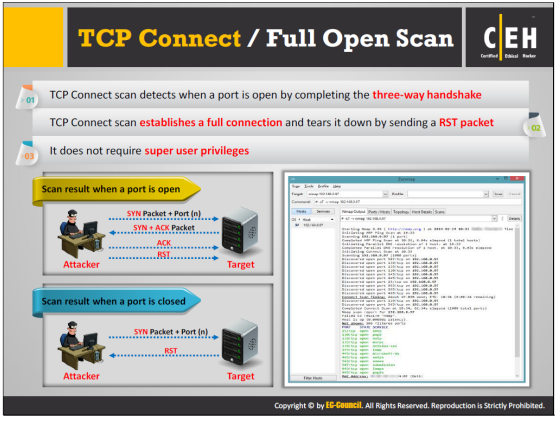
snmp-trap	162/tcp	
snmp-trap	162/udp	
cmip-man	163/tcp	CMIP/TCP Manager
cmip-man	163/udp	CMIP
cmip-agent	164/tcp	CMIP/TCP Agent
cmip-agent	164/udp	CMIP
irc	194/tcp	Internet Relay Chat
irc	194/udp	Internet Relay Chat
at-rtmp	201/tcp	AppleTalk Routing Maintenance
at-rtmp	201/udp	AppleTalk Routing Maintenance
at-nbp	202/tcp	AppleTalk Name Binding
at-nbp	202/udp	AppleTalk Name Binding
at-3	203/tcp	AppleTalk
at-3	203/udp	AppleTalk
at-echo	204/tcp	AppleTalk Echo
at-echo	204/udp	AppleTalk Echo
at-5	205/tcp	AppleTalk
at-5	205/udp	AppleTalk
at-zis	206/tcp	AppleTalk Zone Information
at-zis	206/udp	AppleTalk Zone Information
at-7	207/tcp	AppleTalk
at-7	207/udp	AppleTalk
at-8	208/tcp	AppleTalk
at-8	208/udp	AppleTalk
ipx	213/tcp	Novel
ipx	213/udp	Novel
imap3	220/tcp	Interactive Mail Access Protocol v3
imap3	220/udp	Interactive Mail Access Protocol v3

aurp	387/tcp	AppleTalk Update-Based Routing
aurp	387/udp	AppleTalk Update-Based Routing
netware-ip	396/tcp	Novell Netware over IP
netware-ip	396/udp	Novell Netware over IP
Name	Port/Protocol	Description
rmt	411/tcp	Remote mt
rmt	411/udp	Remote mt
kerberos-ds	445/tcp	Microsoft DS
kerberos-ds	445/udp	Microsoft DS
isakmp	500/udp	ISAKMP/IKE
fcp	510/tcp	First Class Server
exec	512/tcp	BSD rexecd(8)
comsat/biff	512/udp	used by mail system to notify users
login	513/tcp	BSD rlogind(8)
who	513/udp	whod BSD rwhod(8)
shell	514/tcp	cmd BSD rshd(8)
syslog	514/udp	BSD syslogd(8)
printer	515/tcp	spooler BSD lpd(8)
printer	515/udp	Printer Spooler
talk	517/tcp	BSD talkd(8)
talk	517/udp	Talk
ntalk	518/udp	New Talk (ntalk)
ntalk	518/udp	SunOS talkd(8)
netnews	532/tcp	Readnews
uucp	540/tcp	uucpd BSD uucpd(8)
uucp	540/udp	uucpd BSD uucpd(8)

klogin	543/tcp	Kerberos Login
klogin	543/udp	Kerberos Login
kshell	544/tcp	Kerberos Shell
kshell	544/udp	Kerberos Shell
ekshell	545/tcp	krcmd Kerberos encrypted remote shell –kfall
pcserver	600/tcp	ECD Integrated PC board srvr
mount	635/udp	NFS Mount Service
pcnfs	640/udp	PC-NFS DOS Authentication
bwnfs	650/udp	BW-NFS DOS Authentication
flexlm	744/tcp	Flexible License Manager
flexlm	744/udp	Flexible License Manager
kerberos-adm	749/tcp	Kerberos Administration
kerberos-adm	749/udp	Kerberos Administration
kerberos	750/tcp	kdc Kerberos authentication—tcp
kerberos	750/udp	Kerberos
kerberos_master	751/udp	Kerberos authentication
kerberos_master	751/tcp	Kerberos authentication
krb_prop	754/tcp	Kerberos slave propagation
	999/udp	Applixware
socks	1080/tcp	
socks	1080/udp	
kpop	1109/tcp	Pop with Kerberos

ms-sql-s	1433/tcp	Microsoft SQL Server
ms-sql-s	1433/udp	Microsoft SQL Server
ms-sql-m	1434/tcp	Microsoft SQL Monitor
ms-sql-m	1434/udp	Microsoft SQL Monitor
pptp	1723/tcp	Pptp
pptp	1723/udp	Pptp
nfs	2049/tcp	Network File System
nfs	2049/udp	Network File System
eklogin	2105/tcp	Kerberos encrypted rlogin
rkinit	2108/tcp	Kerberos remote kinit
kx	2111/tcp	X over Kerberos
kauth	2120/tcp	Remote kauth
lyskom	4894/tcp	LysKOM (conference system)
sip	5060/tcp	Session Initiation Protocol
sip	5060/udp	Session Initiation Protocol
x11	6000-6063/tcp	X Window System
x11	6000-6063/udp	X Window System
irc	6667/tcp	Internet Relay Chat
afs	7000-7009/udp	Andrew File System
afs	7000-7009/udp	Andrew File System

TABLE 3.2: Reserved Ports Table



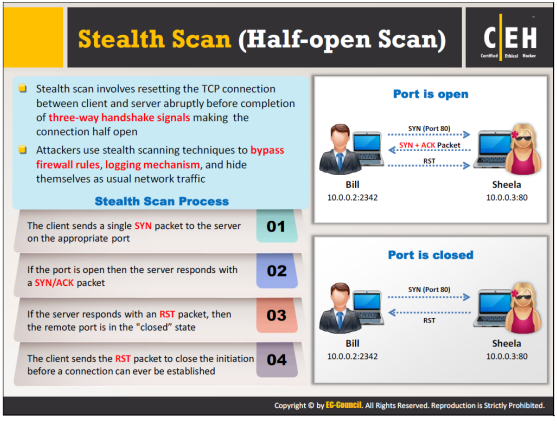
TCP Connect/Full Open Scan is one of the most reliable forms of TCP scanning. In TCP Connect scanning, the operating system's TCP connect() system call tries to open a connection to every interesting port on the target machine. If the port is listening, the connect() call will result in successful connection with the host on that particular port; otherwise, it will return an error stating that the port is not reachable.

TCP Connect scan completes a three-way handshake with the target machine. In the TCP three-way handshake, the client sends a SYN packet, which the recipient acknowledges with a SYN+ACK packet. In turn, the client acknowledges the SYN+ACK packet with an ACK packet to complete the connection. Once the handshake is completed, the scanner sends a RST packet to end the connection.

Making a separate connect() call for every targeted port in a linear fashion would take a long time over a slow connection. The attacker can accelerate the scan by using many sockets in parallel. Using non-blocking, I/O allows the attacker to set a low time-out period and watch all the sockets simultaneously.

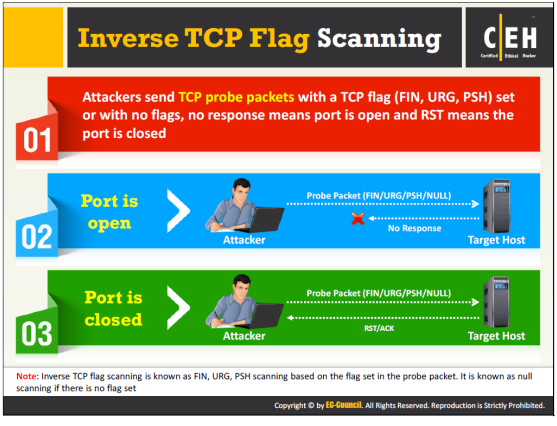
The drawback of this type of scan is that it is easily detectable and filterable. The logs in the target system will disclose the connection.

Source: *http://www.insecure.org*



A stealth scan sends a single frame to a TCP port without any TCP handshaking or additional packet transfers. This scan type sends a single frame with the expectation of a single response. The half-open scan partially opens a connection but stops halfway through. The stealth scan is also called a "SYN scan," because it only sends the SYN packet. This stops the service from notifying the incoming connection. TCP SYN, or half-open, scanning is a stealth method of port scanning.

The stealth scan also implements the three-way handshake methodology. In the last stage, it examines the packets entering the interface and terminating the connection before triggering a new initialization to identify remote ports. The stealth scan process is shown in the above slide.



Attackers send TCP probe packets with a TCP flag (FIN, URG, PSH) set, or with no flags. When the port is open, the attacker doesn't get any response from the host, whereas when the port is closed, he or she receives the RST from the target host.

Security mechanisms such as firewalls and IDS detect the SYN packets sent to the sensitive ports of the targeted hosts. Programs such as Synlogger and Courtney are available to log half-open SYN flag scan attempts. At times, the probe packets enabled with TCP flags can pass through filters undetected, depending on the security mechanisms installed.

Inverted Technique is probing a target using a half-open SYN flag because the closed ports can only send the response back. According to RFC 793, an RST/ACK packet sent for connection reset, when the host closes a port. Attackers take advantage of this feature to send TCP probe packets to each port of the target host with various TCP flags set.

Common flag configurations used for a probe packet include:

- A FIN probe with the FIN TCP flag set
- An XMAS probe with the FIN, URG, and PUSH TCP flags set
- A NULL probe with no TCP flags set
- A SYN/ACK probe

All closed ports on the targeted host will send an RST/ACK response. Because operating systems such as Windows completely ignore the RFC 793 standard, you cannot see the RST/ACK

response when connected to a closed port on the target host. However, this technique is effective when used with UNIX-based operating systems.

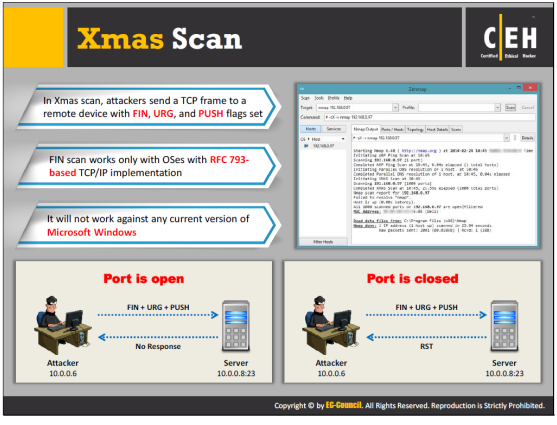
Advantages

- Avoids many IDS and logging systems, highly stealthy

Disadvantages

- Needs raw access to network sockets, thus requiring super-user privileges
- Mostly effective against hosts using a BSD-derived TCP/IP stack (not effective against Microsoft Windows hosts, in particular)

Note: Inverse TCP flag scanning is known as FIN, URG, PSH scanning based on the flag set in the probe packet. If there is no flag set, it is known as null scanning.



Xmas Scan is a port scan technique with FIN, URG, and PUSH flags set to send a TCP frame to a remote device. If the target has opened the port, then you will receive no response from the remote system. If the target has closed the port, then you will receive a remote system reply with a RST. You can use this port scanning technique to scan large networks and find which host is up and what services it is offering. It is a technique to describe all TCP flag sets. When all flags are set, some systems hang; so the flags most often set are the nonsense pattern URG-PSH-FIN. This scan only works when systems are compliant with RFC 793-based TCP/IP implementation.

BSD Networking Code

This method relies on BSD networking code, thus, you can use this only for UNIX hosts; it does not support Windows NT. If the user scans any Microsoft system, it shows all the ports on the host are open.

Transmitting Packets

You can initialize all the flags when transmitting the packet to a remote host. If the target system accepts packet and does not send any response, the port is open. If the target system sends RST flag, the port is closed.

Advantages

- It avoids the IDS and TCP three-way handshake.

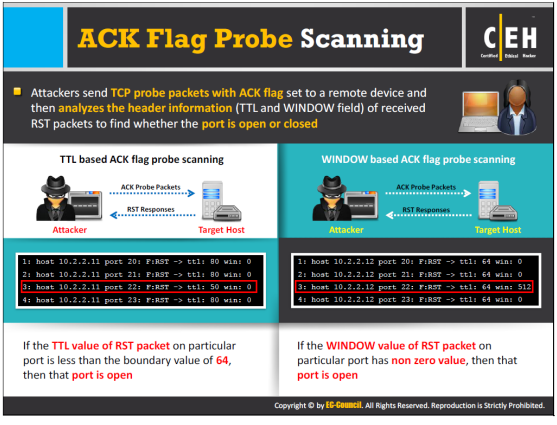
Disadvantages

- It works on the UNIX platform only.

Xmas Scan Output Using Nmap

Source: *http://nmap.org*

Zenmap is the official graphical user interface (GUI) for the Nmap Security Scanner. Using this tool, you can save the frequently used scans as profiles to make them easy to run repeatedly.



Attackers send TCP probe packets with the ACK flag set to a remote device and then analyze the header information (TTL and WINDOW field) of received RST packets to find whether the port is open or closed. The ACK flag probe scanning exploits the vulnerabilities within BSD derived TCP/IP stack. Thus, this scanning is effective only on those operating systems and platforms on which the BSD derives TCP/IP stacks.

Categories of ACK Flag Probe Scanning include:

- TTL-based ACK flag probe scanning
- WINDOW-based ACK flag probe scanning

TTL based ACK flag probe scanning

In this scanning technique, you will first need to send ACK probe packets (thousands in number) to different TCP ports, and then analyze the TTL field value of the received RST packets.

If the TTL value of RST packet on a particular port is less than the boundary value of 64, then that port is open. Here is an example displaying a log of the first four RST packets received:

```
1: host 10.2.2.11 port 20: F:RST -> ttl: 80 win: 0
2: host 10.2.2.11 port 21: F:RST -> ttl: 80 win: 0
3: host 10.2.2.11 port 22: F:RST -> ttl: 50 win: 0
4: host 10.2.2.11 port 23: F:RST -> ttl: 80 win: 0
```

FIGURE 3.2: Screenshot showing the open port based on the TTL value of RST packet

In the above example, port 22 has returned a TTL value of 50, which is less than 64; all other ports returned a TTL value of 80, which is greater than 64. Therefore, port 22 is open.

WINDOW based ACK flag probe scanning

In this scanning technique, you will first need to send ACK probe packets (thousands in number) to different TCP ports, and then analyze the Window field value of the received RST packets. The user can use this scanning technique when all the ports return the same TTL value.

If the WINDOW of RST packet on a particular port has a non-zero value, then that port is open. Here is an example displaying a log of the first four RST packets received:

```
1: host 10.2.2.12 port 20: F:RST -> ttl: 64 win: 0
2: host 10.2.2.12 port 21: F:RST -> ttl: 64 win: 0
3: host 10.2.2.12 port 22: F:RST -> ttl: 64 win: 512
4: host 10.2.2.12 port 23: F:RST -> ttl: 64 win: 0
```

FIGURE 3.3: Screenshot showing the open port based on the window value of RST packet

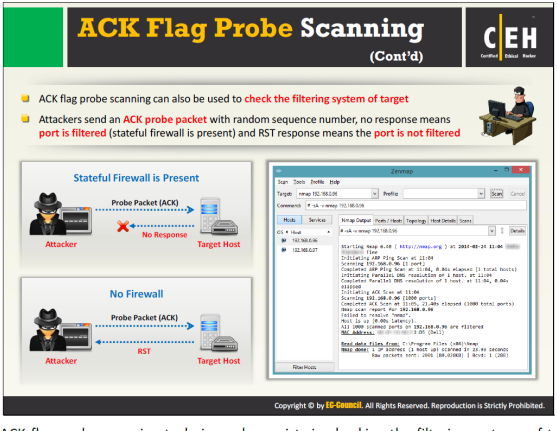
Figure 3.3 shows that the TTL value returned for each packet is the same, so you cannot perform TTL based ACK flag probe scanning to find the open ports. Therefore, when you observe the window value, the third packet has a non-zero window value, which means that the port is open.

Advantages:

- This type of scan can evade IDS in most cases.

Disadvantages:

- This scan is very slow and can exploit only older operating systems with vulnerable BSD derived TCP/IP stacks.



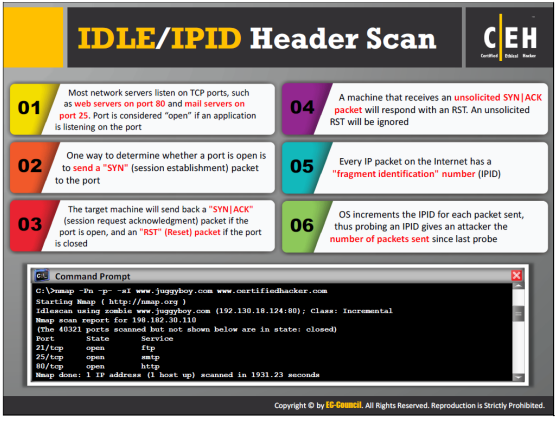
The ACK flag probe scanning technique also assists in checking the filtering systems of target networks. The attacker sends an ACK probe packet to check the filtering mechanism (Firewalls) of packets employed by the target network.

