1 Systems Vulnerability Scanning

Syllabus

Systems Vulnerability Scanning Overview of vulnerability scanning, Open Port / Service Identification, Banner / Version Check, Traffic Probe, Vulnerability Probe, Vulnerability Examples, OpenVAS, Metasploit. Networks Vulnerability Scanning - Netcat, Socat, understanding Port and Services tools - Datapipe, Fpipe, WinRelay, Network Reconnaissance - Nmap, THC-Amap and System tools. Network Sniffers and Injection tools – Tcpdump and Windump, Wireshark, Ettercap, Hping Kismet.

Contents

1.1 Overview of Vulnerability Scanning

- **Vulnerability** is a weakness in the security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user identity before allowing data access. Bugs in the system that enable users to violate the site security policy are called **Vulnerability.**
- Vulnerability : A design flaw, defect or mis-configuration which can be exploited by an attacker.
- A vulnerability scanner scans a specified set of ports on a remote host and tries to test the service offered at each port for its known vulnerabilities.
- **Threat** is a set of circumstances that has the potential to cause loss or harm.
- Hardware is more visible than software, largely because it is composed of physical objects. Software is vulnerable to modification that either cause it to fail or cause it to perform an unintended task. Data is especially vulnerable to modification.
- A vulnerability scanner is software application that assesses security vulnerabilities in networks or host systems and produces a set of scan results. However, because both administrators and attackers can use the same tool for fixing or exploiting a system, administrators need to conduct a scan and fix problems before an attacker can do the same scan and exploit any vulnerability found.
- Vulnerability remediation is the process of fixing vulnerabilities. There are different types of vulnerability scanners that operate at different levels of invasiveness. Some simple scanners just check the windows registry and software version information to determine whether the latest patches and updates have been applied.
- Scanners use predefined tests to identify vulnerabilities. Scanner may produce false positive if written test is poor. There is no vulnerability attack but scanner reports it as vulnerable.
- Fig. 1.1.1 shows vulnerability scanner.

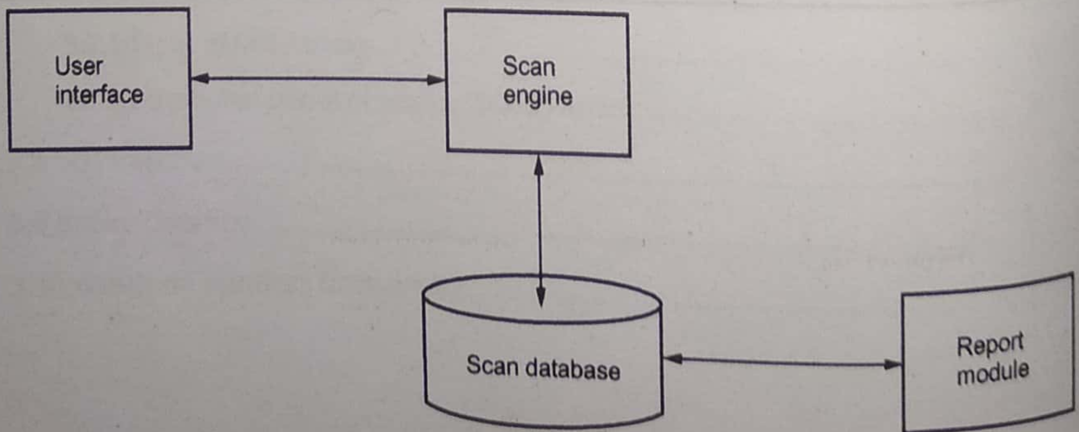


Fig. 1.1.1 Vulnerability scanner

- Vulnerability scanner is made up of four main modules : *Scan engine, scan batabase, report module and a user interface.*
- Once the assets have been identified, the vulnerability scan will begin by simply aiming the scanner at them.
- Step 1 : Information gathering → Identify hosts and restricted hosts (i.e., systems and devices not to be tested).
- Step 2 : Discovery and vulnerability scanning → Comprehensive port scanning, fingerprinting of services and applications; utilization of automated scanning tools and technologies to identify publicly known operating system and application vulnerabilities. (Network-based or authenticated scans);
- Step 3 : Reporting → Draft an executive summary detailing the overall state of the environment.

Working of vulnerability scanning

- Steps for scanning :

1. Checking if the remote host is alive
2. Detect firewall if any
3. TCP / UDP port scanning
4. Detection of operating system
5. TCP / UDP service discovery
6. Vulnerability assessment based on the services detected.

- Vulnerability scanners can be divided broadly into two groups : *Network-based scanners and host-based scanners.*
- A **network-based scanner** is usually installed on a single machine that scans a number of other hosts on the network. It helps detect critical vulnerabilities such as mis-configured firewalls, vulnerable web servers, risks associated with vendor-supplied software and risks associated with network and systems administration.
- Network scanners are often configured either to scan "internal" networks or "external" networks.
- A **host-based scanner** is installed in the host to be scanned and has direct access to low-level data, such as specific services and configuration details of the host's operating system. A database scanner is an example of a host-based vulnerability scanner.

Vulnerability scanning vs. penetration testing

- Vulnerability scanning is very often confused with penetration testing but there are some major differences between the two.

1. A vulnerability scan is automated high-level test that looks for potential security vulnerabilities, while a penetration test is an exhaustive examination that includes a live person actually digging into your network's complexities to exploit the weakness in your systems.
2. A vulnerability scan only identifies vulnerabilities, while a penetration tester digs deeper to identify the root cause of the vulnerability that allows access to secure systems or stored sensitive data. The pen tester also looks for business logic vulnerabilities that might be missed by an automatic scanner.
3. Vulnerability scans can be instigated manually or on an automated basis and will complete in as little as several minutes to as long as several hours.

Limitations of vulnerability scanners

1. Generate overwhelming amount of data.
2. No indication of how vulnerabilities can be combined.
3. Vulnerability scanners can only report vulnerabilities according to the plug-ins installed in the scan database.

- The key difference between vulnerability assessment and penetration testing is the lack of exploitation in vulnerability assessment and the actual exploitation in penetration testing.

1.1.1 Open Port / Service Identification

- Some of the services are naturally secure. Services do not always run on default ports.
- The main goal of port scanning is to find out which ports are open, which are closed, and which are filtered. When we say a port is filtered, what we mean is that the packets passing through that port are subject to the filtering rules of a firewall.
- In TCP/IP and UDP networks, a port is an endpoint to a logical connection and the way a client program specifies a specific server program on a computer in a network. Some ports have numbers that are pre-assigned to them by the IANA, and these are called the "well-known ports".
- A port number is a 16-bit unsigned integer that ranges from 0 to 65535.
- A specific network port is identified by its number commonly referred to as port number, the IP address in which the port is associated with and the type of transport protocol used for the communication.