Sending an ACK probe packet with a random sequence number and getting No Response from the target means that the port is filtered (stateful firewall is present); an RST response from the target means that the port is not filtered (No Firewall is Present).

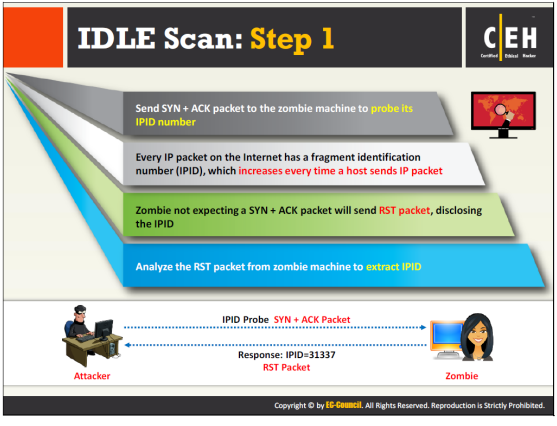
```
nmap -sA -P0 10.10.0.25

Starting nmap 5.21 (http://nmap.org) at 2010-05-16 12:15 EST

All 529 scanned ports on 10.10.0.25 are: filtered
```



The IDLE/IPID Header scan is a TCP port scan method that you can use to send a spoofed source address to a computer to find out what services are available. It offers complete blind scanning of a remote host. The attacker performs this scan by impersonating another computer through spoofing. The attacker does not send a packet from her/his own IP address, instead using another host, often called a "zombie," to scan the remote host and identify any open ports. In this attack, the attacker expects the sequence numbers of the zombie host and if the remote host checks the IP of the scanning party, the IP of the zombie machine will display.



Every IP packet on the Internet has a fragment Internet protocol identification (IPID) number that uniquely identifies fragments of an original IP datagram. Because many operating systems simply increment this number for each packet they send, probing for the IPID can tell an attacker how many packets the user sent since the last probe.

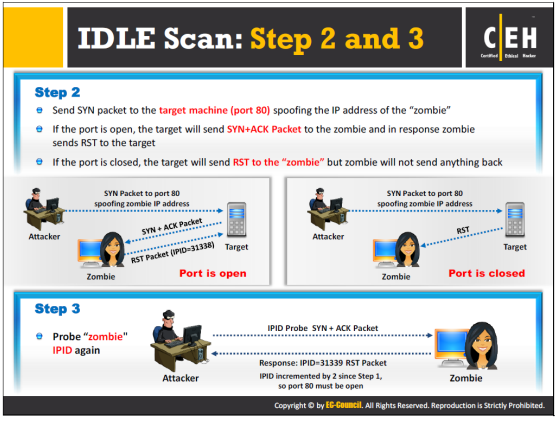
The first step in performing an idle scan is to find an appropriate zombie. The zombie that assigns IPID packets incrementally on a global basis is an appropriate or idle zombie to perform the idle scan. The lower the time interval for request/response between the attacker-zombie and the zombie-target, the faster the scan.

Choose a "Zombie" and Probe for Its Current IP Identification (IPID) Number

In the first step, you will send SYN+ACK packet to the zombie machine to probe its IPID number. Here, the reason you send the SYN+ACK packet is to probe the IPID number but not establish a TCP connection (3-way handshake).

As the zombie does not expect a SYN+ACK packet, it will deny the connection by sending back an RST packet.

Analyze the RST packet sent by the zombie machine to extract the IPID. In the diagram shown in the slide above, assume the zombie responds with IPID=31337. Assume this IPID is X.



Attacker sends a SYN packet to the target machine on port 80 spoofing the IP address of the Zombie.

Idle Scan: Step 2.1 (Open Port)

If the port is open, the target will send the SYN+ACK packet to the zombie (as the IP address was spoofed) to proceed with the 3-way handshake.

As the zombie did not expect a SYN+ACK packet from the target machine, it responds with a RST packet.

Because every IP packet has a "fragment identification" number, which increments by one for every packet transmission, this time the zombie will use its next available IP ID i.e., 31338 (X + 1).

Idle Scan: Step 2.2 (Closed Port)

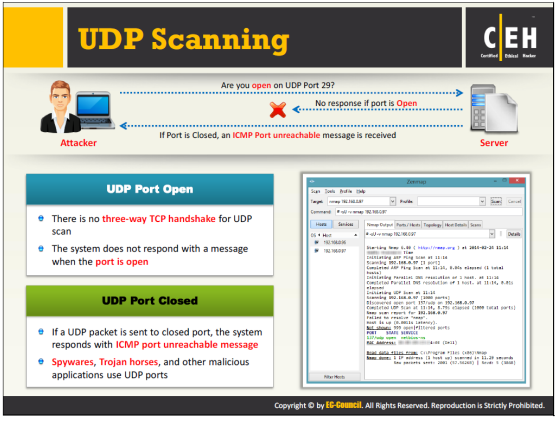
Assume that the port on the target is closed. Then, on receiving the SYN packet from the attacker (you), the target responds with a RST and the zombie remains idle without taking any further action.

Idle Scan: Step 3

Now, follow step 1 again to probe the IP ID number.

Send a SYN+ACK packet to the zombie and it responds with a RST packet containing the IPID. Assuming that the port on the target was open, and the zombie has already sent a RST packet

to the target; the IPID number has incremented by 1. This time the zombie responds with a RST packet to the attacker, using its next IPID i.e., 31339 (X + 2). So, the IP ID has incremented by 2, which infers that the port on the target machine was open. Thus, using an Idle scan, an attacker can find out the open ports and services on the target machines by spoofing his/her IP address with a zombie's IP address.



UDP Raw ICMP Port Unreachable Scanning

UDP port scanners use the UDP protocol instead of TCP. The UDP protocol can be more difficult to use than TCP scanning, because you can send a packet, but you cannot determine whether the host is alive, dead, or filtered. However, you can use one ICMP that checks for open or closed ports. If you send a UDP packet to a port without an application bound to it, the IP stack will return an ICMP port unreachable packet. If any port returns an ICMP error, then it will close, leaving the ports that didn't answer are either open or filtered by the firewall.

This happens because open ports do not have to send an acknowledgement in response to a probe, and closed ports are not even required to send an error packet.

UDP Packets

Source: *http://nmap.org*

When you send a packet to a closed UDP port, most of the hosts send an **ICMP_PORT_UNREACH** error. Thus, you can determine whether a port is NOT open if UDP packets or ICMP errors are not guaranteed to arrive. Thus, UDP scanners of this sort must implement retransmission of packets that appear lost. UDP scanners interpret lost traffic as open ports.

In addition, this scanning technique is slow because of limiting the ICMP error message rate as compensation to machines that apply RFC 1812 section 4.3.2.8. A remote host will require access to the raw ICMP socket to distinguish closed from unreachable ports.

UDP RECVFROM () and WRITE () Scanning

Although non-root users cannot read port unreachable errors directly, Linux informs you indirectly when they receive messages.

Example:

For example, a second write () call to a closed port will usually fail. Various scanners, such as Netcat and Pluvial pscan.c do recvfrom () on non-blocking UDP sockets, usually return EAGAIN ("Try Again," errno 13) if the ICMP error has not been received, and ECONNREFUSED ("Connection refused," errno 111), if it has. This is the technique used for determining open ports when non-root users use -u (UDP). Root users can also use the -l (lamer UDP scan) options to force this.

Advantage:

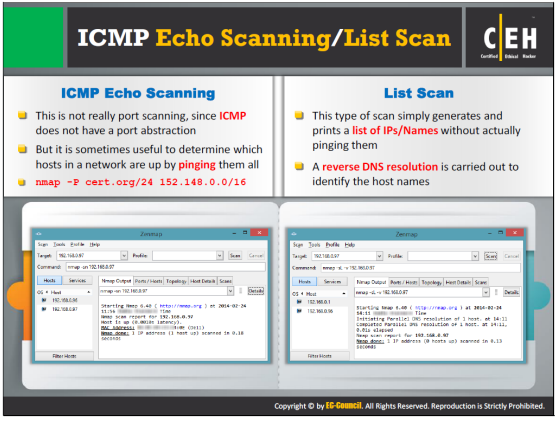
The UDP scan is less informal regarding an open port, because there's no overhead of a TCP handshake. However, if ICMP is responding to each unavailable port, the number of total frames can exceed those from a TCP scan. Microsoft-based operating systems do not usually implement any type of ICMP rate limiting, so this scan operates very efficiently on Windows-based devices.

Disadvantage:

The UDP scan provides port information only. If additional version information is needed, the scan must be supplemented with a version detection scan (-sV) or the operating system fingerprinting option (-O).

The UDP scan requires privileged access, so this scan option is only available on systems with the appropriate user permissions.

Most networks have huge amounts of TCP traffic; as a result, the efficiency of the UDP scan is lost. The UDP scan will locate these open ports and provide the security manager with valuable information for identifying successful attacker invasions on open UDP ports caused by spyware applications, Trojan horses, and other malicious software.



ICMP echo scanning pings all the machines in the target network to discover live machines. Attackers send ICMP probes to the broadcast or network address relay to all host addresses in the subnet. The live systems will send ICMP echo reply message to the source of the ICMP echo probe.

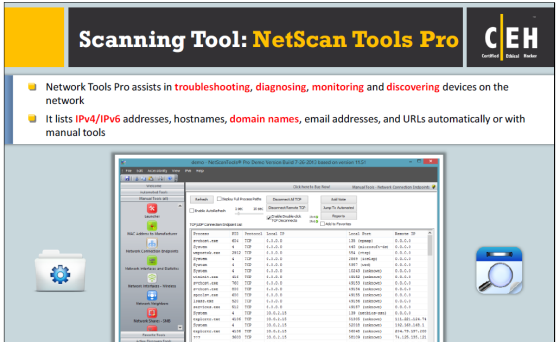
UNIX/Linux and BSD-based machines use ICMP echo scanning; the TCP/IP stack implementations in these operating system respond to the ICMP echo requests to the broadcast addresses. This technique does not work on Windows-based networks, as their TCP/IP stack implementation does not reply to ICMP probes directed at the broadcast address.

ICMP echo scanning is not same as port scanning, as it does not have a port abstraction. ICMP echo scanning is useful to determine which hosts in a network are active by pinging them all. Active hosts are displayed in Zenmap as "Host is up (0.020s latency)," as shown in the screenshot on the slide.

In a list scan, discovery of the active network host is indirect. A list scan simply generates and prints a list of IPs/Names without actually pinging or scanning the hosts. As a result, the list scan shows all IP addresses as "not scanned" (0 hosts up). By default, a reverse DNS resolution is still carried out on each host by Nmap for learning their names.

Advantages:

- A list scan can perform a good sanity check.
- The list scan detects incorrectly defined IP addresses on the command line or in an option file. It primarily repairs the detected errors to run any "active" scan.



NetScan Tools Pro is an investigation tool that allows you to troubleshoot, monitor, discover, and detect devices on your network. You can gather information about the local LAN, as well as Internet users, IP addresses, ports, and so on using this tool. You can find vulnerabilities and exposed ports in your system. NetScan Tools Pro combines many network tools and utilities categorized by their functions, such as active, passive, DNS, and local computer.

Active Discovery and Diagnostic Tools: Used for testing and locating devices connected to your network.

Passive Discovery Tools: Monitor the activities of the devices connected to your network and gather information from third parties.

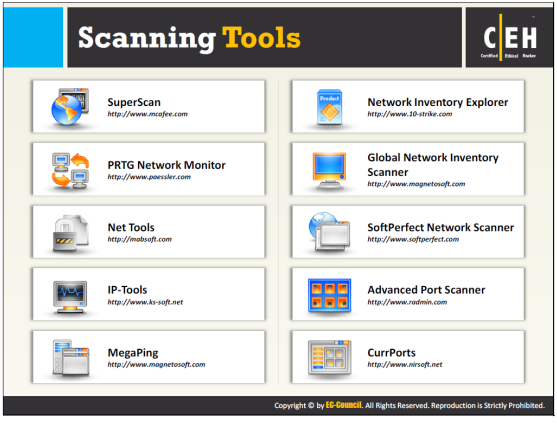
DNS Tools: Help to detect DNS problems.

Local Computer and General Information Tools: Provide details about your local computer's network.

Benefits:

- The information gathering process is made simpler and faster by automating the use of many network tools.
- Produces the result reports in your web browser clearly.

Source: *http://www.netscantools.com*



Scanning tools scan and identify live hosts, open ports, and running services on a target network. Information obtained helps an attacker in creating the profile of the target organization.

Some of the scanning tools are listed below:

SuperScan

Source: *http://www.mcafee.com*

SuperScan is a connect-based TCP port scanner, pinger, and hostname resolver with multithreaded and asynchronous techniques to scan a network. Some of the features include:

- Performing ping scans and port scans using any IP range
- Using a text file to extract addresses
- Scanning any port range from a built-in list or any given range
- Viewing responses from connected hosts
- Saving the scan list to a text file
- Transmission speed control

PRTG Network Monitor

Source: http://www.paessler.com

PRTG Network Monitor is a network monitoring application for Windows-based systems. It is suitable for small, medium, and large networks and used for LAN, WAN, WLAN, and VPN monitoring. You can also monitor physical or virtual web, mail, and file servers, Linux systems, Windows clients, routers, and so on. PRTG monitors network availability and bandwidth use, as well as other network parameters such as quality of service, memory load, and CPU use. It provides system administrators with live readings and periodical usage trends to optimize the efficiency, layout, and setup of leased lines, routers, firewalls, servers, and other network components.

Net Tools

Source: http://mabsoft.com

Net Tools is a combination of network scanning, security, file, system, and administrator tools useful in diagnosing networks and monitoring a PC and computer's network connections for system administrators. Designed for the Microsoft Windows OS, Net Tools contains a variety of tools such as Active and Passive port scanner, Advanced Netstat Monitoring, Web Page Scanner, Whois & MX Lookup, and Remote LAN PC Lister.

IP-Tools

Source: http://www.ks-soft.net

IP-Tools offers many TCP/IP utilities in one program. This program is indispensable for anyone who uses the Internet or an intranet. IP-Tools includes utilities such as Local Info, NetBIOS Info, Ping Scanner, Port Scanner, and IP-Monitor.

MegaPing

Source: http://www.magnetosoft.com

MegaPing is a toolkit that scans your entire network and provides information such as open shared resources, open ports, services/drivers active on the computer, key registry entries, users and groups, trusted domains, printers, and more. MegaPing security scanner checks your network for potential vulnerabilities that might use to attack your network and saves information insecurity reports. The tools save the scan results in HTML or TXT reports, which secure your network—for example, by shutting down unnecessary ports, closing shares.

Network Inventory Explorer

Source: http://www.10-strike.com

Network Inventory Explorer is network inventory software that helps you create and maintain the inventory database of network computers. You can view hardware and software on network computers remotely, and track hardware and software changes. You can create reports on the availability of particular programs and number of copies installed on computers, and reports on versions of operating system, installed updates and bug-fixes, codecs, and so on. You can also plan upgrades and generate reports on computers with insufficient RAM size or disk space.

Global Network Inventory Scanner

Source: http://www.magnetosoft.com

Global Network Inventory is a software and hardware inventory system that audits remote computers and even network appliances, including switches, network printers, and document centers.

SoftPerfect Network Scanner

Source: http://www.softperfect.com

SoftPerfect Network Scanner is a multi-threaded IP, NetBIOS, and SNMP scanner. The program pings computers, scans for listening TCP/UDP ports and displays the types of resources shared on the network, including system and hidden ones. In addition, it can mount shared folders as network drives, browse them using Windows Explorer, filter the results list, and more. SoftPerfect Network Scanner can also check for a user-defined port and report if one is open. It can also resolve host names and auto-detect the local and external IP range. It supports remote shutdown and Wake-On-LAN.

Advanced Port Scanner

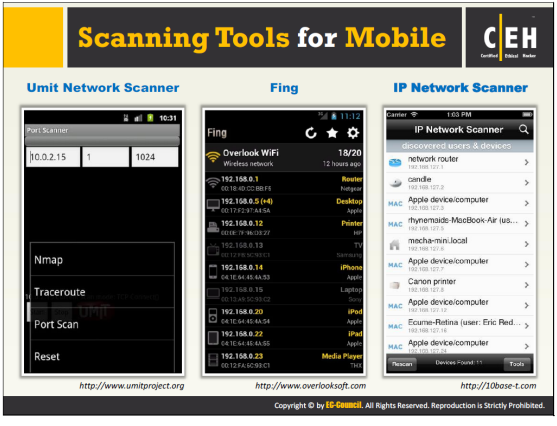
Source: http://www.radmin.com

Advanced Port Scanner is a port scanner for the Win32 platform. It uses a multithread technique, so on fast machines you can scan ports very fast. In addition, it contains descriptions for common ports, and can perform scans on predefined port ranges.

CurrPorts

Source: http://www.nirsoft.net

CurrPorts is a network monitoring software that displays the list of all currently opened TCP/IP and UDP ports on your local computer. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, and so on), the time that the process was created, and the user that created it.



Given below are few scanning tools for mobile devices:

Umit Network Scanner

Source: http://www.umitproject.org

Umit Network Scanner for Android devices helps in finding the network. It runs a complete Nmap scan and gives options for scanning specific ports, port ranges, and network ranges. Features include inventory, mapping, diffs, reports, profiles, and a wizard.

Fing

Source: http://www.overlooksoft.com

Fing is a mobile app for Android and iOS that scans and provides complete network information, such as IP address, MAC address, device vendor, and ISP location.

Features:

- Discovers all devices connected to a Wi-Fi network
- Displays MAC Address and device manufacturer
- Full search by IP, MAC, Name, Vendor, and Notes
- Wake On LAN: Allows you to switch on your devices from mobile or tablet
- Ping and traceroute: Assesses network performance
- Automatic DNS lookup and reverse lookup

- Checks the availability of Internet connection
- Works also with hosts outside your local network
- Tracks when a device has gone online or offline
- Launch Apps for specific ports, such as Browser, SSH, FTP
- Displays NetBIOS names and properties
- Displays Bonjour info and properties
- Supports identification by IP address for bridged networks
- Sort by IP, MAC, Name, Vendor, State, Last Change

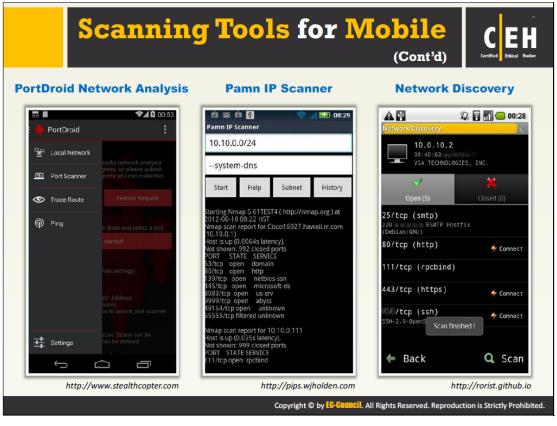
IP Network Scanner

Source: http://10base-t.com

IP Scanner for iOS scans your local area network to determine the identity of all its active machines and Internet devices.

Features:

- In-built Ping, Portscan, WOL tools
- Traverse to native VNC, web browser or any custom service directly from the scan results
- Customizable display options for assigning names and icons to discovered devices
- Ability to create your own custom device categories with your own images
- Ability to Export, email, and print scan results
- Synchronize customizations across devices using iCloud or DropBox
- Save and import the device lists for different networks



Below are listed a few more scanning tools for mobile devices:

PortDroid Network Analysis

Source: *http://www.stealthcopter.com*

The PortDroid Network analysis app provides several useful tools including ping, traceroute, port scanner, and local network discovery.

- **Portscanner** – Scans an IP for open TCP ports. Alternatively, it will use Banner Grabbing on each port to gain more information or discover a Web service. When a service is found on a port, external applications will be offered to deal with certain protocols (ssh, telnet, http, https, ftp, etc.).
- **Local Network Information** – Shows device and connection information, and finds devices on the same network (Wi-Fi only).
- **Ping** – Allows ping of Hostname/IPs.
- **Traceroute** – Can perform a traceroute and geolocate IPs to view on map.

Pamn IP Scanner

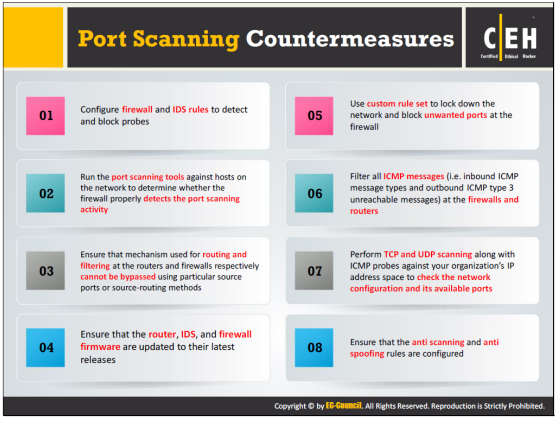
Source: *http://pips.wjholden.com*

Pamn IP Scanner (or PIPS), formerly titled "Nmap for Android," is simply a wrapper around a cross-compiled Nmap binary built for the Android phone.

Network Discovery

Source: *http://rorist.github.io*

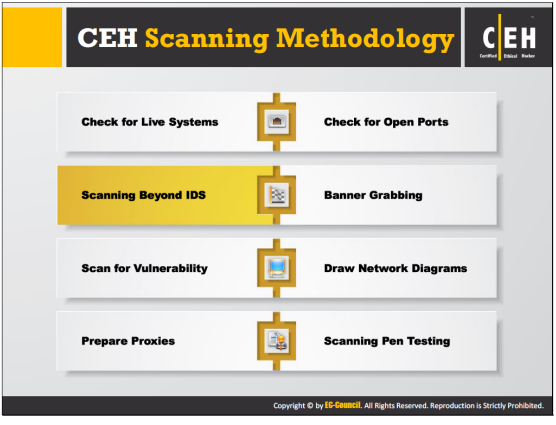
Network Discovery is an Android network tool that discovers hosts and scans their ports on a Wi-Fi network.



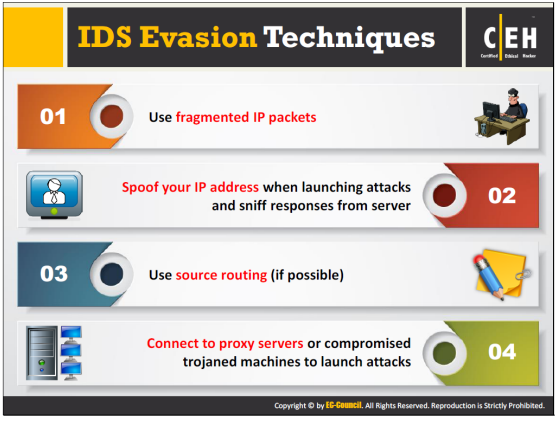
As discussed previously, port scanning provides a lot of useful information, such as IP addresses, host names, open ports, and services running on ports, to the attacker. Open ports especially provide an easy means for the attacker to break into the network. But there is nothing to worry about, provided that you secure your system or network against port scanning by applying the following countermeasures:

- The firewall should be effective enough to detect probes sent by the attackers using port scanning tools. It should not allow traffic to pass through it after simply inspecting the TCP header. The firewall should be able to examine the data contained in each packet before allowing the traffic to pass through it.
- Some firewalls do a better job than others in detecting stealth scans. For example, many firewalls have specific options to detect SYN scans, while others completely ignore FIN scans.
- Configure commercial firewalls to protect your network against fast port scans and SYN floods. You can run tools such as portsentry to detect and stop port scan attempts on Linux/UNIX systems.
- Hackers use tools such as Nmap and perform OS-detection methods to sniff the details of a remote operating system. Thus, it's important to employ intrusion detection systems in such cases. Snort (http://www.snort.org) is an intrusion detection and prevention technology that can be very useful, mainly because signatures are frequently available from public authors.

- Keep as few ports open as necessary and filter the rest, as the intruder will try to enter through any open port. Use a custom rule set to lock down the network, block unwanted ports at the firewall, and filter the following ports: 135–159, 256–258, 389, 445, 1080, 1745, and 3268.
- Block inbound ICMP message types and all outbound ICMP type-3 unreachable messages at border routers arranged in front of a company's main firewall.
- Attackers try to perform source routing and send packets to the targets (which may not be reachable via Internet) by making use of an intermediate host that can interact with the target. Such mechanisms can be adapted for hacking purposes, so ensure that your firewall and router can block such source-routing techniques.
- Test your own IP address space using TCP and UDP port scans as well as ICMP Probes to determine network configuration and accessible ports.
- If a commercial firewall is in use, then ensure that:
  - It is Patched with the latest updates
  - It has correctly defined antispoofing rules
  - Its Fastmode services are unusable in Check Point Firewall-1 environments



An Intrusion Detection System (IDS) is a security mechanism intended to prevent an attacker from accessing a network. But even IDSs have some security limitations. Attackers try to launch attacks by exploiting these limitations. This section highlights IDS evasion techniques and SYN/FIN scanning using IP fragments.



Though Firewalls and IDSs avoid malicious traffic (packets) from entering a server, attackers manage to send intended packets to the destination server by implementing techniques such as:

- **Packet Fragmentation**, in which attackers send fragmented probe packets to the intended server which re-assembles it after receiving all the fragments
- **Source Routing**, in which the attacker specifies the routing path for the malformed packet to reach the intended server

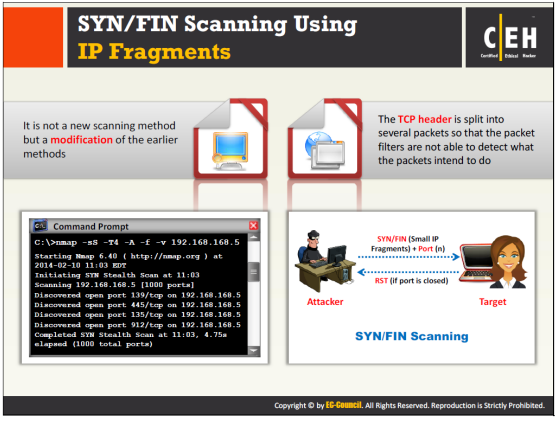
Use Fragmented IP packets

Packet fragmentation refers to splitting a probe packet into several smaller packets (fragments) while sending it to a network. When these packets reach a host, IDSs and firewalls behind the host generally queue all of them and process them one by one. However, since this method of processing involves greater CPU consumption as well as network resources, configuration of most of the IDSs makes it skip fragmented packets during port scans.

Therefore, attackers use packet fragmentation tools such as Nmap and fragroute to split the probe packet into smaller packets that circumvent port-scanning techniques employed by intrusion detection systems. Once these fragments reach the destined host, they again re-assemble to form a single packet.

Use Source Routing (If Possible)

An IP datagram contains various fields, including the IP options field, which stores source routing information and contains a list of IP addresses through which the packet travels to its destination. When attackers send malformed packets to a target, these packets hop through various routers and gateways to reach the destination. In some cases, routers in the path might include configured firewalls and IDSs that block such packets. To avoid this, attackers enforce a loose or strict source routing mechanism, in which they manipulate the IP address path in the IP options field, so that the packet takes the attacker-defined path (without firewall-/IDS-configured routers) to reach the destination, thereby evading firewalls and IDSs.

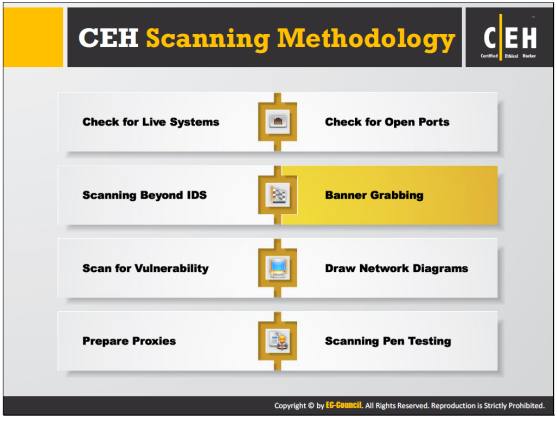


This method of scanning was created to avoid false positives generated by other scans because of a packet filtering device on the target system. The TCP header splits into several packets to evade the packet filter. For any transmission, every TCP header must have the source and destination port for the initial packet (8-octet, 64-bit). The initialized flags in the next packet let the remote host reassemble the packet upon receipt via an Internet protocol module that detects the fragmented data packets by means of field equivalent values of source, destination, protocol, and identification.

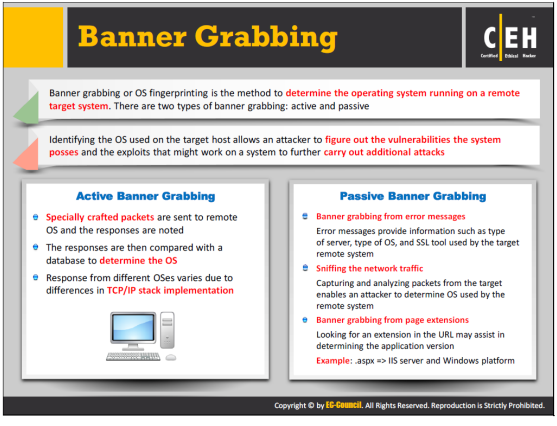
In this scan, the system splits the TCP header into several fragments and transmits them over the network. However, IP reassembly on the server-side may result in unpredictable and abnormal results, such as fragmentation of IP header data. Some hosts may fail to parse and reassemble the fragmented packets, thus leading to crashes, reboots, or even network device monitoring dumps.

Some firewalls might have rule sets that block IP fragmentation queues in the Kernel (e.g., CONFIG_IP_ALWAYS_DEFRAG option in the Linux kernel), even though this is not widely implemented because of adverse effects on performance. Because many IDSs use signature-based methods to indicate scanning attempts on IP and/or TCP headers, the use of fragmentation will often evade this type of packet filtering and detection, resulting in a high probability of causing problems on the target network.

The screenshot on the slide above illustrates the SYN/FIN scan using the Nmap tool.



An attacker uses banner grabbing techniques to identify network hosts running versions of applications and OSs with known exploits. This section introduces you to banner grabbing, its types, and its tools, as well as useful countermeasures you can employ against it.



Banner grabbing, or "OS fingerprinting," is a method used to determine the operating system that is running on a remote target system. It is an important scanning method, as the attacker will have a greater probability of success if the OS of the target system is known (many vulnerabilities are OS-specific). The attacker can then formulate an attack strategy based on the OS of the target system.

There are two methods of banner grabbing: spotting the banner while trying to connect to a service such as FTP site, or downloading the binary file/bin/ls to check the system architecture.

A more advanced fingerprinting technique depends on stack querying, which transfers the packets to the network host and evaluates them by the reply. The first stack-querying method designed with regard to the TCP mode of communication evaluates the response to connection requests.

The next method, known as ISN (Initial Sequence Number) analysis, identifies the differences in random number generators found in the TCP stack.

ICMP response analysis is another method used to fingerprint an OS. It consists of sending ICMP messages to a remote host and evaluating the reply.

Discussed below are two different types of banner grabbing techniques:

Active Banner Grabbing

Active banner grabbing applies the principle that an operating system's IP stack has a unique way of responding to specially crafted TCP packets. This happens because of different

interpretations that vendors apply while implementing the TCP/IP stack on the particular OS. In active banner grabbing, the attacker sends a variety of malformed packets to the remote host, and the responses are compared to a database.

For instance, the scanning utility Nmap uses a series of nine tests to determine an OS fingerprint or banner grabbing. The tests listed below give some idea of an active banner grabbing attack, as described in www.packetwatch.net:

Test 1: A TCP packet with the SYN and ECN-Echo flags enabled is sent to an open TCP port.

Test 2: A TCP packet with no flags enabled is sent to an open TCP port. This type of packet is a NULL packet.

Test 3: A TCP packet with the URG, PSH, SYN, and FIN flags enabled is sent to an open TCP port.

Test 4: A TCP packet is sent with the ACK flag enabled to an open TCP port.

Test 5: A TCP packet is sent with the SYN flag enabled to a closed TCP port.

Test 6: A TCP packet is sent with the ACK flag enabled to a closed TCP port.

Test 7: A TCP packet is sent with the URG, PSH, and FIN flags enabled to a closed TCP port.

Test 8 PU (Port Unreachable): A UDP packet is sent to a closed UDP port. The objective is to extract an "ICMP port unreachable" message from the target machine.

Test 9 TSeq (For TCP Sequencability test): This test tries to determine the sequence generation patterns of the TCP initial sequence numbers (also known as TCP ISN sampling), the IP identification numbers (also known as IPID sampling), and the TCP times tamp numbers. It sends six TCP packets with the SYN flag enabled to an open TCP port.

The objective of these tests is to find patterns in the initial sequence of numbers that the TCP implementations chose while responding to a connection request. These can be categorized into groups, such as the traditional 64K (many old UNIX boxes), random increments (newer versions of Solaris, IRIX, FreeBSD, Digital UNIX, Cray, and many others), or true random (Linux 2.0.*, OpenVMS, newer AIX, etc.). Windows boxes use a "time-dependent" model in which the ISN is incremented by a fixed amount for each occurrence.