Standard port numbers are listed below :

1. Ports number 0 to port number 1023 are known as **well known ports**

2. Port number 1024 to port number 49151 are named as **registered ports**

3. Port number 49152 to port number 65535 **are dynamic and/or private ports**

Port number	Protocol name
21	FTP
22	SSH server listing port
23	Telnet port
25	SMTP mail port
53	DNS port
67	DHCP
80	HTTP
110	POP3 port
123	NTP
135	RPC
143	IMAP4 port
161	SNMP port
179	BGP port
443	SSL port

- Port scanning may involve all of the 65,535 ports or only the ports that are well-known to provide services vulnerable to different security-related exploits.
- **Open port :** A service process is listening at the port. The operating system receives packets arriving at this port and gives the messages to the service process. If the operating system receives a SYN at an open port, this is the first packet of the three way handshake.
- **Closed port :** No process is listening at the port. If the OS receives a SYN at a closed port, an RST is sent.
- **Filtered port :** A packet filter is listening at the port.
- Port scanner tool can be used to identify available services running on a server, it uses raw IP packets to find out what ports are open on a server or what operating system is running or to check if a server has firewall enabled etc.
- Port scanner is an essential security tool for finding open ports corresponding to the TCP or UDP services running on a target device. This scanner allows you to

run four different types of scanning patterns while looking for TCP or UDP open ports.

- **Port scanning technique** consists of sending a message to a port and listening for an answer. The received response indicates the port status and can be helpful in determining a host's operating system and other information relevant to launching a future attack.
- The vertical scan is a port scan that targets several destination ports on a single host. A horizontal scan is a port scan that targets the same port on several hosts.
- Various port scanning techniques are available. Following are the standard methods used by Nmap and Nessus tool.

1. **Address resolution protocol :** ARP finds an active device on the local network segment by sending series of ARP broadcasts packets.
2. **Vanilla TCP connect scan :** It is the most basic scanning method. The connect ( ) system call is used to open a connection to port on the machine. If the port is listening, connect ( ) will succeed, otherwise the port isn't reachable. The attacker first sends a SYN probe packet to the port he wishes to test. Upon receiving a packet from the port with the SYN and ACK flags set, he knows that the port is open. The attacker completes the three-way handshake by sending an ACK packet back. Fig. 1.1.2 shows vanilla TCP scan result when a port is open.

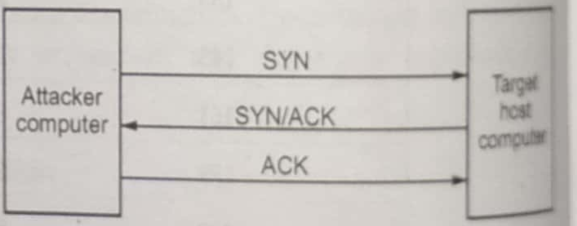


Fig. 1.1.2 Vanilla TCP scan result when a port is open

   - If the target port is closed, the attacker receives an RST/ACK packet directly back. Fig. 1.1.3 vanilla TCP scans result when a port is closed.

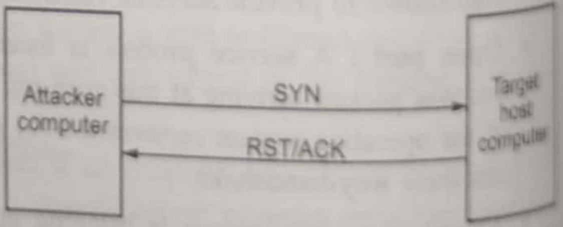


Fig. 1.1.3 Vanilla TCP scan result when a port is closed

   - The attacker sends a SYN probe packet, but the target server responds with an RST/ACK.

3. **TCP SYN scanning :** This technique is often referred to as "half-open" scanning, because the attacking system doesn't close the open connections. The attacker will send a SYN packet to the target and wait for a response

A SYN/ACK indicates the port is listening. If the port is closed, the target will send an RST. This type of scan is difficult to detect.

4. **TCP FIN scanning :** It has the ability to pass undetected through most firewalls, packet filters, and scan detection programs. The attacking system sends FIN packets to the targeted system. The closed ports will respond with an RST. The open ports will ignore the packets. The attacking system will take note of which ports it received an RST on and report on the ports that did not respond with an RST.
5. **FTP bounce attack :** The FTP Bounce Attack uses the FTP protocol support for proxy FTP connections. The attacker can hide behind an FTP server and scan another target without being detected. If the FTP server allows reading from and writing to a directory, then attacker can send arbitrary data to ports that attacker find open. The downside is that most FTP servers have this service disabled.
6. **The TCP ACK scan :** This method is used to identify active web sites that may not respond to standard ICMP pings. The scan utilizes TCP packets with the ACK flag set to a probable port number. If the port is open, the target will send an RST in reply. If the port is closed, the target will ignore the packet.
7. **TCP NULL scan :** An attacker uses a TCP NULL scan to determine if ports are closed on the target machine. If the target's TCP port is closed, the port will send an RST. If the port is open, the port will ignore the packet. NULL scanning requires the use of raw sockets, and thus cannot be performed from some windows systems. On UNIX and linux, raw socket manipulations require root privileges.
8. The **UDP ICMP port scan** uses the UDP protocol. This port scan is successful in finding high number ports, especially in solaris systems. The scan is slow and unreliable.

1.1.2 Banner / Version Check

- SMTP banners usually contain version information. Some of the services announce information about themselves. Secure shell service is one example of this type. When you try to connect to SSH service, it will display following line :

```
$ nc -v localhost _name 22
```

- System admin normally remove or change banner to make them less verbose. It cannot remove vulnerability but impact is less.

1.1.3 Traffic Probe

- Probe is an action taken or an object used for the purpose of learning something about the state of the network. Relative to computer security in a network, a probe is an attempt to gain access to a computer and its files through a known or probable weak point in the computer system.
- A network traffic pattern is information about the source, destination, protocol, port and bandwidth of network packets. Network scanning is systematic attempts to communicate with a class of network addresses via a particular port or protocol to see which computers respond. It is a first step to identify and exploit vulnerabilities.
- Web service will not respond until it receives data from the client machine. Consider the example of valid HTTP request with HEAD method. To get the home page of technical publication pune :

```
[IAD@localhost ~] $echo -e -n "GET /
HTTP/1.1\r\nHost:www.vtubooks.com\r\n\r\n"|nc www.vtubooks.com 80
    [IAD@localhost ~] $ nc  localhost 80
HEAD / HTTP/1.0
HTTP/1.1 200 OK
MIME-Version: 1.0
Server: Edited out
Content-length: 0
Cache-Control: public
Expires: Sat, 03 Jan 2021 19:00:00 GMT

[IAD@localhost ~] $
```

- The nc (netcat) utility can open TCP connections, send UDP packets, listen on arbitrary TCP and UDP ports, do port scanning, and deal with both IPv4 and IPv6. Net-cat is a utility that is able to write and read data across TCP and UDP network connections. If you are responsible for network or system security it essential that you understand the capabilities of net-cat. net-cat can be used as port scanner, a backdoor, a port re-director, a port listener.
- Traffic probe uses valid request. Valid protocol messages are rarely crashed. But traffic probe is not perfect tool.
- **Vulnerability probe :** Payloads identify the some security bugs which are not identified by vulnerability scanner.