Passive Banner Grabbing

Source: *http://honeynet.org*

Like active banner grabbing, passive banner grabbing also depends on the differential implementation of the stack and the various ways an OS responds to packets. However, instead of relying on scanning the target host, passive fingerprinting captures packets from the target host via sniffing to study for telltale signs that can reveal an OS.

Given below are the four areas that typically determine the operating system:

- TTL (time to live) of the packets: What the operating system sets as the Time To Live on the outbound packet
- Window Size: What the operating system sets the Window size

- Whether the DF (Don't Fragment) bit is set: Does the operating system set the Don't Fragment bit
- TOS (Type of Service): Does the operating system set the Type of Service, and if so, what setting is it?

Passive fingerprinting has to be neither fully accurate nor be limited to these four signatures. However, one can improve accuracy by looking at several signatures, and combining the information. The following is an analysis of a sniffed packet dissected by Lance Spitzner in his paper on passive fingerprinting (http://www.honeynet.org/papers/finger/):

```
04/20-21:41:48.129662 129.142.224.3:659 -> 172.16.1.107:604
TCP TTL:45 TOS:0x0 ID:56257
***F**A* Seq: 0x9DD90553
Ack: 0xE3C65D7 Win: 0x7D78
```

According to the four criteria, the following are identified:

- TTL: 45
- Window Size: 0x7D78 (or 32120 in decimal)
- DF: The Don't Fragment bit is set
- TOS: 0x0

Compare this information to a database of signatures.

TTL: The TLL from the analysis is 45. The original packet went through 19 hops to get to the target, so it set the original TTL to 64. Based on this TTL, it appears that the user sent the packet from a Linux or FreeBSD box (however, more system signatures need to be added to the database). This TTL confirms it by doing a traceroute to the remote host. If the trace needs to be done stealthily, the traceroute TTL (default 30 hops) can be set to one or two hops less than the remote host (-m option). Setting the traceroute in this manner reveals path information (including the upstream provider) without actually touching the remote host.

Window Size: In this step, window sizes are compared. Window size is another effective tool for determining specifically what window size is used and how often it is changed. In the previous signature, the window size is set at 0x7D78, a default window size commonly used by Linux. In addition, FreeBSD and Solaris tend to maintain the same window size throughout a session. However, Cisco routers and Microsoft Windows NT window sizes constantly change. Window size is more accurate when measured after the initial three-way handshake (due to TCP slow start).

DF bit: Most systems use the DF bit set, so this is of limited value. However, this does make it easier to identify few systems that do not use the DF flag (such as SCO or OpenBSD).

TOS: TOS is also of limited value, as it seems to be more session-based than OS-based. In other words, it is not so much the OS that determines the TOS, but the protocol used.

From the information obtained from the packet, specifically TTL and window size, one can compare the results to the database of signatures and, with some degree of confidence, determine the OS (in this case, Linux kernel 2.2.x).

Passive fingerprinting, like active fingerprinting, has some limitations. First, applications that build their own packets (e.g., Nmap, Hunt, Nemesis, etc.) will not use the same signatures as the OS. Second, it is relatively simple for a remote host to adjust the TTL, window size, DF, or TOS setting on packets.

Passive fingerprinting has several other uses. Crackers can use stealthy fingerprinting; for example, to determine the operating system of a potential target such as a Web server, a user need only request a Web page from the server and then analyze the sniffer traces. This bypasses the need for using an active tool that various IDS systems can detect. Passive fingerprinting also helps in identifying remote proxy firewalls. Because proxy firewalls rebuild connections for clients, it may be possible to ID proxy firewalls from the signatures, as discussed above. Likewise, passive fingerprinting can be used to identify rogue systems.

Why Banner Grabbing?

An attacker uses banner grabbing to identify the OS used on the target host and thus determine system vulnerabilities and the exploits that might work on that system to further carry out additional attacks.

Banner Grabbing Tools

ID Serve

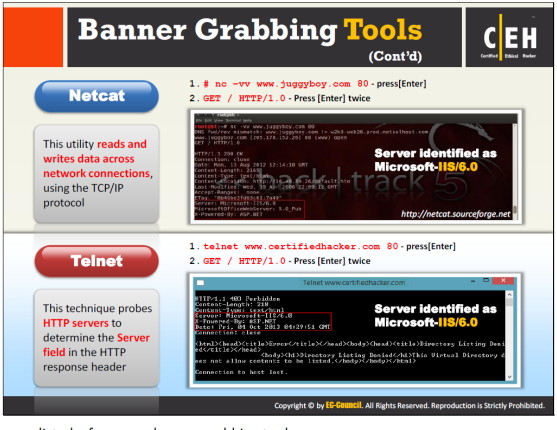
- ID Serve is used to identify the **make**, **model**, and **version** of any web site's server software
- It is also used to **identify non-HTTP** (non-web) **Internet servers** such as FTP, SMTP, POP, NEWS, etc.

Netcraft

- Netcraft reports a **site's operating system**, **web server**, and **netblock** owner together with, if available, a graphical view of the time since last reboot for each of the computers serving the site

http://www.grc.com

http://toolbar.netcraft.com



Below are listed a few more banner grabbing tools:

Netcat

Source: http://netcat.sourceforge.net

Netcat is a networking utility that reads and writes data across network connections, using the TCP/IP protocol. It is a reliable "back-end" tool used directly or driven by other programs and scripts. It is also a network debugging and exploration tool.

Features:

- Outbound and inbound connections, TCP or UDP, to or from any ports
- Tunneling mode, which allows special tunneling such as UDP to TCP, with the possibility of specifying all network parameters (source port/interface, listening port/interface), and the remote host allowed to connect to the tunnel
- Built-in port-scanning capabilities, with randomizer
- Usage options, such as buffered send-mode (one line every *N* seconds) and hexdump (to stderr or to a specified file) of transmitted and received data
- Optional RFC854 telnet codes parser and responder

Discussed below are commands used to perform banner grabbing (e.g., www.juggyboy.com), to gather information (e.g., server type, version, etc.).

- `# nc –vv www.juggyboy.com 80` - press[Enter]
- `GET / HTTP/1.0` - Press [Enter] twice

Telnet

Telnet is a network protocol. It is widely used on the Internet or local area networks. It is a client-server protocol. It provides the login sessions for a user on the Internet. The single terminal attached to the other computer emulates with Telnet. The main security problems with Telnet are:

- It does not encrypt any data sent through the connection.
- It lacks an authentication scheme.

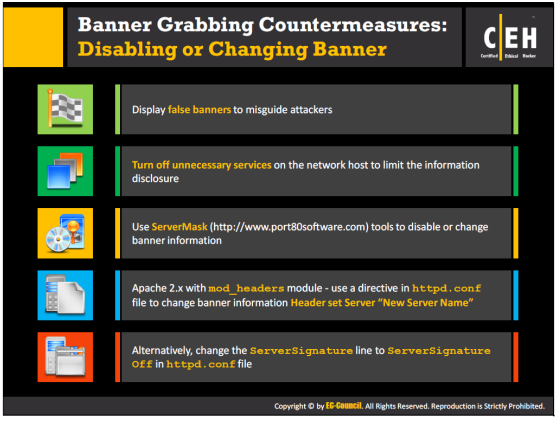
Telnet helps the user to perform banner grabbing attack. It probes HTTP servers to determine the Server field in the HTTP response header.

For instance, to enumerate a host running on http (tcp 80), follow the procedure given below:

- Open the command prompt window.

  Go to **Start** → Open **Run** dialogue box → type **cmd**, and press **Enter** or click **OK**.
- In the command prompt window, request telnet to connect to a host on a specific port: `C:\>telnet www.certifiedhacker.com 80` and press **Enter**. A blank screen appears.
- Type `GET / HTTP/1.0` and press **Enter** twice.

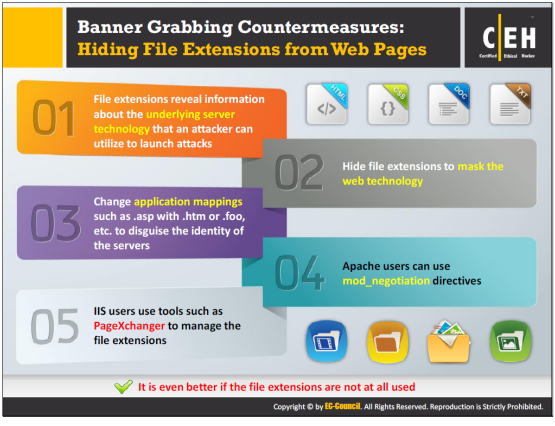
The HTTP server responds with the information (see the screenshot on the slide).

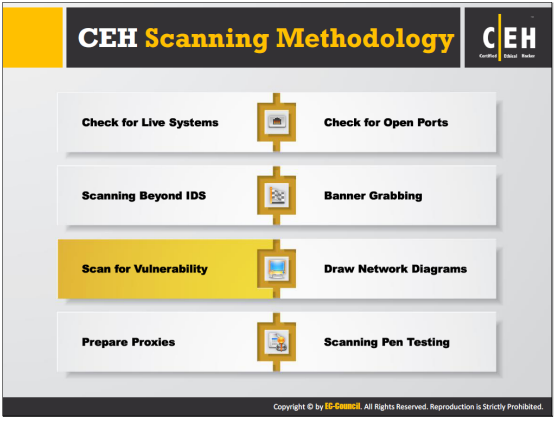


Whenever a port is open, it means a service/banner is running on it. When attackers connect to the open port using banner grabbing techniques, the system presents a banner containing sensitive information such as OS, server type, and version. With the help of the information gathered, the attacker identifies specific vulnerabilities to exploit and thereafter launches attacks. The countermeasures to defend against banner grabbing attacks are as follows:

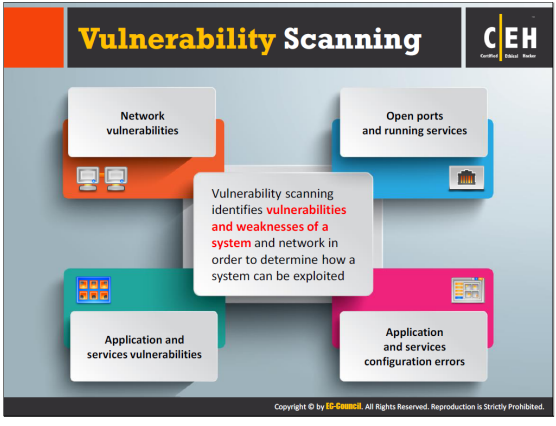
- Display false banners to misguide attackers.
- Turn off unnecessary services on the network host to limit information disclosure.
- Use ServerMask (http://www.port80software.com) tools to disable or change banner information.

  ServerMask removes unnecessary HTTP header and response data and camouflages the server by providing false signatures. It also lets you to eliminate file extensions such as .asp or .aspx, and it clearly indicates that a site is running on a Microsoft server.
- Apache 2.x with `mod_headers` module: use a directive in `httpd.conf` file to change banner information Header set Server "New Server Name".
- Alternatively, change the **`ServerSignature`** line to **`ServerSignature Off`** in the **`httpd.conf`** file.





An attacker performs vulnerability scanning in order to identify security loopholes in the target network that attackers exploit to launch attacks. This section describes vulnerability scanning and various vulnerability scanning tools.



Vulnerability scanning allows an attacker to identify vulnerabilities or weaknesses in a system or network to determine how they can exploit the system. On the other hand, it also assists security professionals in securing the network by determining the security loopholes or vulnerabilities in the current security mechanism before the bad guys could exploit them.

There are two approaches to network vulnerability scanning:

Active Scanning: The attacker interacts directly with the target network to find vulnerabilities

Example: An attacker sends probes and specially crafted requests to the target host in the network in order to identify vulnerabilities.

Passive Scanning: The attacker tries to find vulnerabilities without directly interacting with the target network. The attacker identifies vulnerabilities via information exposed by systems in their normal communications.

Example: An attacker guesses operating system information, applications, and application and service versions, by observing TCP connection setup and teardown.

Attackers scan for vulnerabilities using tools such as Nessus, GFI LanGuard, and Nsauditor Network Security Auditor. Vulnerability scanning enables an attacker to identify network vulnerabilities, open ports and running services, application and services configuration errors, and application and services vulnerabilities.

Nessus performs vulnerability, configuration, and compliance assessment.

Features:

- **Discovery**

  Asset discovery

  Scan IPv4/IPv6/hybrid networks

  Un-credentialed vulnerability discovery

  Credentialed scanning for system misconfigurations and missing patches

- **Broad Asset Coverage and Profiling**

  Network devices: Firewalls/Routers/Switches (Juniper, Check Point, Cisco, Palo Alto Networks), printers, storage

  Offline configuration: auditing of network devices

  Virtualization: VMware ESX, ESXi, vSphere, vCenter

  Operating Systems: Windows, Mac, Linux, Solaris, BSD, Cisco iOS, IBM iSeries

  Databases: Oracle, SQL Server, MySQL, DB2, Informix/DRDA, PostgreSQL

  Web applications: Web servers, web services, OWASP vulnerabilities

Cloud: Deployed as AWS AMI

- **Patch Auditing**

  Integrates with patch management solutions (IBM, Microsoft, Red Hat®, Dell, and VMware®)

- **Control Systems Auditing**

  SCADA systems, embedded devices and ICS applications

- **Sensitive content auditing**

  Personal Identifiable Information (PII) (e.g. credit card numbers, SSNs)

- **Mobile Device Auditing**

  Lists iOS, Android, and Windows Phone 7 devices accessing the network and detects mobile vulnerabilities. Integrates with major MDMs (MSFT, Apple, Good, MobileIron, AirWatch)

- **Automatic Scan Analysis**

  Remediation action priority and scan tuning recommendations

- **Threats: Botnet/Malicious Process/Anti-virus Auditing**

  Detect Viruses, malware, backdoors, hosts communicating with Botnet-Infected systems, known/unknown processes, and web services linking to malicious content

- **Compliance Auditing**

  FFIEC, FISMA, CyberScope, GLBA, HIPAA/ HITECH, NERC, PCI, SCAP, SOX, Configuration, Auditing

- **Configuration Auditing**

  CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA

- **Risk Assessment**

  Risk rankings based on CVE scoring and there are five severity levels: Critical, High, Medium, Low, Info

- **Targeted Email Notifications**

  Targeted email notifications of scan results, remediation recommendations, and scan configuration improvements

- **Results /Report Sharing**

  Automatic post-scan analysis with attachments/screenshots stored in scanning reports (report sharing requires Nessus Enterprise)

Source: *http://www.tenable.com*

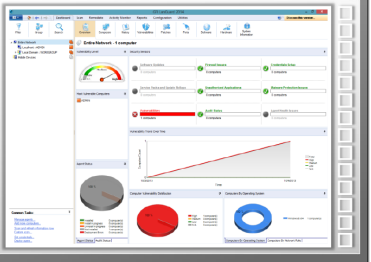
Vulnerability Scanning Tool: GFI LanGuard

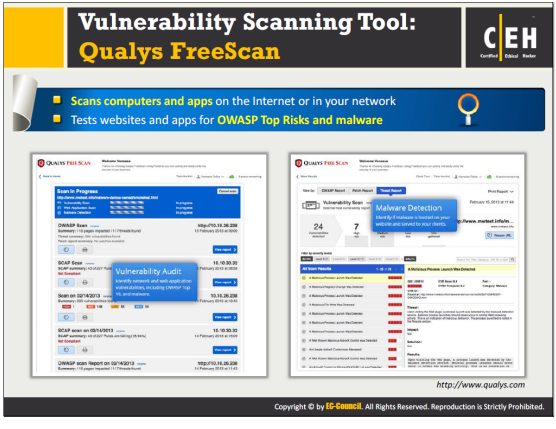
GFI LanGuard assists in **asset inventory**, change management, **risk analysis**, and proving compliance

Features

- Selectively creates **custom vulnerability checks**
- Identifies **security vulnerabilities** and takes remedial action
- Creates different types of **scans and vulnerability tests**
- Helps ensure third-party security applications offer **optimum protection**
- Performs **network device vulnerability checks**

http://www.gfi.com



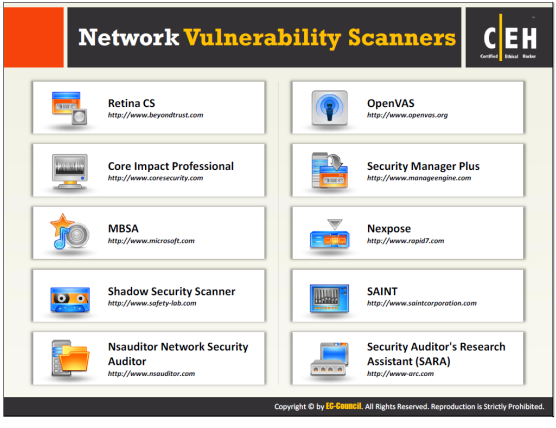


Qualys FreeScan checks network, servers, desktops and web apps for security vulnerabilities. It is a network security tool for business networks, and is limited to 10 unique security scans of Internet accessible assets. It provides a detailed report that helps to correct and fix security threats proactively.