1.2 OpenVAS

- OpenSource Vulnerability Assessment Scanner (OpenVAS) is a security scanner to allow future free development of the now-proprietary NESSUS tool. OpenVAS now offers 15'000 Network Vulnerability Tests (NVTs) more all NASL plugins.
- OpenVAS is a GUI-based application and is relatively easy to use.
- Nessus is one of the most popular vulnerability scanning tools. It is a commercial product and many companies often desire an individual that is skilled with it. OpenVAS, which is the older open-source version of Nessus, is still available. It comes pre-packaged with linux distributions such as Kali Linux.
- The OpenVAS scanner is a comprehensive vulnerability assessment system that can detect security issues in all manner of servers and network devices. It collect and manage security information for network, hardware device etc.
- OpenVas is an open source vulnerability scanner that can test a system for security holes using a database of over 28'0000 test plugins. OpenVAS is not an attack tool and it do not fix vulnerable systems.
- You can download from site : **www.openvas.org**
- OpenVAS depends upon client server architecture. It collects data from client and server separately for data management purpose.
- OpenVAS uses Nessus Attack Scripting Language (NASL). NASL is a scripting language designed for the nessus security scanner. The scanner very efficiently executes the actual Network Vulnerability Tests (NVTs) which are served with daily updates via the OpenVAS NVT Feed or via a commercial feed service.
- OpenVAS uses different types of probing techniques and recognize the services running on any port.
- The company Greenbone Networks develops and uses OpenVAS as a base for its appliance product family for vulnerability scanning and management. The new version can be downloaded free and is available as Free Software under the GNU GPL license.
- OpenVAS follows a client-server model. A server component is responsible for scheduling and running scans, and a client component is used to configure scans and access the results. The server is normally installed on a linux or unix server, and the client is typically run from the administrator's own workstation.
- OpenVMS security scanner protects the communication between the client and the server by using SSL. SSL requires the server to present a certificate to the client, and the client can optionally present a certificate to the server.

- The Internet Assigned Numbers Authority officially assigned OpenVAS TCP port 9390. OpenVAS is a security conscious project, and the connection to this port from an OpenVAS client is always tunneled over SSL with strong ciphers to ensure that only the intended user can access the data generated by OpenVAS.
- OpenVAS is available in binary package form for most major linux distributions.
- The OpenVAS project maintains a public feed of Network Vulnerability Tests (NVTs). It contains more than 35,000 NVTs , growing on a daily basis. This feed is configured as the default for OpenVAS.

1.3 Metasploit

Imp

- Metasploit is an open-source framework used for security development and testing. Metasploit is a framework that allows testing attacks. Fig. 1.3.1 shows architecture of metasploit.

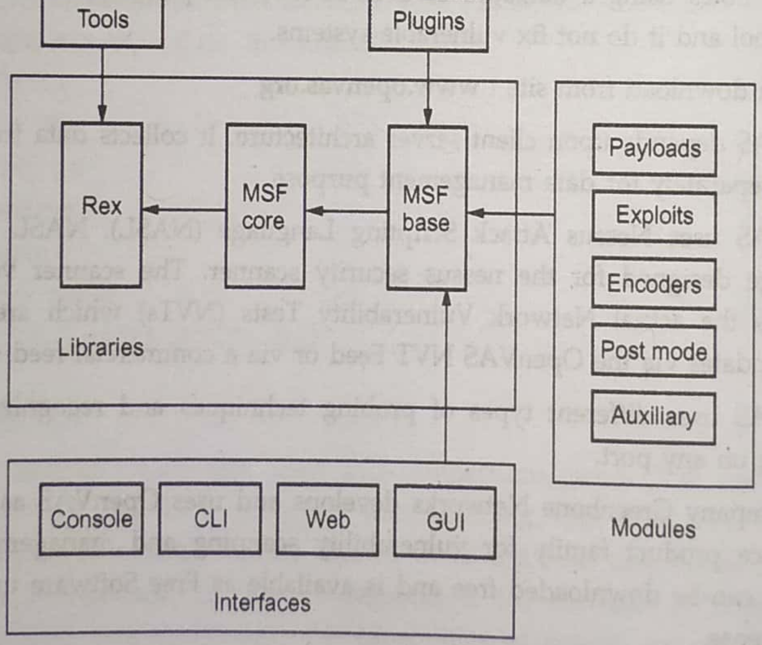


Fig. 1.3.1 Architecture of metasploit

- Modules built on top of libraries, accessed via interfaces to conduct exploitation tasks. Plugins hook directly into the framework to add commands to the interface, etc.
- Source code of metasploit is in ruby. It uses PostgreSQL database. Metasploit manage database for scan, sessions and post hack information. Database is installed separately.

Installing the framework

- To install the framework on UNIX **operating system** simply downloads the latest release to a working directory. Extract the tarball and change into the created directory. Since it is written in PERL you should be able to simply execute the UI of your choice. It is recommended to also install the supporting PERL modules from $MSFDIR/extras. These allow command completion and SSL support.
- To install to a system wide location copy the entire tree to a directory (/usr/local/msf) and create symlinks from the msf* applications to a system wide binary path like /usr/local/bin. User created modules can be place in their home directory but need to reside under the ~/.msf directory.

On windows operating system

- A downloadable installer utilizing cygwin is provided on the metasploit site. This installer is a stipped down version of cygwin and includes everything you need to act like its UNIX counterpart.
- Commands used :
  1. Connect : Like netcat, connects to host on specified port
  2. Search : Search module database, by name, platform, app, cve and more
  3. Sessions : List or manipulate your open sessions (shells, VNC, etc)
  4. Show : Show anything : Show modules, exploits, payloads, options (for selected module)
- On UNIX OS machine, start the database process manually with the pg_ctl command. Metasploit interface is start with following command :

```
$ ./ msfconsole
```

- The above command is used for text based interface.

1.4 Networks Vulnerability Scanning

- Socket interface is a protocol independent interface to multiple transport layer primitives. In order to write applications which need to communicate with other applications.
- Socket is an abstraction that is provided to an application programmer to send or receive data to another process. Data can be sent to or received from another process running on the same machine or a different machine. It is like an endpoint of a connection. It exists on either side of connection and identified by IP address and port number.
- Sockets works with UNIX I/O services just like files, pipes and FIFO. API stands for Application Programming Interface. It is an interface to use the network.

Socket API defines interface between application and transport layer. The API defines function calls to create, close, read and write to/from a socket.

- Socket is the basic abstraction for network communication in the socket API. Socket defines an endpoint of communication for a process.
- Operating system maintains information about the socket and its connection Fig. 1.4.1 shows the socket and process.
- Most socket functions require a pointer to a socket address structure as an argument. Each supported protocol suite defines its own socket address structure.

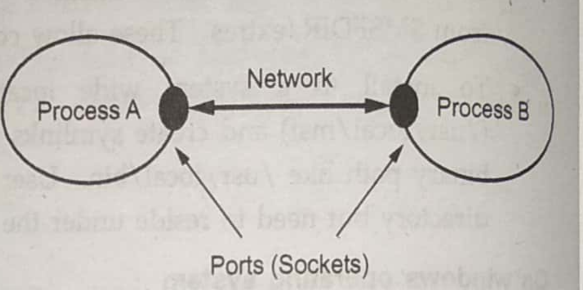


Fig. 1.4.1 Socket and process

- Socket functions like connect( ), accept( ), and bind( ) require the use of specifically defined address structures to hold IP address information, port number, and protocol type. This contains the protocol specific addressing information that is passed from the user process to the kernel and vice versa.
- Each of the protocols supported by a socket implementation have their own socket address structure sockaddr_suffix where suffix represents the protocol family.
- Socket-based communication is programming language independent. To the kernel, a socket is an endpoint of communication. To an application, a socket is a file descriptor that lets the application read/write from/to the network.
- A server (program) runs on a specific computer and has a socket that is bound to a specific port. The server waits and listens to the socket for a client to make a connection request.
- There are five significant steps that a program which uses TCP must take to establish and complete a connection. The server side would follow these
- **Steps :**
  1. Create a socket.
  2. Listen for incoming connections from clients.
  3. Accept the client connection.
  4. Send and receive information.
  5. Close the socket when finished, terminating the conversation.
- In the case of the client, these steps are followed :
  1. Create a socket.
  2. Specify the address and service port of the server program.