Features:

- Scans computers and apps on the Internet or in the network
- Detects security vulnerabilities and the patches needed to fix them
- Enables viewing of interactive scan reports by threat or by patch
- Tests websites and apps for OWASP Top Risks and malware
- Tests computers against SCAP security benchmarks

Source: *http://www.qualys.com*



Network vulnerability scanners help in identifying vulnerabilities in the target network or network resources by means of vulnerability assessment and network auditing.

Some network vulnerability scanners are listed below:

Retina CS

Source: *http://www.beyondtrust.com*

Retina CS delivers large-scale, cross-platform vulnerability assessment and remediation, with available configuration compliance, patch management and compliance reporting. Retina CS Enterprise Vulnerability Management allows the user to:

- Discovers network, web, mobile, cloud, and virtual infrastructure
- Profiles asset configuration and risk potential
- Pinpoints vulnerabilities, malware, and attacks
- Analyzes threat potential and return on remediation
- Allows remediation of vulnerabilities via integrated patch management
- Reports on vulnerabilities, compliance, benchmarks, and so on
- Protects endpoints against client-side attacks

Core Impact Professional

Source: http://www.coresecurity.com

Core Impact® Professional is the comprehensive software solution for assessing and testing security vulnerabilities throughout the organization. It tests across a broad spectrum of risk areas, including:

- Endpoint systems
- Passwords and identities
- Mobile device
- Wireless networks
- Web applications and services
- Network systems and devices

MBSA

Source: http://www.microsoft.com

Microsoft Baseline Security Analyzer (MBSA) allows administrators to scan local and remote systems for missing security updates as well as common security misconfigurations.

Shadow Security Scanner

Source: http://www.safety-lab.com

Safety Lab Shadow Security Scanner scans for network security vulnerabilities. It provides a secure, prompt, and reliable detection of a vast range of security system holes. After completing the system scan, it analyzes the data collected, locates vulnerabilities, and possible errors in server tuning options, and suggests possible problem-solving methods.

Nsauditor Network Security Auditor

Source: http://www.nsauditor.com

Nsauditor Network Security Auditor is a network security auditing tools suite designed for network auditing, network scanning, vulnerability scanning, network monitoring, and so on.

Features:

- Scans networks and hosts for vulnerabilities and provide security alerts
- Checks enterprise network for all potential methods that a hacker might use to attack it, and creates a report of potential problems that were found
- Provides insight into services running locally, with the option of digging down into each connection and analyzing the remote system, terminating connections, and viewing data
- Helps network administrators identify security holes and flaws in their networked systems
- Includes a firewall system, real-time network monitoring, packet filtering, and analyzing software

OpenVAS

Source: http://www.openvas.org

OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.

Features:

- **OpenVAS Scanner:** Target hosts are scanned concurrently, OpenVAS Transfer Protocol (OTP), SSL support for OTP (always), WMI support (optional).
- **OpenVAS Manager:** OpenVAS Management Protocol (OMP), SQL Database (sqlite) for configurations and scan results, SSL support for OMP (always), concurrent scans tasks (OpenVAS Scanners), scheduled scans, master-slave mode to control many instances from a central one, and Reports Format Plugin framework with various plugins (for XML, HTML, LateX, etc.).
- **OpenVAS CLI:** Client for OMP (runs on Windows, Linux, etc.), plugin for Nagios.

Security Manager Plus

Source: http://www.manageengine.com

Security Manager Plus is a network security scanner that reports on network vulnerabilities and helps to remediate them and ensure compliance. It protects the network from security threats and malicious attacks with vulnerability scanning, open ports detection, patch management, Windows file/folder/registry change management, and vulnerability reporting capabilities.

Nexpose

Source: http://www.rapid7.com

Nexpose is a vulnerability scanner that discovers, prioritizes, and remediates security threats in the network, which helps to:

- **Know your network**: Provides clear visibility by discovering and assessing risks to the business across physical, virtual, and cloud environments.
- **Prioritize** and **manage risk** effectively.
- Simplify **compliance effort**: Enables organizations to stay compliant with PCI DSS, NERC CIP, FISMA, HIPAA/HITECH, SANS Top 20 CSC, DISA STIGS, USGCB and CIS standards for risk, vulnerability, and configuration management requirements.

SAINT

Source: http://www.saintcorporation.com

SAINT (System Administrator's Integrated Network Tool) is a vulnerability scanner that uncovers areas of weakness in the network and recommends fixes.

Features:

- Identifies vulnerabilities on network devices, operating systems, desktop applications, Web applications, databases, and so on

- Allows the detection and reparation of possible weaknesses in network's security before they can be exploited by intruders
- Allows the anticipation and prevention of common system vulnerabilities
- Demonstrates compliance with current government and industry regulations, such as PCI DSS, NERC, FISMA, SOX, GLBA, and HIPAA
- Performs configuration audits with policies defined by FDCC, USGCB, and DISA

Security Auditor's Research Assistant (SARA)

Source: http://www-arc.com

The Security Auditor's Research Assistant (SARA) is a network security analysis tool that integrates the National Vulnerability Database (NVD), performs SQL injection tests, performs exhaustive XSS tests, adapts to many firewalled environments, and supports remote self-scan and API facilities. It is used for CIS benchmark initiatives and has plug-in facility for third-party apps, and offers CVE standards support, an enterprise search module, standalone or daemon mode, and so on.

Some of the vulnerability scanning tools for mobile devices are listed below:

Retina CS for Mobile

Source: *http://www.beyondtrust.com*

Retina CS for Mobile is the industry's innovative approach to security, policy, and health management for mobile devices. It provides comprehensive vulnerability management for mobile devices, smart phones, and tablets. It integrates mobile device assessment and vulnerability management for proactively discovering, prioritizing, and fixing smartphone security weaknesses.

Features:

- Reduce risk across BlackBerry, Android, and ActiveSync-managed mobile devices
- Access reports locally via the mobile app and alongside enterprise vulnerability data in the BeyondInsight console
- Ease compliance via in-depth mobile vulnerability management audit trails
- Reveal vulnerability profiles of mobile devices accessing the network
- Streamline remediation through severity-based mobile threat prioritization
- Audit mobile device hardware, applications, and configurations
- Rely on automatic vulnerability audit updates from BeyondSaaS

SecurityMetrics MobileScan

Source: *https://www.securitymetrics.com*

SecurityMetrics MobileScan is a mobile defense tool that helps to identify mobile device vulnerabilities to protect the customer's sensitive data. It helps to avoid threats that originate from mobile malware, device theft, Wi-Fi network connectivity, data entry, personal and business use, unwarranted app privileges, data and device storage, account data access, Bluetooth, Infrared (IR), Near-field communication (NFC), and SIM and SD cards.

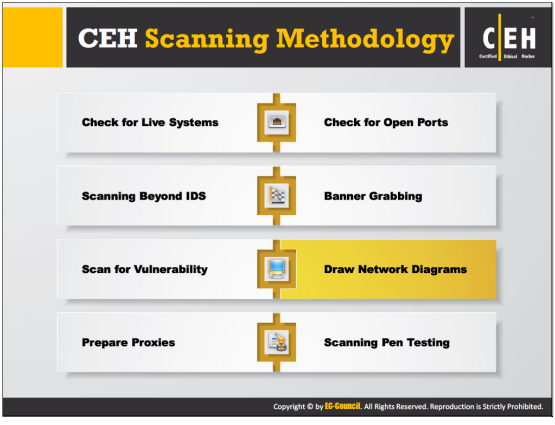
SecurityMetrics MobileScan complies with PCI SSC (Payment Card Industry Security Standards Council) guidelines to prevent mobile data theft. On completion of a scan, the report generated comprises a total risk score, summarization of discovered vulnerabilities, and recommendations on how to resolve threats.

Nessus Vulnerability Scanner

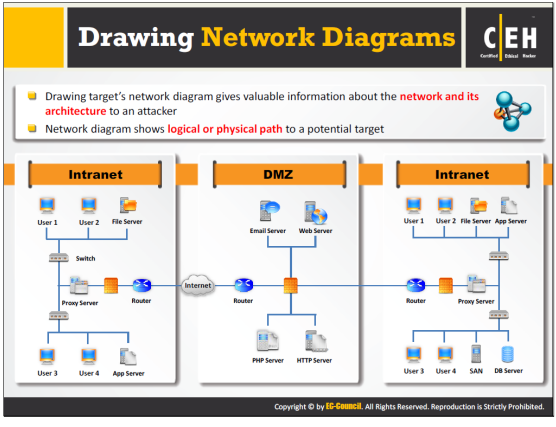
Source: *http://www.tenable.com*

Security administrators and compliance auditors can use the Tenable Nessus® vulnerability scanner and its built-in integration with Apple® Profile Manager, Microsoft® Exchange via Active Directory®, MobileIron MDM, and Good Technology™ Good for Enterprise to:

- Enumerate iOS, Android-based, and Windows Phone devices accessing the corporate network
- Provide detailed mobile device information, including serial number, model, version, timestamp of last connection, and user
- Detect known mobile vulnerabilities, including out-of-date versions of Apple iOS
- Discover “jailbroken” iOS devices

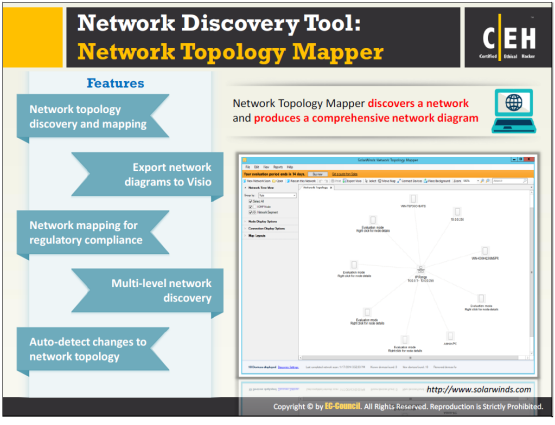


A network diagram helps in analyzing complete network topology. This section highlights the importance of the network diagram, how to draw one, how an attacker uses one to launch an attack, and the tools that help in drawing network maps.



Drawing a network diagram helps an attacker identify the topology or architecture of a target network. The network diagram also helps to trace out the path to the target host in the network and enables the attacker to understand the position of firewalls, IDSs, routers, and other access control devices. Once the attacker has this information, he/she can try to find the vulnerabilities or weak points of those security mechanisms. Then, the attacker can exploit those security weaknesses to find his/her way into the network.

The network diagram also helps network administrators manage their networks. Attackers use network discovery or mapping tools to draw network diagrams of target networks. An example of a network diagram is illustrated in the slide.



Network Topology Mapper allows one to automatically discover and create a network map of the target network. It is also able to display in-depth connections such as OSI Layer 2 and Layer 3 topology data (e.g. displaying switch-to-switch, switch-to-node, and switch-to-router connections). It can keep track of network changes and allow the user to perform inventory management of hardware and software assets.

Features:

- **Network topology discovery and mapping**

  Automatically discovers entire network and creates comprehensive, detailed network maps

- **Export network diagrams to Visio**

  Exports network diagrams to Microsoft Office® Visio®, Orion Network Atlas, PDF, and PNG formats

- **Network mapping for regulatory compliance**

  Allows one to directly address PCI compliance and other regulations that require maintenance of an up-to-date network diagram

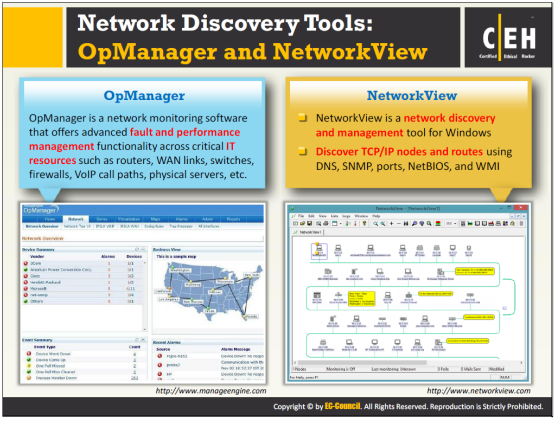
- **Multi-level network discovery**

  Performs multi-level network discovery to produce an integrated OSI Layer 2 and Layer 3 network map that includes detailed device information

- **Auto-detection of changes to network topology**

  Automatically detects new devices and changes to network topology with scheduled network scanning

Source: *http://www.solarwinds.com*



OpManager

Source: *http://www.manageengine.com*

OpManager is a network performance management and monitoring tool that offers advanced fault and performance management functionality across critical IT resources such as routers, WAN links, switches, firewalls, VoIP call paths, physical servers, virtual servers, domain controllers, and other IT infrastructure devices. This tool is helpful in discovering the specific network automatically. It can also present a live network diagram that helps to visualize and pinpoint network outages and performance degradation.

Features:

- Availability and uptime monitoring
- Network traffic analysis
- IP address management
- Switch port mapper
- Network performance reporting
- Network configuration management
- Exchange-server monitoring
- Active directory monitoring

- Hyper-V monitoring
- SQL Server monitoring

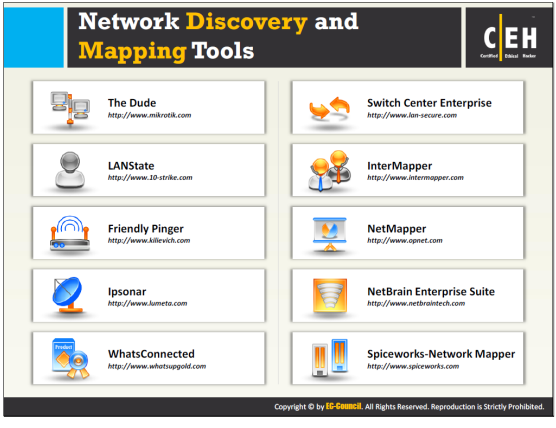
Network Discovery Tool: NetworkView

Source: *http://www.networkview.com*

NetworkView is a network discovery and management tool for Windows.

Features:

- Discover TCP/IP nodes and routes using DNS, SNMP, Ports, NetBIOS, and WMI
- Get MAC addresses and NIC manufacturer names
- Monitor nodes and receive alerts
- Document with printed maps and reports
- Control and secure network with the SNMP MIB browser, the WMI browser, and the port scanner



Network discovery and mapping tools allow you to view the map of your network. They help you detect rogue hardware and software violations, and notify you whenever a particular host becomes active or goes down. Thus, you can also determine server outages or problems related to performance. An attacker can use the same tools to draw a diagram of the target network, analyze the topology, find the vulnerabilities or weak points, and launch an attack by exploiting them.

Some of the tools an attacker uses to create a network map are discussed below:

The Dude

Source: *http://www.mikrotik.com*

The Dude is a network-monitoring tool designed to represent network structure in one or more cross-linked graphical diagrams, allowing you to draw and monitor your network. It will automatically scan all devices within specified subnets, draw and layout a map of your networks, and monitor services of your devices to alert you to problems.

LANState

Source: *http://www.10-strike.com*

LANState is a network mapping and monitoring application used for corporate Microsoft Windows network management and administration. This tool helps to scan the network, find hosts, place them on a network diagram, and monitor their state visually. It builds a network

map automatically by scanning the Windows network neighborhood or IP address range, and exports network diagrams to graphic images, Microsoft Visio, and XML files.

Friendly Pinger

Source: http://www.kilievich.com

Friendly Pinger is an application for network administration, monitoring, and inventory.

Features:

- Visualization of computer network
- Monitoring of network devices availability
- Notification when any server wakes up or goes down
- Ping of all devices in parallel
- Auditing of software and hardware components installed on the computers over the network
- Tracking of user access and files opened on the computer via the network
- Assignment of external commands (like telnet, tracert, net.exe) to devices
- Searching of HTTP, FTP, e-mail and other network services

IPsonar

Source: http://www.lumeta.com

IPsonar is a network discovery tool that discovers network assets, including those not currently under management, and maps the connectivity between assets and networks to help with issues such as mergers and acquisitions, IT compliance, cyber security, critical infrastructure protection, data leak prevention, and large-scale network transformations and roll-outs. It provides visibility into every IP asset, host, node, and connection on the network. IPsonar includes, for example, network discovery, host discovery, service discovery, enhanced perimeter discovery, and layer 2 discovery.

WhatsConnected

Source: http://www.whatsupgold.com

WhatsConnected is a layer 2/3 discovery, mapping, inventory, and asset reporting tool. It automatically discovers, maps, inventories and documents your network (devices, servers, workstations, virtual resources, hardware, and software assets) and port-to-port connectivity. It allows you to document your network, topology maps, and network diagrams for regulatory compliance, ensure complete accuracy, and visualize how everything is connected.