3. Establish the connection with the server.
4. Send and receive information.
5. Close the socket when finished, terminating the conversation.

Socket system calls for connectionlesss protocol

- There are some instances when it makes to use UDP instead of TCP. Some popular applications built around UDP are DNS, NFS and SNMP. Initially client does not establish a connection with the server. Instead, the client just sends a datagram to the server using the sendto function which requires the address of the destination as a parameter.
- Similarly, the server does not accept a connection from a client. Instead, the server just calls the recvfrom function, which waits until data arrives from some client.
- The recvfrom returns the protocol address of the client, along with the datagram, so the server can send a response to the client.

Steps on the client side are as follows :

1. Create a socket using the socket( ) function;
2. Send and receive data by means of the recvfrom( ) and sendto( ) functions.

Steps on the server side are as follows :

1. Create a socket with the socket() function;
2. Bind the socket to an address using the bind( ) function;
3. Send and receive data by means of recvfrom( ) and sendto ( ).

1.4.1 Netcat

- Netcat is a utility that is able to writeand read data across TCP and UDP network connections. Netcat can be used as port scanner, a backdoor, a port redirector, a port listener etc.
- It is a simple unix utility which reads and writes data across network connections, using TCP or UDP protocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts.
- Netcat will try connecting to every port between 20 and 30 at the target. One of Netcat's neat features is command redirection. This means that Netcat can take an exe file and redirect the input, output and error messages to a TCP/UDP port, rather than to the default console.
- You can read more about Netcat here **http://www.atstake.com/research/tools/nc110.txt**

- You can download for UNIX OS from **http://www.atstake.com/research/tools/nc110.tgz**
- You can download for Win 95/98/NT/2000 from **http://www.atstake.com/research/tools/nc11nt.zip**
- In the simplest form, " nc host port" creates a TCP connection to the specified port on the given target host. Your standard input is then sent to the host, and anything that comes back across the connection is sent to your standard output. This continues indefinitely, until the network side of the connection shuts down.
- Netcat can operate in 2 modes :
  1. **Client mode :** The client always initiates the connection with the listener. All the errors in client mode are put into the standard error. In client mode, it requires the IP address and port of the listener.
  2. **Listener mode :** In this mode, the listener always listens for the connection on a specific port. Its output can be a standard output, file etc. It asks for just listening port.

Netcat command syntax :

```
$ nc [options] [target_system] [remote port]
```

Options :

Sr. No.	Options	Description
1.	-l	This option tells the Netcat to be in listen mode.
2.	-u	Makes a UDP connection instead of TCP connection.
3.	-p	For the listener, this is the listened port. For the client, this is source port.
4.	-e	This tells what operation to perform after a successful connection.
5.	-L	This makes a persistent listener. Work for windows only.
6.	-wN	This option defines the timeout value.
7.	-v	This is the verbose mode.
8.	-d	Allows to run in detached mode without console window.
9.	-o	Dumps communication over this channel to the specified file.
10.	-L	Tells Netcat to not close and wait for connections.

- Use -L switch to reconnect to the same Netcat sessions. This way you can connect over and over to the same Netcatprocess. Forces netcat to listen for an inbound connection.

- For example "nc-l -p 1111 <filename", this command line tells netcat to listen on port 1111 and once a connection is made to send the file named filename.

Data transfer

- Netcat can be used to transfer files between machines. Netcat works with both TCP and UDP. Data transfer can be done in two ways :
  1. Pulling a file from listener from client. In this type of transfer, the file is actually pulled from a listener.
  2. Pushing a file to listener from client: This includes pushing a file to the listener from the client.

1.4.2 Socat

- Socat is a command line based utility that establishes two bidirectional byte streams and transfers data between them. This command opens a proxy listening on localhost : 8080 and forwards all requests through Tor to the target 10.10.10.100 : 80
- Four phases of socat :
  1. The init phase : The command line options are parsed and logging is initialized.
  2. Open phase : Socat opens the first address and afterwards the second address
  3. Transfer phase : Socat watches both streamscq read and write file descriptors via CWselect() , and, when data is available on one side and can be written to the other side, Socat reads it, performs newline character conversions if required, and writes the data to the write file descriptor of the other stream, then continues waiting for more data in both directions.
  4. Close phase : Socat transfers the EOF condition to the other stream, i.e. tries to shutdown only its write stream, giving it a chance to terminate gracefully.

1.5 Understanding Port and Services Tools

1.5.1 Datapipe

- Datapipe is a unix-based port redirection tool written by Todd Vierling. It uses standard system and network libraries, which enable it to run on the alphabet of UNIX platforms. A port redirection tool passes TCP/IP traffic received by the tool on one port to another port to which the tool points.
- A port redirection tool is neither a client nor a server. It is based on the UNIX OS. A port redirection tool passes TCP/IP traffic received by the tool on one port to another port to which the tool points.

1.5.2 FPipe

- FPipe implement port redirection techniques natively in windows. It adds UDP protocol and outbound source port number support, which datapipe lacks.
- You can download from **http://www.foundstone.com/ or http://www.mcafee.com/in/downloads/free-tools/fpipe.aspx**
- FPipe is a TCP source port forwarder/redirector. It can create a TCP /UDP stream with a source port of your choice. This is useful for getting past firewalls that allow traffic with source ports of say 23, to connect with internal servers.
- FPipe runs on windows operating system. There is no need of privilege user account and support from dynamic link library. FPipe can run on the local host of the application that you are trying to use to get inside the firewall.
- When you start FPipe, it wait for a client to connect on its listening port. It makes a listening connection is made a new connection to the destination machine and port with the specified local source port will be made. When the full connection has been established, FPipe forwards all the data received on its inbound connection to the remote destination port beyond the firewall.
- **FPipe options :**

Sr. No.	Option	Description
1.	-? Or -h	Display help text
2.	-c	Maximum allowed simultaneous TCP connections. Default 32 connections are allowed.
3.	-i	listening interface IP address
4.	-l	listening port number
5.	-r	remote port number
6.	-s	Source port used for outbound traffic
7.	-u	It support UDP mode
8.	-v	For Verbose mode

- You cannot run FPipe as background process.

1.5.3 WinRelay

- WinRelay is windows based port redirection tool. It uses static source port for redirected traffic.
- Some antivirus software consider as malicious software.

- You can download from site **www.ntsecurity.nu/toolbox/winrelay/**
- Online games use datapipe and fpipe tools. Port redirection tools are useful for assigning the alternative port to a service.

1.6 Network Reconnaissance

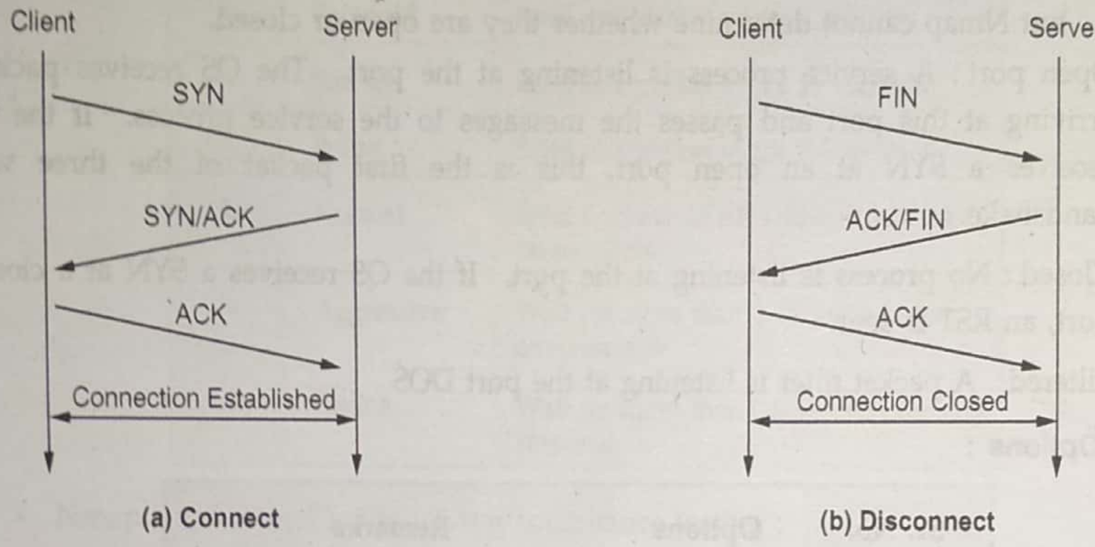
- Reconnaissance attack is a kind of information gathering on network system and services. This enables the attacker to discover vulnerabilities or weaknesses on the network.
- One of the old reconnaissance methods was simply to sequentially ping every IP address on a network, starting with the local subnet and then expand outward. If an IP address responded to a ping then the attacker knew there was a active device at that IP address and would add it to a locally list of potential attack targets. This ping method would require the attacker to guess what subnets existed on the network.
- Reconnaissance attack can be active or passive. Tools that could be used for active reconnaissance are
  1. Application Mapper (AMAP) : AMAP uses the results from Nmap to mine for more information.
  2. Nessus : It is vulnerability scanner
  3. Scanrand : It is fast network scanner
  4. Paratrace : TCP Traceroute that utilizes selected TTL messages
- Intruders are increasingly making use of compromised hosts to launch reconnaissance against target networks

1.6.1 Nmap

- Nmap was developed by Fyodor Yarochkin. This tool is available for Windows and Linux as a GUI and command-line program. It is most widely-used port scanner tool. It can performs many types of scans and OS identification, and also allows user to control the speed of the scan.
- Network mapped (Nmap) is a network scanning and host detection tool that is very useful during several steps of penetration testing. It is an open-source port or security scanner. Primary function of Nmap is discovery and mapping of hosts on a network.
- Nmap available at **www.insecure.org/Nmap**
- Unix version available at **http://www.insecure.org/Nmap**

- Windows NT version available at **http://www.eeye.com/html/Databases/Software/Nmapnt.html**
- Almost every Linux install its packaged, Windows you will need to download Nmap and the Win-Pcap files.
- Nmap can perform ping sweeps. Port scanning tools depends upon communication between two machines and TCP, UDP services. State of the connection is represented by flags in TCP connection. TCP uses six flags. For connecting to a TCP port, client sends a packet with the SYN flag. When SYN flag is set, it indicates clients wish to communicate with the port services.
- Nmap tool is capable to detect types of victims' operation systems just using TCP fingerprinting. TCP fingerprinting uses advanced fingerprinting analyses of the TCP stack implementation. A TCP packet is crafted by switching on or off certain flags and sent to the remote machine. The remote operating system, based on its TCP stack implementation sends a response, with some specific flags turned on or off. Depending on TCP responses collected for each crafted packet we can make an intelligent guess of the operating system from its database of TCP stack signatures.
- Standard TCP communications are controlled by flags in the TCP packet header. Following are the list of TCP connection flags :
  a. Urgent (URG) : The Urgent pointer is valid if it set to 1.
  b. Acknowledgement (ACK) : ACK bit is set to 1 to indicate that the acknowledgment number is valid.
  c. Push (PSH) : The receiver should pass this data to the application as soon as possible.
  d. Reset (RST) : This flag is used to reset the connection. It is also used to reject an invalid segment.
  e. Synchronize (SYN) : Synchronize sequence number to initiate a connection. The connection request has SYN = 1 and ACK = 0 to indicate that the piggyback acknowledgement field is not in use.
  f. Finish (FIN) : The FIN bit is used to release a connection. It specifies that the sender is finished sending data.
- The port number along with the source and destination IP addresses in the IP header, uniquely identify each connection. The combination of an IP address and a port number is sometimes called a socket. When a new connection is being established, the SYN flag is turned on. The sequence number of the first byte of data sent by this host will be the ISN plus one because; the SYN flag consumes a sequence number.

- The three-way handshake involves the exchange of three messages between the client and the server. Three messages are client SYN, service SYN-ACK and client ACK etc. Fig 1.6.1 shows three-way handshake for TCP.



(a) Connect (b) Disconnect

Fig. 1.6.1 Three way handshake TCP connection

- The client initiates a connection to the server via a packet with only the **SYN** flag set. The server replies with a packet with both the **SYN** and the **ACK** flag set. For the final step, the client responds back the server with a single **ACK** packet. If these three steps are completed without complication, then a TCP connection has been established between the client and server.
- Client sends a single **SYN** packet to the server on the appropriate port. If the port is open then the server responds with a **SYN/ACK** packet. If the server responds with an **RST** packet, then the remote port is in state closed. The client sends **RST** packet to close the initiation before a connection can ever be established. This scan also known as "half-open" scan.

Command Line Syntax

```
$ nmap [ <Scan Type> ...] [ <Options> ] { <target specification> }
```

- Target specification can be hostnames, IP address etc.
- The output of Nmap is a list of scanned targets, with additional information on each depending on the options used. Port table is the main information of Nmap. Table list the port number and protocol, service name and state. The state is either open, filtered, closed, or unfiltered.
  1. Open state means that an application on the target machine is listening for connections/packets on that port.
  2. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed.

3. Closed means ports have no application listening on them, though they could open up at any time.
4. Ports are classified as unfiltered. When they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed.

- Open port : A service process is listening at the port. The OS receives packets arriving at this port and passes the messages to the service process. If the OS receives a SYN at an open port, this is the first packet of the three way handshake.
- Closed : No process is listening at the port. If the OS receives a SYN at a closed port, an RST is sent.
- Filtered : A packet filter is listening at the port DOS

Nmap Options :

Sr. No.	Options	Remarks
1	-sS	TCP SYN scan
2	-sF -sX -sN	Stealth FIN, Xmas tree, or Null scan modes
3	-sP	Ping scanning
4	-sW	Window scan
5	-sA	ACK scan
6	-sL	List scan
7	-P0	Do not try to ping hosts at all before scanning them
8	-sT	TCP connect
9	-U	UDP scanning : Sends a UDP packet to target ports to determine if a UDP service is listening
10	-b	Bounces a TCP scan off of an FTP server, hiding originator of the scan.
11	-sR	RPC scanning : Scans RPC services using all discovered open TCP/UDP ports on the target to send RPC NULL commands.