Switch Center Enterprise

Source: http://www.lan-secure.com

Switch Center is network management and monitoring software for managed network switches, routers, and hubs from any vendor supporting SNMP BRIDGE-MIB that helps to discover, monitor, and analyze network connectivity and performance, and provides real-time

network discovery, mapping, and topology solutions for IT environments. The tool provides network topology mapping and performance monitoring of local and remote network devices. It supports SNMPv1/2 and SNMPv3 discovery options, including VLANs monitoring engine and port mapping capabilities. The built-in central software viewer supports multiple management levels, and provides automatic network discovery and mapping using OSI Layer 2 and Layer 3 topology monitoring, including real-time reports, statistics, and alerts.

InterMapper

Source: http://www.intermapper.com

The InterMapper suite of network monitoring software includes network mapping functionality. It helps you visualize network topology and allows you to arrange maps in physical, logical, or geographic layouts. It provides color-coded icons, which indicate the performance level of routers, switches, servers, workstations, and so on.

NetMapper

Source: http://www.opnet.com

NetMapper is a network mapping tool that automatically generates up-to-date network maps and inventory reports. It automatically discovers network elements and configuration, creates high definition network diagrams by correlating configuration and operational data, understands multi-device relationships (e.g., HSRP, OSPF, BGP, VLANs, Spanning Tree) to generate physical and logical diagrams, and archives diagrams to maintain historical information and track changes.

NetBrain Enterprise Suite

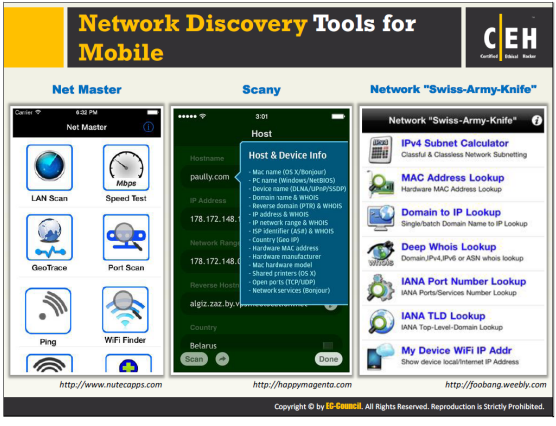
Source: http://www.netbraintech.com

NetBrain Enterprise Suite automates critical network tasks such as documentation, troubleshooting diagnosis, and change verification. It automates topology diagrams, inventory reports, and design documents, and keeps them updated automatically.

Spiceworks-Network Mapper

Source: http://www.spiceworks.com

Spiceworks Network Mapper displays an interactive network diagram of how network devices relate to each other. One can manually add, edit, move and resize devices to exactly reflect your network, and even choose filters and views to display the device details in the network map. It diagrammatically represents which device is consuming the most bandwidth. On the network map, one can view info such as IP address, serial number, and bandwidth usage of a device over time, by clicking on the device.



Given below are network discovery tools for mobile devices:

Net Master

Source: *http://www.nutecapps.com*

Net Master is a mobile solution for network analysis and diagnostic problems. It is a utility application developed for Network Administrators and IT Professionals but presented in a format targeted for non-professionals.

It comprises of essential networking tools given below:

LAN Scan: For complete scanning and diagnostics of all devices connected to a Local Area Network. It includes:

- TCP Connect LAN Scanning, ARP table scan, NetBIOS Scan, Bonjour Scan and Port Scanning
- Reverse DNS Lookup
- Wake On LAN functionality
- Dictionary lookups for MAC addresses, port addresses, and many Bonjour Services

Speed Test: Monitors cellular (3G/4G/LTE) or Wi-Fi connection rate and response to the mobile device. It tests Internet speed, download rate, upload rate, and latency (response) time.

Port Scanning: Checks what services are listening on a network and is useful for making sure no service ports are open that should not be.

- Multi-thread TCP port scanner on cellular or Wi-Fi network
- Performs Quick scan for the most popular ports
- Display common protocol used by each open port and allow connection if port protocol known
- Scanning parameters can be adjusted to handle different network environments

Geographical Trace Route: Determines the route path and measures the transit times across an IP network.

- Uses an Asynchronous Trace algorithm to provide results faster
- Graphical plotting of ping results for all hops
- Geolocation information for hops
- Reverse Hostname (DNS Information)
- IP Address of each hop
- Monitors average packet round trip time
- Packet count and lost information
- WHOIS hostnames and IP address range
- Works over Wi-Fi or cellular network connection
- Save previous traces to review later

Ping: Determines the availability of a host via a domain name or IP address.

- Bookmark feature allows the user to store and monitor multiple game servers' latency
- Email ability for saving results

Wi-Fi Finder: It is a Wi-Fi hotspot locator that includes Yelp business information and reviews for each hotspot.

- Finds FREE or paid Wi-Fi hotspots from your current location
- Integrated with Yelp database to provide complete information on the business associated with each Wi-Fi hotspot
- View Wi-Fi hotspot search results in a list view or on a map without leaving the app
- Look up business addresses and phone numbers for Wi-Fi hotspots

Subnet Calculator: Provides information needed to make decisions regarding subnetting.

Scany

Source: http://happymagenta.com

Scany, a network scanner app for iPhone and iPad, scans LAN, Wi-Fi networks, web sites, open ports, discovers network devices and digs network info. It supports a number of networking protocols and anti-stealth technologies. It is a multifunctional networking instrument for finding connected devices, looking up detailed device information, network troubleshooting, scanning ports, and testing network security and firewalls.

Features:

- Scan both LAN and the Internet
- Scan any IP address or network range
- Bonjour hostnames lookup
- Windows hostnames lookup (NetBIOS, Samba)
- Device names lookup (UPnP, SSDP, DLNA)
- Country of origin detection of the network owner
- Network range and AS number lookup
- MAC address and hardware vendor lookup
- Wake on LAN or Wi-Fi (by MAC address)
- Wake over the Internet (using proper routers)
- Ping/Trace hosts with integrated tools
- WHOIS hostnames, IP addresses, ASNs
- Know Wi-Fi, VPN, 3G/EDGE and external IPs
- Checks ICMP, TCP and UDP
- Faster asynchronous network I/O
- Works with Wi-Fi, 3G, EDGE and GPRS

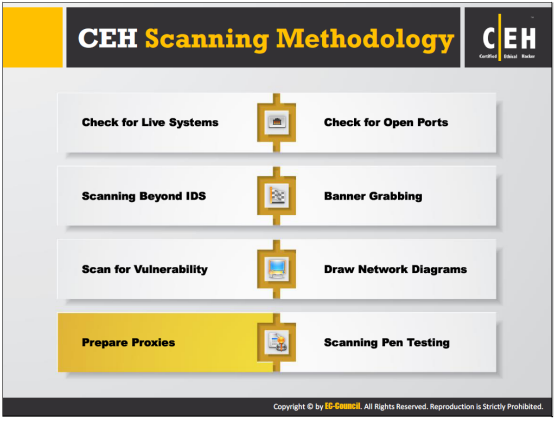
Network "Swiss-Army-Knife"

Source: http://foobang.weebly.com

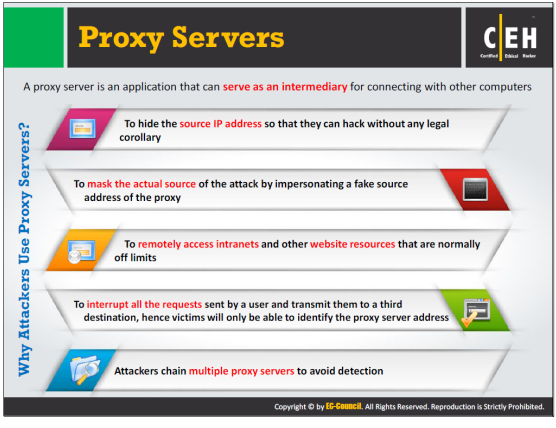
Network "Swiss-Army-Knife" is a network application for iPhone to perform tasks mentioned below:

- Calculate IPv4 subnet (Classful and Classless) and all the related valid subnet information
- Find Offline hardware MAC address to organization lookup and vice versa
- Perform Single/Batch Domain-name lookup: For a list of domain names, equivalent IP address can be found

- Perform Whois lookup directly from the idevice. Whois lookup allows one to query list of NICes for details information. Lookup relays on IP addresses either IPv4 or IPv6, domain name or AS Number. Results can be stored on a local repository for future reference.
- Offline IANA Port number lookup: allows IANA assigned port number to name and vice versa
- IANA Top level domain lookup: identifies which countries domain end with .cz, .cv, .su etc.
- My device Wi-Fi IP addr: allows to identify your local device Wi-Fi IP address



This section describes proxy servers, why an attacker uses proxy server, how she/he uses proxy to launch attacks, and various proxy tools.



A proxy server is an application that can serve as an intermediary for connecting with other computers.

Proxy server is used:

- As a firewall, and to protect the local network from outside attacks
- As an IP address multiplexer, allowing a number of computers to connect to the Internet when you have only one IP address (NAT/PAT)
- To anonymize web surfing (to some extent)
- To filter out unwanted content, such as ads or "unsuitable" material (using specialized proxy servers)
- To provide some protection against hacking attacks
- To save bandwidth

How a proxy server works?

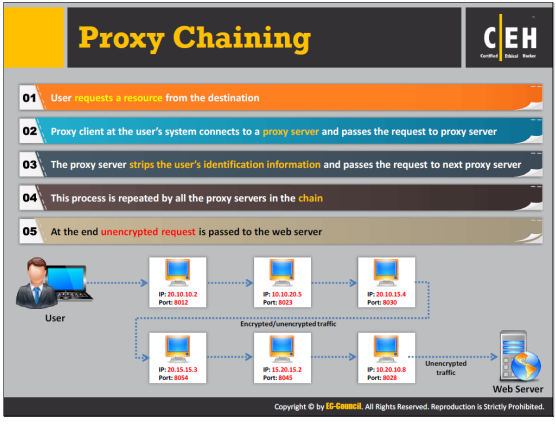
Initially, when you use a proxy to request a particular web page on an actual server, the proxy server receives it. The proxy server then sends your request to the actual server on behalf of your request—it mediates between you and the actual server to send and respond to the request, as shown in Figure 3.4.

FIGURE 3.4: Attacker using a proxy server for connecting to the target

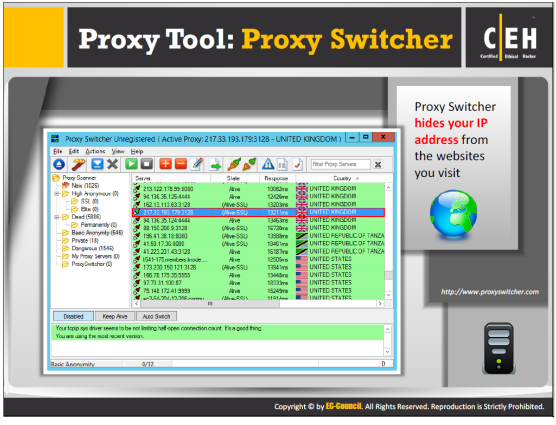
In this process, the proxy receives the communication between the client and the destination application. To take advantage of a proxy server, an attacker must configure client programs so that they can send their requests to the proxy server instead of the final destination.

Why Attackers Use Proxy Servers?

It is easier for an attacker to attack or hack a particular system than to conceal the attack source. Therefore, the main challenge for an attacker is to hide his/her identity so that he/she cannot be traced. Thus, the attacker uses the proxy server to avoid detection of attack evidence by masking his/her IP address. When the attacker uses a proxy to connect to the target system, the server logs record the proxy's source address, rather than the attacker's source address.



Proxy chaining helps an attacker to increase his/her Internet anonymity. Internet anonymity depends on the number of proxies used for fetching the target application: the larger the number of proxy servers used, the greater the attacker's anonymity.

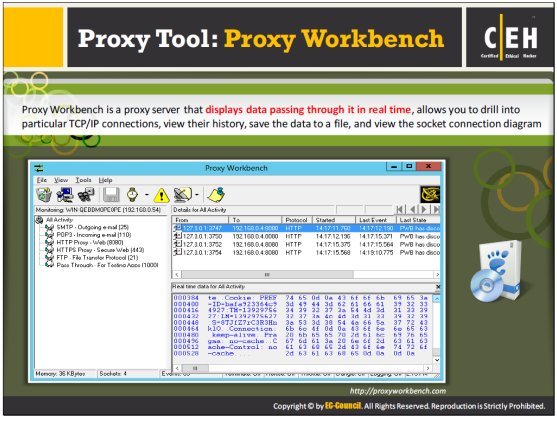


Proxy Switcher allows you to surf anonymously on the Internet without disclosing your IP address. It also helps you to access various blocked sites in the organization. It avoids all sorts of limitations imposed by target sites.

Features:

- Hides your IP address from the web sites you visit
- Penetrate bans and blocks on forums, classifieds, and download sites (e.g., rapidshare)
- Automatic proxy server switching for improved anonymous surfing
- Full support of password-protected servers
- Full support of Socks v5 and Elite servers

Source: http://www.proxyswitcher.com

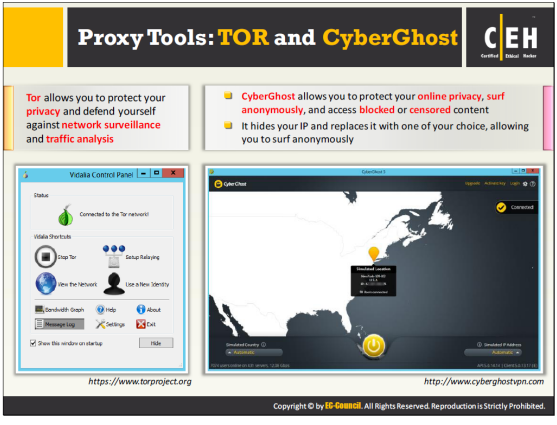


Proxy Workbench is a proxy server that displays the data passing through it in real time and allows you to drill into particular TCP/IP connections, view their history, save the data to a file, and view the socket connection diagram. The socket connection diagram is an animated graphical history of all of the events that took place on the socket connection.

Features:

- Connection failure simulation strategies allow you to simulate:
  - Slow or asymmetric Internet connections (bandwidth throttling)
  - Servers that are underpowered, overloaded or under attack (connection refusal)
  - Intermittent connections (connection termination)
  - Disconnected network cables (connection dangling)
  - Data floods and droughts
- Native ability to analyze HTTP, FTP, SOAP, HTTPS (secure sockets), POP3, Web services and "pass through" communications
- The data can be presented in 5 formats: ASCII, hexadecimal, octal, decimal, or binary

Source: http://proxyworkbench.com



Some proxy tools are discussed below:

Proxy Tool: TOR

Source: *https://www.torproject.org*

Tor is software and an open network that helps to defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

Features:

- Provides anonymous communication over the Internet
- Ensures the privacy of both sender and recipient of a message
- Provides multiple layers of security to a message
- Uses cooperating proxy routers throughout the network
- The initiating “onion” router (a "Tor client") determines the path of transmission
- Enables software developers to create new communication tools with built-in privacy features
- Allows connection to news sites and instant messaging services when they are blocked by the local Internet providers

Proxy Tool: CyberGhost

Source: *http://www.cyberghostvpn.com*

CyberGhost VPN allows users to protect their online privacy, surf anonymously, and access blocked or censored content.

Features:

- **Privacy**: hides your IP and replaces it with one of your choice. This way, you surf anonymously.
- **Security:** encrypts your connection and does not keep logs, thus securing data.
- **Freedom**: allows access to censored or geo-restricted content.

In addition to the proxy tools mentioned before, there are many other proxy tools intended to allow users to surf the Internet anonymously. Discussed below are some additional proxy tools:

SocksChain

Source: *http://ufasoft.com*

SocksChain is a program that allows working with any Internet service through a chain of SOCKS or HTTP proxies to hide the real IP address. SocksChain can function as a usual SOCKS server that transmits queries through a chain of proxies. Attackers use SocksChain with client programs that do not support the SOCKS protocol but work with one TCP connection, such as TELNET, HTTP, and IRC (FTP uses two connections). It hides your IP address in the server's logs or mail headers.

Burp Suite

Source: *http://www.portswigger.net*

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work together to support the entire testing process, from initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities.