Nmap timing options :

Sr. No.	Option	Remarks
1.	Paranoid	Send one packet every 5 minutes
2.	Sneaky	Send one packet every 15 seconds
3.	Polite	Send one packet every 0.4 seconds
4.	Normal	Send packets ASAP without missing target ports
5.	Aggressive	Wait no more than 1.25 seconds for any response
6.	Insane	Wait no more than 0.3 seconds for any response

- Nmap can be used for following compliance testing :
  1. Testing for open ports on the interfaces of a firewall.
  2. Performing scans across workstation IP address ranges to determine if any unauthorized networking applications are installed.
  3. Determining if the correct version of web service is installed in De-Militarized zone
  4. Locating systems with open file sharing ports.
  5. Locating unauthorized FTP servers, printers or operating systems.

Nmap with help :

```
C:\nmap>nmap -h
Nmap 3.93 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
-sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
-sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
-sV Version scan probes open ports determining service and app names/versions
-sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
-p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
-F Only scans ports listed in nmap-services
-v Verbose. Its use is recommended. Use twice for greater effect.
```

```
-P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
-6 scans via IPv6 rather than IPv4
-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
-n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
-oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
-iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
--interactive Go into interactive mode (then press h for help)
--win_help Windows-specific features
```

- Nmap is considered a required tool for all ethical hackers.

1.6.2 THC-Amap

- Amap is a tool for determining what application is listening on a given port. THC means The Hackers Choice.
- Most of port scanners assume that if a particular port is open, then default application for that port must be present. Amap probes these ports to find out what is really running on that port.
- You can download from **http://thc.segfault.net/thc-amap/**
- THC-Amap runs in following modes :

Sr. No.	Modes	Remarks
1	-A	It identifies the service associated with the port.
2	-B	This mode does not perform identification.
3	-P	It conducts a port scan.

1.7 System Tools

1. Whois

- Whois is a query/response protocol tool. It is widely used for querying an official database in order to determine the owner of a domain name, an IP address, or an autonomous system number on the Internet.
- Whois normally runs on TCP port 43. Whois is the primary tool used to query Domain Name Services.

- Linux system provides built in facility of whois. Windows does not have a built-in Whois client. Windows users will have to use a third-party tool or website to obtain Whois information.

```
$ whois vtubooks.com
Whois Server Version 2.0
Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.
Domain Name: VTUBOOKS.COM
Registrar: DOMAIN.COM, LLC
Sponsoring Registrar IANA ID: 886
Whois Server: whois.domain.com
Referral URL: http://www.domain.com
Name Server: NS5.INDIALINKS.COM
Name Server: NS6.INDIALINKS.COM
Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Updated Date: 23-oct-2013
Creation Date: 18-nov-2000
Expiration Date: 18-nov-2015
>>> Last update of whois database: Sun, 26 Jul 2015 17:11:41 GMT <<<
$ whois google.com
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2015-06-12T10:38:52-0700
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2020-09-13T21:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited
(https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Registry Registrant ID:
```

```
Registrant Name: Dns Admin
Registrant Organization: Google Inc.
Registrant Street: Please contact contact-admin@google.com, 1600 Amphitheatre Parkway
Registrant City: Mountain View
Registrant State/Province: CA
Registrant Postal Code: 94043
Registrant Country: US
Registrant Phone: +1.6502530000
Registrant Phone Ext:
Registrant Fax: +1.6506188571
Registrant Fax Ext:
Registrant Email: dns-admin@google.com
Registry Admin ID:
Admin Name: DNS Admin
Admin Organization: Google Inc.
Admin Street: 1600 Amphitheatre Parkway
Admin City: Mountain View
Admin State/Province: CA
Admin Postal Code: 94043
Admin Country: US
Admin Phone: +1.6506234000
Admin Phone Ext:
Admin Fax: +1.6506188571
Admin Fax Ext:
Admin Email: dns-admin@google.com
Registry Tech ID:
Tech Name: DNS Admin
Tech Organization: Google Inc.
Tech Street: 2400 E. Bayshore Pkwy
Tech City: Mountain View
Tech State/Province: CA
Tech Postal Code: 94043
Tech Country: US
Tech Phone: +1.6503300100
Tech Phone Ext:
Tech Fax: +1.6506181499
Tech Fax Ext:
Tech Email: dns-admin@google.com
Name Server: ns1.google.com
```

Name Server: ns3.google.com

Name Server: ns2.google.com

Name Server: ns4.google.com

DNSSEC: unsigned

URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

>>> Last update of WHOIS database: 2015-07-26T09:56:49-0700

1.8 Network Sniffers and Injection Tools

- A packet sniffer is a wire-tap device that plugs into computer networks and eavesdrops on the network traffic.
- Sniffers are the best tools for hackers to attack computers. Network administrators use Sniffers for network troubleshooting and security analysis. Many sniffing and anti sniff packages available on the Internet for download.
- Network Sniffers are tools used to watch over networks as well as collect all kinds of information including diagnostic information. The sniffer was first introduced by Network General Corporation in 1988.
- You can download the following sniffers from the following site :
  - Tcpdump **http://www.tcpdump.org**
  - Windump **http://netgroup-serv.polito.it/windump**
  - Snort **http://www.snort.org**
  - Ethereal **http://www.ethereal.com**
  - Sniffit **http://reptile.rug.ac.be/~coder/sniffit/sniffit.html**
  - Dsniff **http://www.monkey.org/~dugsong/dsniff**
- **Sniffing packages used for network traffic analysis to**
  1. Identify the type of network application used.
  2. Identify the hosts using the network.
  3. Identify the bottlenecks.
  4. Capture data sniffing packages used for troubleshooting of network applications.
  5. Create network traffic logs

1.8.1 Tcpdump and Windump

- TCPdump is a network debugging tool runs under command line. It allows user to intercept and display TCP/IP and other packets being transmitted or received over a network. It is frequently used to debug applications that generate or receive network traffic.

- TCPdump also used for debugging the network setup itself, by determining whether all necessary routing is occurring properly, allowing the user to further isolate the source of a problem.
- TCPdump is a UNIX tool. It is used to gather data from network, decipher the bits, and display the output in a semi coherent fashion. It works on Linux, Solaris, BSD, Mac OS X etc.
- TCPdump uses the libpcap library to capture packets. It can be used for intercepting and displaying the communications of another user or computer.
- A user with privileges acting as a router or gateway through which unencrypted traffic such as TELNET or HTTP passes can use TCPdump to view login IDs, passwords, the URLs and content of websites being viewed, or any other unencrypted information.
- You can download from **http://www.tcpdump.org**
- Tcpdump can only be used by the root user. It can decode and monitor the header data of
  - a. Internet Protocol (IP)
  - b. Transmission Control Protocol (TCP)
  - c. User Datagram Protocol (UDP)
  - d. Internet Control Message Protocol (ICMP)
- It captures packets based on a wide range user-specified criteria, and can save the traffic in different formats.

Syntax :

```
$ tcpdump
TCPdump: listing on eth1
0 packets received by filter
0 packets dropped by kernel.
$ tcpdump -i eth1
14:59:26.608728 IP xx.domain.netbcp.net.52497 > valh4.lell.net.ssh: . ack 540 win 16554
14:59:26.610602 IP resolver.lell.net.domain > valh4.lell.net.24151: 4278 1/0/0 (73)
14:59:26.611262 IP valh4.lell.net.38527 > resolver.lell.net.domain: 26364+ PTR?
```

Sr. No.	Options	Remarks
1.	-F	Use file as input for the filter expression.
2.	-i	Listen on interface. If unspecified, tcpdump searches the system interface list for the lowest number.