Burp Suite contains:

- An intercepting Proxy, which lets you inspect and modify traffic between your browser and the target application

- An application-aware Spider, for crawling content and functionality
- An advanced web application Scanner, for automating the detection of numerous types of vulnerability
- An Intruder tool, for performing customized attacks to find and exploit unusual vulnerabilities
- A Repeater tool, for manipulating and resending individual requests
- A Sequencer tool, for testing the randomness of session tokens
- Extensibility, for writing your own plugins, to perform complex and highly customized tasks within Burp

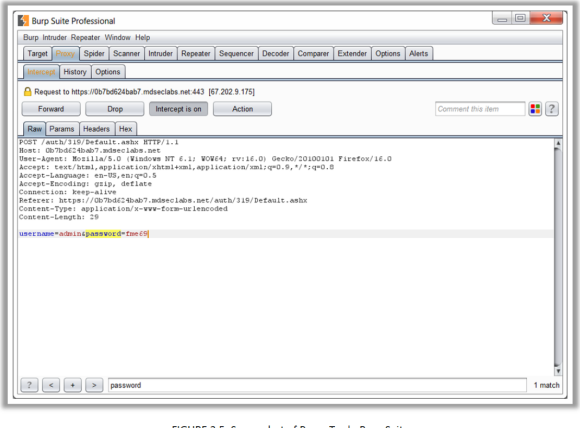


FIGURE 3.5: Screenshot of Proxy Tool - Burp Suite

Proxifier

Source: *https://www.proxifier.com*

Proxifier allows network applications that do not support working through proxy servers to operate through a SOCKS or HTTPS proxy and chains.

Proxy Tool Windows App

Source: *http://webproxylist.com*

Proxy Tool Windows App is a Windows App tool that allows you to automatically download the checked/tested/filtered proxy list(s) from Proxylist.co server directly, using your username and password to your proxy list directory on your Windows hard drive (e.g., C:\Scrapebox\proxies\).

Charles

Source: http://www.charlesproxy.com

Charles is an HTTP proxy/HTTP monitor/reverse proxy that enables you to view all the HTTP and SSL/HTTPS traffic between your machine and the Internet. This includes requests, responses, and HTTP headers (which contain the cookies and caching information).

Fiddler

Source: http://www.telerik.com

Fiddler is a web debugging proxy for any browser, system, or platform. It logs all HTTP(s) traffic between a computer and the Internet to perform security testing of web applications, manipulate and edit web sessions, an run performance tests, among other things.

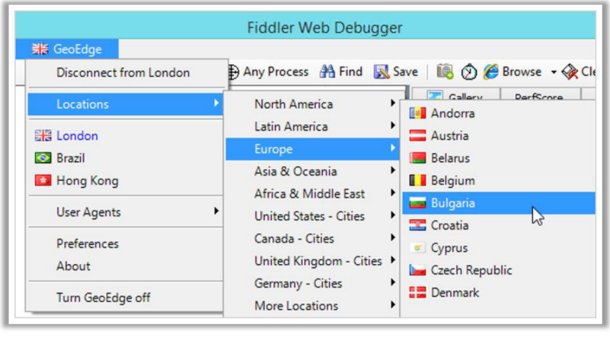


FIGURE 3.6: Screenshot of Proxy Tool - Fiddler

Proxy

Source: http://www.analogx.com

AnalogX Proxy is a server that allows any other machine on your local network to route its requests through a central machine. It supports HTTP, HTTPS, POP3, SMTP, NNTP, FTP, Socks4/4a, and partial Socks5 (no UDP) protocols.

Protoport Proxy Chain

Source: http://www.protoport.com

Protoport Proxy Chain is a proxy tool that allows surfing anonymously using up to 10 chained proxy servers. With Protoport Proxy Chain software, you can build a chain of proxy servers from different countries.

Features:

- Cut off cookies, user agency, and language from browser requests
- Automatically rank proxy servers, with the fastest servers at the top of list
- Automatically download a fresh list of proxy servers from website
- Parse any text for proxy servers; copy and paste it into Protoport Proxy Chain

ProxyCap

Source: http://www.proxycap.com

ProxyCap enables you to redirect your computer's network connections through proxy servers. You can use ProxyCap define which applications will connect to the Internet through a proxy and under what circumstances. It provides a user-friendly interface and does not need to reconfigure Internet clients. ProxyCap provides native support for the SSH protocol, allowing you to specify a SSH server as the proxy server.

Features:

- Support for SOCKS and HTTPS proxy servers
- Built-in support for SSH tunneling
- Support for "pure" HTTP proxying
- Support for TCP- and UDP-based network protocols
- Support for proxy chains
- Built-in proxy checker

CCProxy

Source: http://www.youngzsoft.net

CCProxy is a proxy server that supports broadband, DSL, dial-up, optical fiber, satellite, ISDN, and DDN connections, it helps to build your own proxy server and share the Internet connection in the LAN. CC Proxy Server can act as an HTTP, mail, FTP, SOCKS, news, telnet, and HTTPS proxy server. It features account management functions, including Internet access control, bandwidth control, Internet web filtering, content filtering, and time control. It also provides web caching, online access monitoring, access logging, and bandwidth usage statistics.

Given below are proxy tools for mobile devices:

Proxy Browser for Android

Source: *https://play.google.com*

Proxy Browser for Android helps to browse blocked websites at school, work, or the library, or any site protected by a firewall.

Features:

- Compatible with Facebook mobile and Twitter mobile
- Unblock sites and surf anonymously
- Unblock parental control
- User Agent support (e.g., iPhone/blackberry/android/pc/mac/Linux)
- Surf the Internet incognito with a hidden IP address
- Three proxies (two IP Address) for better performance
- Modifiable cookies
- No browsing history

ProxyDroid

Source: https://github.com

ProxyDroid is an app that can help to set the proxy (http / socks4 / socks5) on Android devices.

Features:

- Support HTTP/HTTPS/SOCKS4/SOCKS5 proxy
- Support basic/NTLM/NTLMv2 authentication methods
- Individual proxy for only one or several apps
- Multiple profiles support
- Bind configuration to WIFI's SSID / Mobile Network (2G/3G)
- Widgets for switching on/off proxy
- Low battery and memory consumption (written in C and compiled as native binary)
- Bypass custom IP address
- DNS proxy for guys behind the firewall that disallows to resolve external addresses
- PAC file support

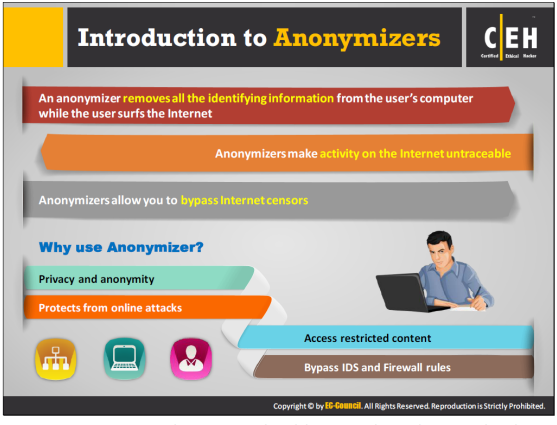
NetShade

Source: http://www.raynersw.com

NetShade is a Proxy and VPN service for the Mac and iOS. It allows you to watch overseas videos, surf anonymously, and secure the Internet traffic from eavesdroppers. One can choose between a Proxy and VPN connection, or combine the two for maximum security and anonymity. The following are the three connection modes for utmost security:

- **Proxy:** A HTTP proxy server acts as a relay for your web connections. Proxy servers have no effect on encryption and they only deal with web traffic. As with a regular web connection, only HTTPS format encrypts the data.
- **VPN (Virtual Private Network):** A secure encrypted tunnel between a user and a remote computer or network. In the case of NetShade, the tunnel goes between the user and one of the NetShade's servers. NetShade's server then provides the user with a securely encrypted link to the Internet.
- **Proxy + VPN:** A dual-mode setup that enables additional anonymity by adding an HTTP proxy to the VPN tunnel. The VPN layer is closer to the user computer, where the proxy layer sits between the VPN servers and the Internet. In this mode, the connection bounces from VPN to Proxy to host.

Besides the proxy tools discussed earlier, there are a number of free proxy servers available on the Internet that help you access restricted sites without revealing your IP address. In the Google search engine, type "Free Proxy Servers" to see a listing of them. Select one among the list to download, and browse anonymously without revealing your legitimate IP address.



An anonymizer is an intermediate server placed between the end user and web site that accesses the website on behalf of you, making your web surfing untraceable. An anonymizer eliminates all the identifying information (IP address) from your system while you are surfing the Internet, thereby ensuring privacy. Most anonymizers can anonymize the web (http :), file transfer protocol (ftp :), and gopher (gopher :) Internet services.

To visit a page anonymously, you can visit your preferred anonymizer site, and enter the name of the target website in the Anonymization field. Alternately, you can set your browser home page to point to an anonymizer, in order to anonymize subsequent web access. Apart from this, you can choose to anonymously provide passwords and other information to sites that request you, without revealing any other information, such as your IP address. Crackers may configure an anonymizer as a permanent proxy server by making the site name the setting for the HTTP, FTP, Gopher, and other proxy options in their applications configuration menu, thereby cloaking their malicious activities.

Why Use an Anonymizer?

The reasons for using anonymizers include:

- **Ensuring privacy**: Protect your identity by making your web navigation activities untraceable. Your privacy is maintained until and unless you disclose your personal information on the web, for example, by filling out forms.
- **Accessing government-restricted content**: Most governments prevent their citizens from accessing certain websites or content deemed inappropriate or containing

sensitive information. However, these sites can still be accessed using an anonymizer located outside the target country.

- **Protection against online attacks**: An anonymizer can protect you from all instances of online pharming attacks by routing all customer Internet traffic via its protected DNS server.
- **Bypassing IDS and firewall rules**: Firewalls are typically bypassed by employees or students accessing websites that they are not supposed to access. An anonymizer service gets around your organization's firewall by setting up a connection between your computer and the anonymizer service. By doing so, firewalls see only the connection from your computer to the anonymizer's web address. The anonymizer will then connect to any website (e.g., Twitter) with the help of an Internet connection, and then direct the content back to you. To your organization, your system appears to be connected simply to the anonymizer's web address, but not to the actual site to which you've browsed.

In addition to protecting users' identities, anonymizers can also be used to attack a web site without being traced.

Types of Anonymizers

An anonymizer is a service through which one can hide their identity when using certain Internet services. It encrypts the data from your computer to the Internet service provider. Anonymizers are of two basic types:

- Networked anonymizers
- Single-point anonymizers

Networked Anonymizers

A networked anonymizer first transfers your information through a network of Internet-connected computers before passing it on to the website. Because the information passes through several Internet computers, it becomes more cumbersome for anyone trying to track your information to establish the connection between you and the anonymizer.

Example: If you want to visit any web page, you have to make a request. The request will first pass through A, B, and C Internet computers prior to going to the website.

Advantage: Complication of the communications makes traffic analysis complex.

Disadvantage: Any multi-node network communication incurs some degree of risk of compromising confidentiality at each node.

Single-Point Anonymizers

Single-point anonymizers first transfer your information through a website before sending it to the target website, and then pass back information, i.e., gathered from the targeted website, through a website, and then back to you to protect your identity.

Advantage: Arms-length communication protects IP address and related identifying information.

Disadvantage: It offers less resistance to sophisticated traffic analysis.

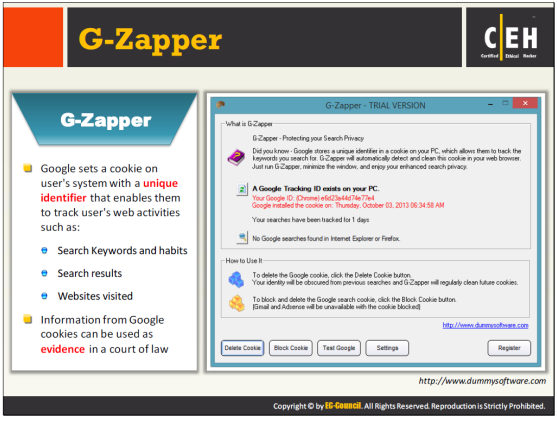
Censorship Circumvention Tool: Tails

Tails is a **live operating system**, that user can start on any computer from a DVD, USB stick, or SD card

It aims at preserving privacy and anonymity and helps you to:

- Use the **Internet anonymously and circumvent censorship**
- **Leave no trace** on the computer
- Use **state-of-the-art cryptographic tools** to encrypt files, emails and instant messaging

https://tails.boum.org



G-Zapper is a utility to block or clean Google cookies, and help you stay anonymous while searching online. It also helps to protect your identity and search history. G-Zapper will read the Google cookie installed on the computer, display the date it was installed, determine how long your searches have been tracked, and display your Google searches. It allows you to automatically delete or entirely block the Google search cookie from future installation. In addition, G-Zapper will block Google Analytics from tracking the web sites you visit.

Source: *http://www.dummysoftware.com*

An anonymizer allows you to mask your IP address to visit websites without being tracked or identified, keeping your activity private. It allows you to access blocked content on the Internet with omitted advertisements. Some anonymizers are discussed below:

Proxify

Source: http://proxify.com

Proxify is an anonymous proxy service that allows to surf the Web privately and securely. Through Proxify, one can use websites without your being uniquely identified or tracked. It hides your IP address, and the encrypted connection prevents monitoring of your network traffic.

Psiphon

Source: http://psiphon.ca

Psiphon is a circumvention tool from Psiphon Inc. that utilizes VPN, SSH, and HTTP Proxy technology to provide you with uncensored access to Internet content. Psiphon client will automatically discover new access points to maximize the chances of bypassing censorship restrictions. Thus, Psiphon provides you with open access to online content.

Anonymous Web Surfing Tool

Source: http://www.anonymous-surfing.com

Anonymous Web Surfing tool hides the IP address from being visible while browsing the Internet. It uses 128-bit SSL encrypted connection to encrypt your Internet traffic and prevents the ISP or administrators from tracking Internet activities.

Hide Your IP Address

Source: http://www.hideyouripaddress.net

Hide Your IP Address protects your privacy on the Internet by hiding your IP Address online.

Features:

- Protect and hide your Identity by hiding your IP address
- Prevent hackers from breaking into your computer
- Allows you to visit sites that are forbidden to you
- Changes your IP address (and location)
- Delete information about ALL your internet activity

Anonymizer Universal

Source: http://www.anonymizer.com

Anonymizer Universal is an anonymous surfing tool that masks your true IP address, allowing you to surf sites discreetly and anonymously. Anonymizer Universal's personal VPN routes all of your Internet traffic through an encrypted tunnel to Anonymizer's secure and hardened servers. Anonymizer Universal then masks your real IP address to ensure complete and continuous anonymity online.

Guardster

Source: http://www.guardster.com

Guardster is an online proxy tool, which helps to surf the web anonymously by hiding your identity. The tool can mask your IP address, and it provides support for cookies and JavaScript. The tool routes all of your Internet traffic through an encrypted tunnel, forwards the request traffic to the intended web server, and returns the response to you.

Spotflux

Source: http://www.spotflux.com

Spotflux is an encrypted VPN client that hides identity while browsing the Internet. It encrypts your Internet traffic and blocks cookies. You can download, chat, or surf the Internet with your IP address masked.

Ultrasurf

Source: *https://ultrasurf.us*

Ultrasurf is anti-censorship, pro-privacy software that helps you to bypass Internet censorship and protect your online privacy. It hides your IP address, and clears browsing history and cookies, among other things.

Head Proxy

Source: *http://www.headproxy.com*

Head Proxy provides an anonymous dedicated server for web surfing. It provides a secure response to bypass restrictive web filters and firewalls that block websites.

Hope Proxy

Source: *http://www.hopeproxy.com*

Hope Proxy is an online anonymous proxy to hide your identity while surfing the Internet. It makes web browsing secure, encrypts browsing records, and remove malicious scripts.

Described below are some anonymizers for mobile devices:

Orbot

Source: *https://guardianproject.info*

Orbot is a proxy app that allows other apps to use the Internet more securely. It uses Tor to encrypt Internet traffic, and then hides it by bouncing through a series of computers around the world. Tor is free software and provides an open network to help you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and a kind of state security monitoring known as "traffic analysis." Orbot creates a truly private Internet connection.

Psiphon

Source: *https://s3.amazonaws.com*

Psiphon is a circumvention tool from Psiphon Inc. that utilizes VPN, SSH, and HTTP Proxy technology to provide you with open, uncensored access to Internet content. However, Psiphon does not increase online privacy, and is not an online security tool.

Features:

- **Browser** or **VPN** (whole-device) mode: one can choose whether to tunnel everything or just the web browser.
- **In-app stats**: let you know how much traffic you've been using.

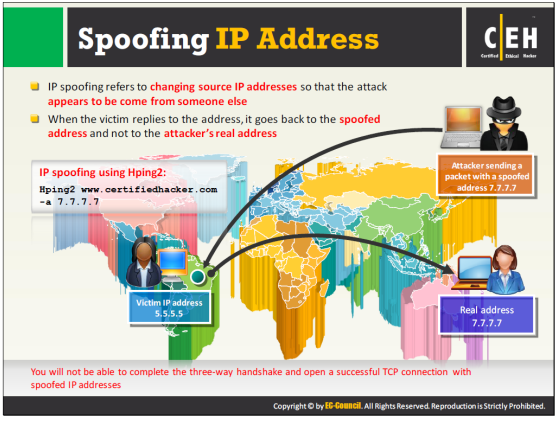
OpenDoor

Source: https://itunes.apple.com

OpenDoor is an app designed for both iPhone and iPad that allows you to browse websites smoothly and anonymously.