3.	-p	Do not put the interface into promiscuous mode
4.	-r	Read packets from file. Standard input is used if file is `` -".
5.	-w	Write the raw packets to file rather than parsing and printing them out.
6.	-n	Do not convert addresses to names.
7.	-q	Quick output. Print less protocol information so output lines are shorter.
8.	-S	Print absolute, rather than relative, TCP sequence numbers.
9.	-t	Do not print a timestamp on each dump line
10.	-tt	Print an unformatted timestamp on each dump line
11.	-e	Print the link-level header on each dump line.
12.	-A	Print each packet in ASCII
13	-c	Exit after receiving count packets.

- TCPdump or Windump has default output length of the size of datagram is 68 bytes. TCPdump does not collect whole output for display.

Output of TCPdump = Frame header + IP header + TCP header + TCP data

68 bytes = 14 bytes + 20 bytes + 20 bytes + 14 bytes

Windump :

- **Windump** is a free version of tcpdump for Windows. WinDump comes in two parts.
  1. **WinPcap :** It is a set of network capture drivers which uses to obtain packet-level access to network interfaces in the computer.
  2. **Windump a program** itself is invoked from the command line after installing the WinPcap library.
- Windump supports all TCPdumps's flags, parameters and settings.

Syntax :

```
C:\> windump [ -aBdDeflnNOpqRStvxX ] [ -c count ] [ -F file ]
[ -i interface ] [ -m module ] [ -r file ]
[ -s snaplen ] [ -T type ] [ -w file ]
[ -E algo:secret ] [ expression]
```

Options :

Sr. No.	Options	Remarks
1.	-a	Attempt to convert network and broadcast addresses to names.
2.	-c	Exit after receiving count packets.
3.	-d	Dump the compiled packet
4.	-e	Print the link-level header on each dump line.
5.	-f	Print `foreign' internet addresses numerically rather than symbolically
6.	-F	Use file as input for the filter expression
7.	expression	Selects which packets will be dumped.
8.	-t	Don't print a timestamp on each dump line.
9.	-tt	Print an unformatted timestamp on each dump line

1.8.2 Wireshark

- Wireshark is the most widely used graphical application for network monitoring and analysis. It is open-source and runs on most popular computing platforms including UNIX, Linux, and Windows. It is available for download from **http://www.wireshark.org.**
- Wireshark is initiated by Gerald Combs under the name Ethereal. First version was released in 1998. The name Wireshark was adopted in June 2006. Wireshark is a free and open source packet analyzer. Wireshark is software that "understands" the structure of different networking protocols.
- Wireshark is a network packet/protocol analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible. Wireshark is perhaps one of the best open source packet analyzers available today for **UNIX** and **Windows.**
- Wireshark does not support intrusion detection system. Wireshark is a GUI Network Protocol Analyzer. Wireshark software has been developed towork on Microsoft Windows, Linux, Solaris, and Mac OS X.

Use of wireshark :

1. Network administrators use it to troubleshoot network problems.
2. Network security engineers use it to examine security problems.

3. Developers use it to debug protocol implementations.
4. People use it to learn network protocol internals.
5. Displays the network traffic in human-readable format.

- Use filters to capture only packets of interest to you. Wireshark uses two types of filters :
  1. ‡ Capture filters
  2. ‡ Display filters
- Capture filters : Filtered while capturing. Like TCPDump. Wireshark contains a powerful capture filter engine that helps remove unwanted packets from a packet trace and only retrieves the packets of our interest.
- ‡ Display filters let you compare the fields within a protocol against a specific value, compare fields against fields, and check the existence of specified fields or protocols. More detailed filtering. Allows to compare values in packets but not real time.
- Fig. 1.8.1 shows wireshark startup screen.

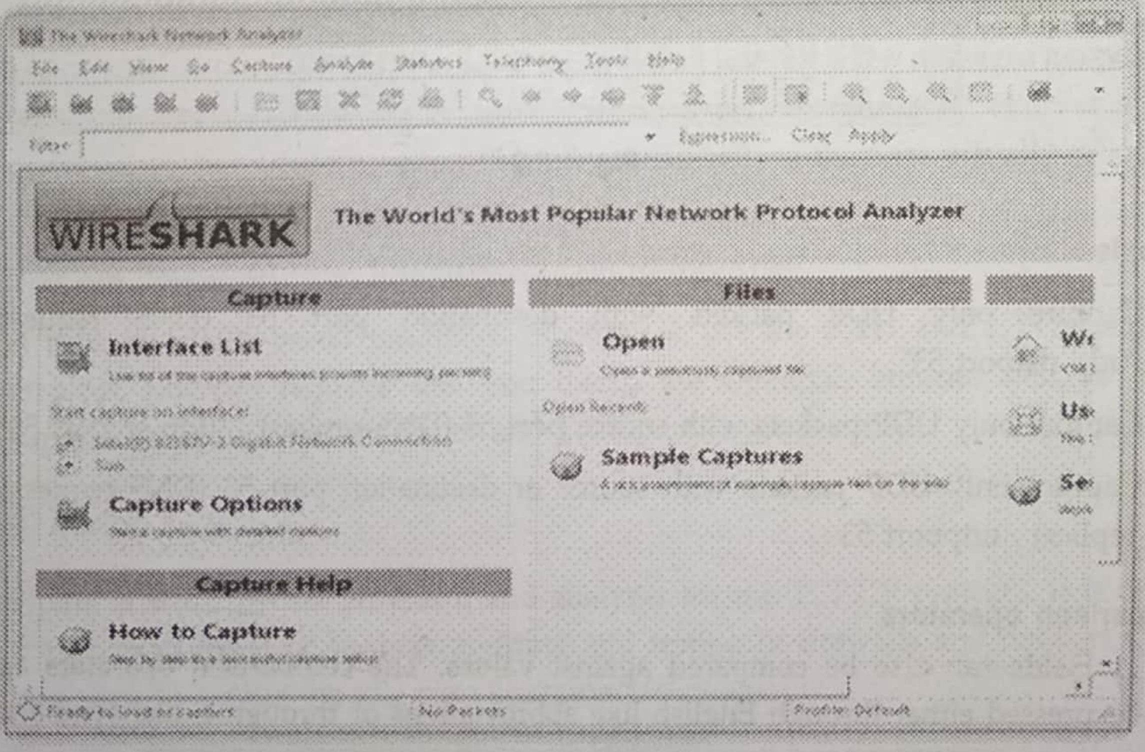

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Capture
Interface List
Start capture on interface:
Capture Options
Capture Help
How to Capture
Files
Open
Open Recent:
Sample Captures
Ready to load or capture
No Packets
Profile: Default

Fig. 1.8.1

- Fig. 1.8.2 shows Wireshark graphical user interface.

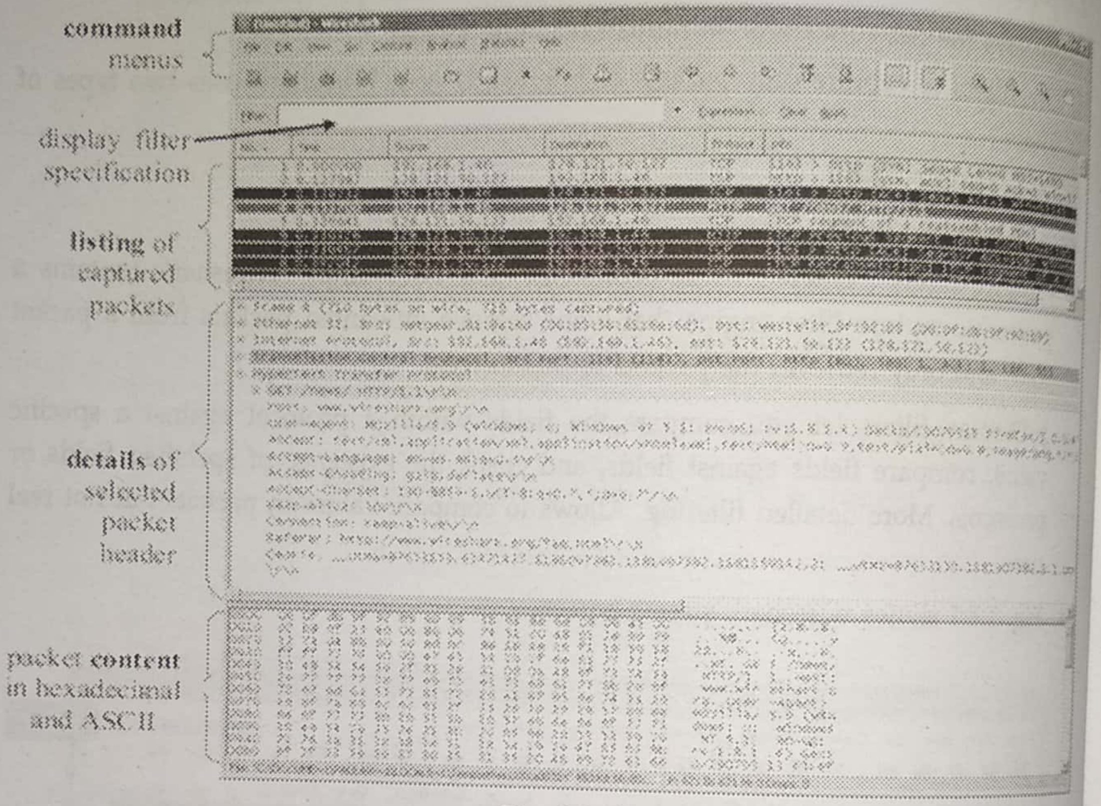

command menus
display filter specification
listing of captured packets
details of selected packet header
packet content in hexadecimal and ASCII

Fig. 1.8.2

Example :

1. Capture only UDP packets with destination port 53 (DNS requests) : "udp dstport 53"
2. Capture only UDP packets with source port 53 (DNS replies) : "udp srcport 53"
3. Capture only UDP packets with source or destination port 53 (DNS requests and replies) : udpport 53

Comparison operators

- ‡ Fields can also be compared against values. The comparison operators can be expressed either through English like abbreviations or through C-like symbols.

Symbol	Meaning
==	Equal (eq)
!=	Not equal (ne)
>	Greater than (gt)
<	Less than (lt)

>=	Greater than or equal to (ge)
<=	Less than or equal to (le)
( )	Grouping

Logical expressions

- Tests can be combined using logical expressions. These too are expressible in C-like syntax or with English like abbreviations :

Symbol	Meaning
&&	Logical AND
||	Logical OR
!	Logical NOT

1.8.3 Ettercap

- Ettercap is a tool made by Alberto Ornaghi and Marco Valleri and is basically a suite for man in the middle attacks on a LAN. It supports active and passive dissection of many protocols.
- Man-In-The-Middle(MITM) attacks occur when the attacker manages to position themselves between the legitimate parties to a conversation. The attacker spoofs the opposite legitimate party so that all parties believe they are actually talking to the expected other, legitimate parties.
- You can download from **http://ettercap.sourceforge.net/**
- It runs on UNIX based machines. In order to use the SSH1 and HTTPS sniffing features, Ettercap requires that you install the OpenSSL libraries first, to allow support for Secure Sockets Layer and Transport Layer Security.

1.8.4 Hping

- Hping is a free packet generator and analyzer for the TCP/IP protocol. It is one of the de facto tools for security auditing and testing of firewalls and networks, and was used to exploit the idle scan scanning technique.
- You can download from *www.hping.org/download*
- It is used to bypass filtering devices and allows users to fragment and manipulate IP packets.
- Hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping UNIX command. It supports TCP, UDP, ICMP

and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.

- Hping doesn't have the ability to spoof MAC addresses, but that still doesn't prevent us from working around it.

1.9 Kismet

- Kismet is a wireless network and device detector. Kismet works with Wi-Fi interfaces, bluetooth interfaces.
- Kismet works on Linux, OSX and, to a degree, windows 10 under the WSL framework. On Linux it works with most Wi-Fi cards, bluetooth interfaces and other hardware devices. On OSX it works with the built-in Wi-Fi interfaces and on Windows 10 it will work with remote captures.
- Kismet is an 802.11 layer-2 wireless network detector, sniffer and intrusion detection system.
- A Wireless Access Point (WAP) broadcasting its signal and SSID is easy for any device with a wireless card to detect. On the other hand, some individuals and organizations choose to attempt to hide or not broadcast their SSID in an effort to be more secure.
- In either case, Kismet is able to identify wireless network traffic as packets are traversing its antennae, giving hackers the ability to identify potential targets as they move. This is a technique called wardriving and is possible because Kismet is limited solely by the ability of the Wireless Network Interface Controller (WNIC) to catch packets based on the range and strength of the WAP(s) broadcasting.
- Kismet is able to identify WAPs in use, SSIDs and the type of encryption used on a network. With this information, penetration testers can use additional open-source tools to gain additional access and privileges into the network.
- **Configuration models :** Kismet is designed as a client-server application, but it can be run as a standalone application, as a server supporting a number of clients and even as a server with "drone" Kismet installations across a network, each monitoring its own wireless hardware and all forwarding captured packets to a server.

□□□

and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.

- Hping doesn't have the ability to spoof MAC addresses, but that still doesn't prevent us from working around it.

1.9 Kismet

- Kismet is a wireless network and device detector. Kismet works with Wi-Fi interfaces, bluetooth interfaces.
- Kismet works on Linux, OSX and, to a degree, windows 10 under the WSL framework. On Linux it works with most Wi-Fi cards, bluetooth interfaces and other hardware devices. On OSX it works with the built-in Wi-Fi interfaces and on Windows 10 it will work with remote captures.
- Kismet is an 802.11 layer-2 wireless network detector, sniffer and intrusion detection system.
- A Wireless Access Point (WAP) broadcasting its signal and SSID is easy for any device with a wireless card to detect. On the other hand, some individuals and organizations choose to attempt to hide or not broadcast their SSID in an effort to be more secure.
- In either case, Kismet is able to identify wireless network traffic as packets are traversing its antennae, giving hackers the ability to identify potential targets as they move. This is a technique called wardriving and is possible because Kismet is limited solely by the ability of the Wireless Network Interface Controller (WNIC) to catch packets based on the range and strength of the WAP(s) broadcasting.
- Kismet is able to identify WAPs in use, SSIDs and the type of encryption used on a network. With this information, penetration testers can use additional open-source tools to gain additional access and privileges into the network.
- **Configuration models :** Kismet is designed as a client-server application, but it can be run as a standalone application, as a server supporting a number of clients and even as a server with "drone" Kismet installations across a network, each monitoring its own wireless hardware and all forwarding captured packets to a server.

□□□