Features:

- **Safe and Smooth Browsing**: OpenDoor caches website contents on its fast and secure servers to speed up access and minimize interruptions
- **Total Anonymity**: protects users' identity on the web via randomized IP address
- **No "Content Striping"**: OpenDoor supports JavaScript, video, and multimedia streaming for a rich browsing experience
- **Multi-tab Browsing**: allows you to view multiple websites simultaneously
- **Easy to use interface** with complete browser functionalities



IP address spoofing is a hijacking technique in which an attacker obtains a computer's IP address, alters the packet headers, and sends request packets to a target machine, pretending to be a legitimate host. The packets appear to be sent from the legitimate machine but are actually sent from the attacker's machine, while her/his machine's IP address is concealed. Attackers mostly use IP address spoofing to perform DoS attacks.

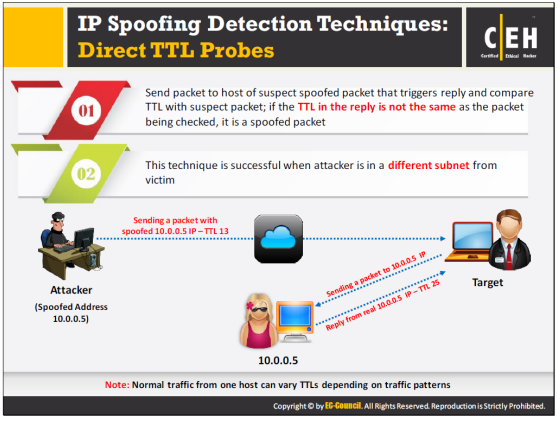
When the attacker sends a connection request to the target host, the target host replies and sends it to the spoofed IP address. When spoofing a nonexistent address, the target replies to a nonexistent system, and then hangs until the session times out, thus consuming target resources.

IP spoofing using Hping2:

```
Hping2 www.certifiedhacker.com -a 7.7.7.7
```

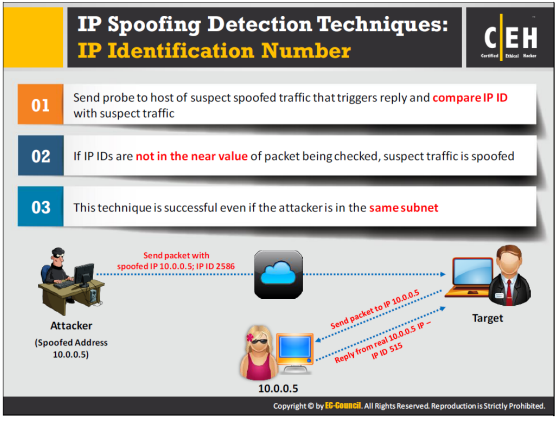
You can use Hping2 to perform IP spoofing. The above command helps you to send arbitrary TCP/IP packets to network hosts.

Note: You will not be able to complete the three-way handshake and open a successful TCP connection with spoofed IP addresses.



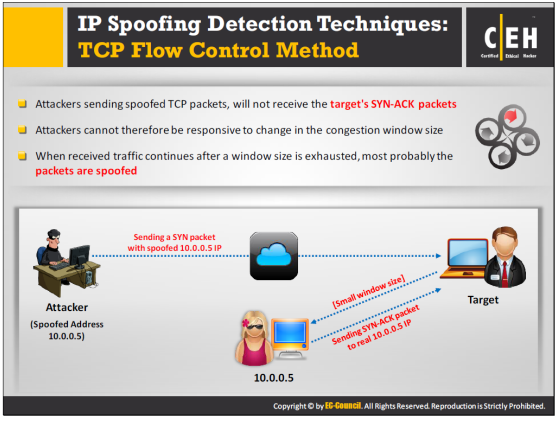
In this technique, you initially send a packet (ping request) to the legitimate host and wait for the reply. Check whether the TTL value in the reply matches that of the packet you are checking. Both will have the same TTL if they are using the same protocol. Although initial TTL values vary according to the protocol used, a few initial TTL values are commonly used: for TCP/UDP, the values are 64 and 128; for ICMP, 128 and 255.

If the reply is from a different protocol, then you should check the actual hop count to detect the spoofed packets. To determine the hop count, deduct the TTL value in the reply from the initial TTL value. If the reply TTL does not match the TTL of the packet you are checking, it is a spoofed packet. If the attacker knows the hop count between the source and host, it will be very easy to launch an attack. In this case, the test results in a false negative.



Users can identify spoofed packets by monitoring the IP identification (IPID) number in the IP packet headers. The IPID increases incrementally each time a system sends a packet. Every IP packet on the network has a "fragment identification" number, which is increased by one for every packet transmission. To identify whether a packet is spoofed, send a probe packet to the source IP address of the packet and observe the IPID number in the reply. The IPID value in the response packet must be close to but slightly greater than the IPID value of the probe packet. The source address of the IP packet is a spoofed if the IPID of the response packet is not close to that of the probe packet.

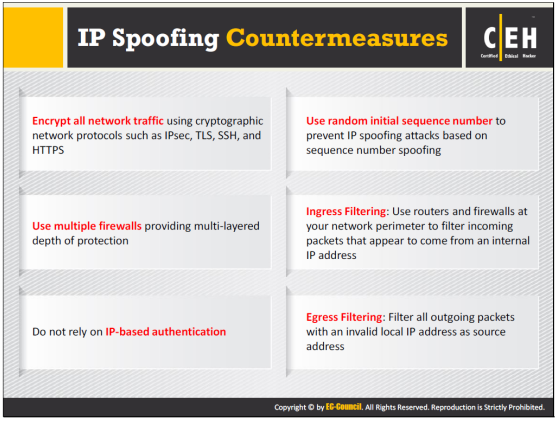
This method is effective even when both the attacker and the target are on same subnet.



The TCP can optimize the flow control on both the sender and the receiver side with its algorithm. The algorithm accomplishes the flow control using the sliding window principle. The user can control the flow of IP packets by the window size field in the TCP header. This field represents the maximum amount of data that the recipient can receive and the maximum amount of data the sender can transmit without acknowledgement. Thus, this field helps us to control data flow. When the window size is set to zero, the sender should stop sending data.

In general flow control, the sender should stop sending data once the initial window size is exhausted. The attacker who is unaware of the ACK packet containing window size information continues to send data to the victim. If the victim receives data packets beyond the window size, then they are spoofed packets. For effective flow control method and early detection of spoofing, the initial window size must be very small.

Most spoofing attacks occur during the handshake, as it is difficult to build multiple spoofing replies with the correct sequence number. Therefore, apply the flow control spoofed packet detection at the handshake. In a TCP handshake, the host sending the initial SYN packet waits for SYN-ACK before sending the ACK packet. To check whether you are getting the SYN request from a genuine client or a spoofed one, you should set the SYN-ACK to zero. If the sender sends an ACK with any data, then it means that the sender is the spoofed one. This is because when the sets SYN-ACK to zero, the sender must respond to it only with the ACK packet, without additional data.



In ethical hacking, the ethical hacker also known as the pen tester, has to perform an additional task that a normal hacker does not follow (i.e., applying countermeasures to the respective vulnerabilities determined through hacking). This is essential, because knowing security loopholes in your network is worthless unless you take measures to protect them against real hackers. As mentioned previously, IP spoofing is one of the techniques that a hacker employs to break into the target network. Therefore, to protect your network from external hackers, you should apply IP spoofing countermeasures to your network security settings. The following are a few IP spoofing countermeasures that you can apply:

- **Avoid trust relationships**

  Attackers may spoof themselves as a trusted host and send malicious packets to you. If you accept these packets, under the assumption that they're "clean" because they're from your trusted host, the malicious code will infect your system. Therefore, it is advisable to test all packets, even when they come from one of your trusted hosts. You can avoid this problem by implementing password authentication along with trust-relationship-based authentication.

- **Use firewalls and filtering mechanisms**

  As stated above, you should filter all the incoming and outgoing packets to avoid attacks and sensitive information loss. A firewall can keep malicious packets from entering your private network and prevent severe data loss. You can use access control lists (ACLs) to

block unauthorized access. At the same time, there is the possibility of an insider attack. Inside attackers could send sensitive information about your business to your competitors, which could lead to monetary loss and other issues. Another risk of outgoing packets is that an attacker will succeed in installing a malicious sniffing program running in hidden mode on your network. These programs gather and send all your network information to the attacker without any notification after filtering the outgoing packets. Therefore, you should assign the same importance to the scanning of outgoing packets as you would incoming packets.

- **Use random initial sequence numbers**

  Most of the devices chose their ISN based on timed counters. This makes the ISNs predictable, as it is easy for a malicious person to determine the concept of generating the ISN. An attacker can determine the ISN of the next TCP connection by analyzing the ISN of the current session or connection. If the attacker can predict the ISN, then he/she can make a malicious connection to the server and sniff your network traffic. To avoid this risk, you should use random initial sequence numbers.

- **Ingress filtering**

  Ingress filtering prohibits spoofed traffic from entering the Internet. It is applied on routers enhances the functionality of the routers and blocks spoofed traffic. Configuring and using access control lists (ACLs) that drop packets with the source address outside the defined range is one way to implement ingress filtering.

- **Egress filtering**

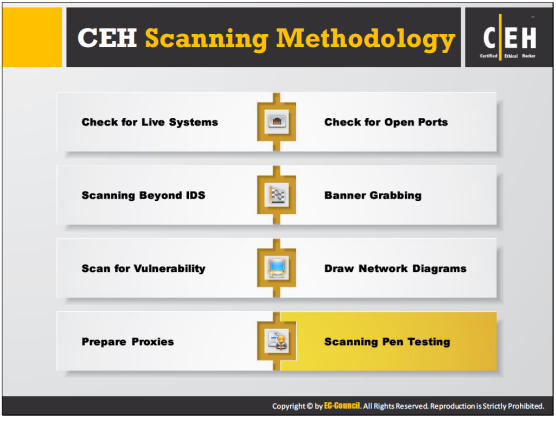
  Egress filtering refers to a practice that aims at IP spoofing prevention by blocking the outgoing packets with a source address that is not inside.

- **Use encryption**

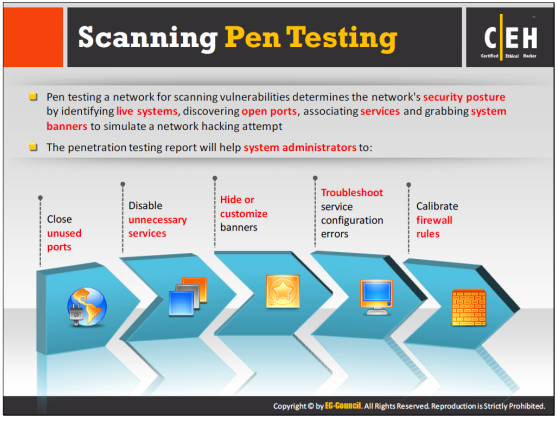
  If you want to attain maximum network security, then use strong encryption for all the traffic placed onto the transmission media, without considering its type and location. This is the best prevention against IP spoofing attacks. Attackers tend to focus on easy-to-compromise targets. If an attacker wants to break into encrypted network, he or she has to face decrypting a whole slew of encrypted packets, which is a difficult task. Therefore, the attacker is likely to move on to try and find another target that is easy to compromise or will simply abort the attempt. Use the latest encryption algorithms that provide strong security.

- **SYN flooding countermeasures**

  Countermeasures against SYN flooding attacks can also help you to avoid IP spoofing attacks.



It is advisable to pen-test the target network to identify its security posture. Pen-testing in anticipation of a possible problem helps to find and fix any security loopholes present in the target network. Such proactive prevention practices can keep an entire network from being compromised. This section describes the steps involved in pen-testing the target network and the various scanning tools used to accomplish this task.



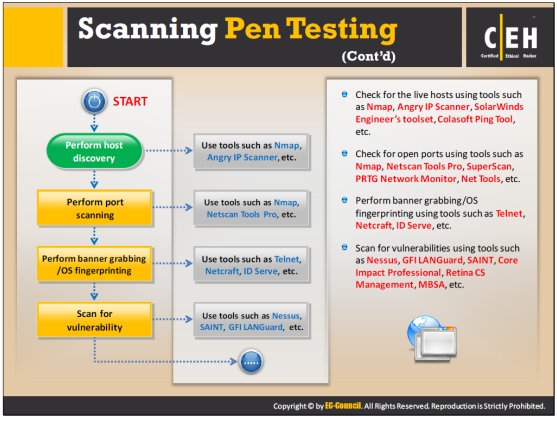
The network scanning penetration test helps to determine a network's security posture by identifying live systems, discovering open ports and associated services, and grabbing system banners from a remote location to simulate a network hacking attempt. You, as an ethical hacker or pen-tester, should scan and test the network in every manner possible to ensure that there is no security loophole in the system.

Once done with the penetration testing, document all your findings at every stage of testing. This will help system administrators to:

- Close unused ports if not necessary/unknown open ports found
- Disable unnecessary services
- Hide or customize banners
- Troubleshoot service configuration errors
- Calibrate firewall rules to impose more restriction

The more ports that are open on the server, the easier it will be for an attacker to connect to it. The first thing an attacker does is monitor network traffic for vulnerabilities such as open ports and services running, through which the network could be compromised. Admins may install, configure some unwanted services, leave services with default settings, and turn them on during OS and application installations. This can cause unwanted traffic to the server or a way for an attacker to intrude into the system. Attackers might also "banner grab" to trace the

server name and its version, and then use this information to break into a network. Therefore, close all the unused/unnecessary open ports, unwanted services, and so on, and configure the server in such a way that it hides the display of the banner. Also create inbound and outbound firewall rules to block all the unwanted ports from allowing any connections from outside the network.



Here is how you can conduct a pen-test of a target network.

Step 1: Host Discovery

The first step of network penetration testing is to detect live hosts on the target network. You can attempt to detect the live hosts (i.e., accessible hosts in the target network), using network scanning tools such as Nmap, Angry IP Scanner, SolarWinds Engineer's toolset, and Colasoft Ping Tool. It is difficult to detect live hosts behind a firewall.

Step 2: Port Scanning

Perform port scanning using tools such as Nmap, Netscan Tools Pro, SuperScan, PRTG Network Monitor, and Net Tools. These tools help to probe a server or host on the target network for open ports. Open ports are the doorways through which an attacker installs malware on a system. Therefore, you should check for open ports and close them if they are not necessary.

Step 3: Banner Grabbing or OS Fingerprinting

Perform banner grabbing/OS fingerprinting using tools such as Telnet, Netcraft, and ID Serve. This determines the operating system running on the target host of a network and its version. Once you know the version and operating system running on the target system, find and exploit the vulnerabilities related to that OS. Try to gain control over the system and compromise the whole network.

Step 4: Scan for Vulnerabilities

Scan the network for vulnerabilities using network vulnerability scanning tools such as Nessus, GFI LANGuard, SAINT, Core Impact Professional, Ratina CS Management, and MBSA. In this step, you will be able to determine the security weaknesses/loopholes of the target system or network.

Step 5: Draw Network Diagrams

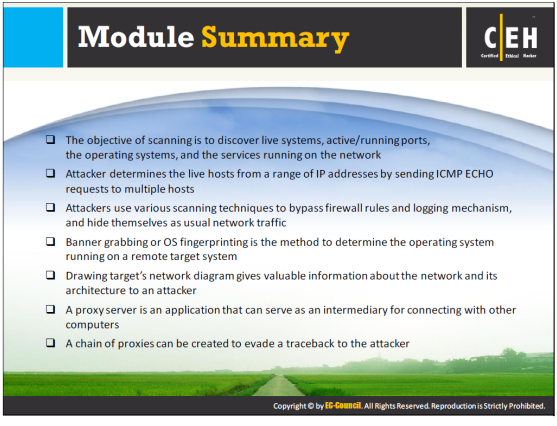
Draw a network diagram of the vulnerable hosts that helps you to understand the logical connection and path to them in the network. You can draw the network diagram with the help of tools such as Network Topology Mapper, OpManager, NetworkView, The Dude, and Friendly Pinger. The network diagrams provide valuable information about the network and its architecture.

Step 6: Prepare Proxies

Use proxy tools such as Proxy Workbench, Proxifier, Proxy Switcher, SocksChain, and TOR to hide yourself from detection.

Step 7: Document all Findings

The last but the most important step in penetration testing is to preserve all outcomes of tests conducted in previous steps in a document. This document will assist in finding potential vulnerabilities in the network, which you can use to suggest countermeasures. Thus, penetration testing helps in assessing the security posture of the network and fixing any security loopholes before they can cause trouble and result in severe organizational loss.



This module ends with an overview discussion of network scanning concepts. In the next module, we will see how attackers, ethical hackers, and pen-testers perform enumeration to collect information about a target before an attack or audit.