# Patching and Vulnerabilities

A Hands-On Approach

# Environment Setup

- Victim 1 VM Windows XP (10.1.1.1)
- Victim 2 Laptop Windows XP (10.1.1.2)
- Victim 3 VM Windows 7 (10.1.1.3)
- Victim 4 VM RHEL 7.4 (10.1.1.4)
- Travis Laptop MAC OS (10.1.1.250)
- Travis Laptop Kali Linux VM (10.1.1.253)

# Terminology

- Software Patch
- Malware
- Spyware
- Exploit
- Vulnerability
- Virus (Computer Virus)
- Virtual Machine (VM)

# Definitions

## Malware (*noun*):

Software intended to damage a computer, mobile device, computer system, or computer network, or to take partial control over its operation.

## Virus (*noun*):

A segment of self-replicating code planted illegally in a computer program, often to damage or shut down a system or network.

## Spyware (*noun*):

Software that is installed surreptitiously and gathers information about an Internet user's browsing habits, intercepts the user's personal data, etc., transmitting this information to a third party.

## Virtual Machine aka VM (*noun*):

A **virtual machine** is a software computer that, like a physical computer, runs an operating system and applications. The **virtual machine** is comprised of a set of specification and configuration files and is backed by the physical resources of a host.

# Definitions cont.

## Vulnerability (*noun*):

A weakness which allows an attacker to reduce a system's information assurance. **Vulnerability** is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.

## Exploit (*noun*):

A software tool designed to take advantage of a flaw in a computer system, typically for malicious purposes such as installing malware.

## Software Patch (*noun*):

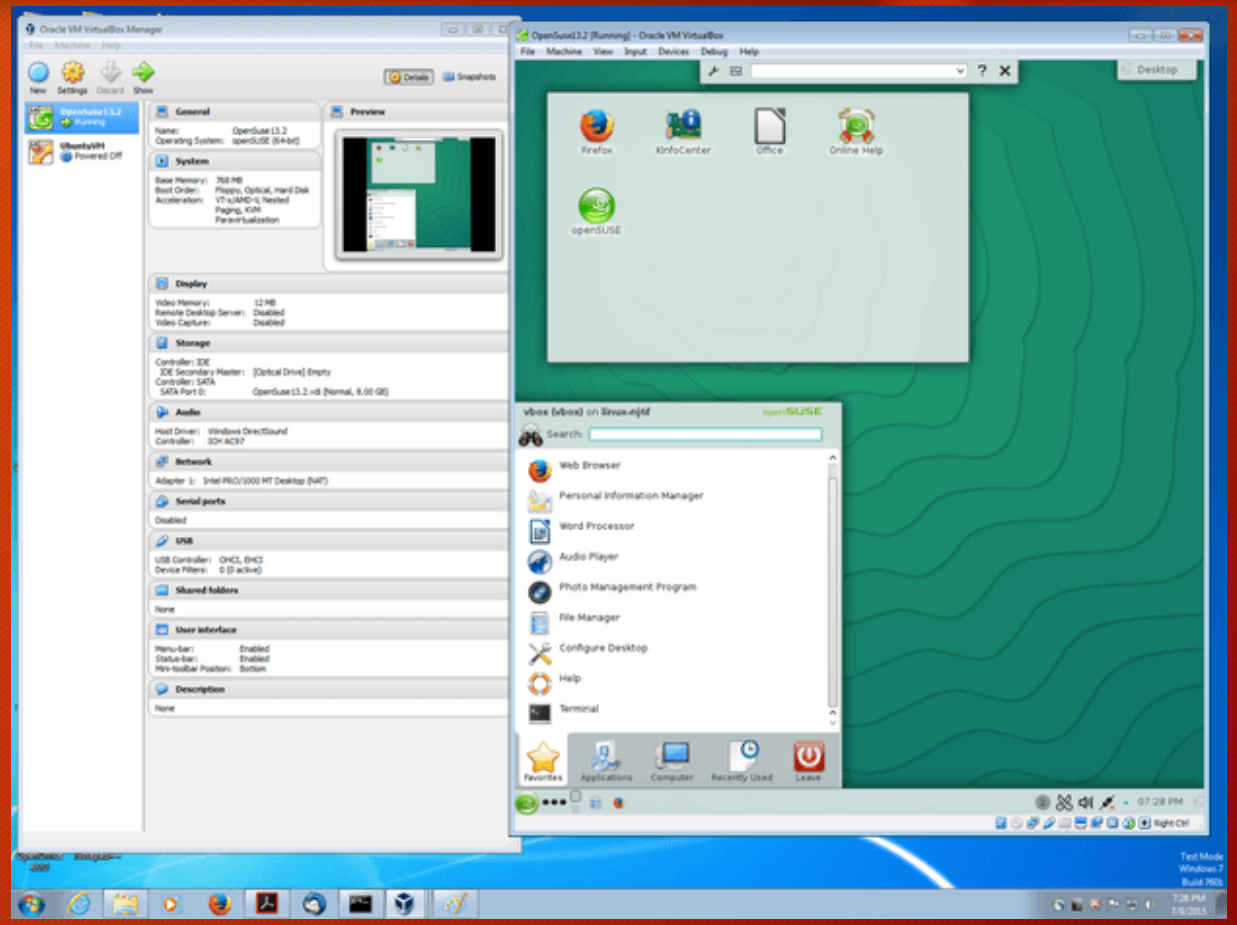
A small piece of code designed to be inserted into an executable program in order to fix errors in, or update the program or its supporting data.

# Tools

- Virtual Box
- Kali Linux (aka Backtrack Linux)
- Metasploit
- Nessus
- Wireshark
- NMap

# VirtualBox

**VirtualBox is a general-purpose full virtualizer for x86 hardware, targeted at server, desktop and embedded use.**



Downloaded From: https://www.virtualbox.org/wiki/Downloads

# Kali Linux

Kali Linux is an open source project that is maintained and funded by Offensive Security, a provider of world-class information security training and penetration testing services. In addition to Kali Linux, Offensive Security also maintains the Exploit Database and the free online course, Metasploit Unleashed.

Downloaded From: https://www.kali.org/downloads/

# Nessus


- Nessus scans for viruses, malware, backdoors, hosts communicating with botnet-infected systems, known/unknown processes as well as web services linking to malicious content.
- Report what matters to responsible parties with exploitability, severity modification, scan scheduling and deliver remediation reports via targeted emails.
- Nessus supports non-credentialed, remote scans; credentialed, local scans for deeper, granular analysis of assets; and offline auditing on a network device's configuration. Nessus supports the widest range of network devices, operating systems, databases, applications in physical, virtual and cloud infrastructures.

# Metasploit


- The Metasploit Project host the world's largest public database of quality-assured exploits. Have a look at our exploit database - it's right here on the site.
- Metasploit was the first software to provide a common framework for a large selection of exploits. Think of it as an abstraction layer ("Meta") for exploits (abbreviated "sploits"). Get it?
- Metasploit's most popular payload is called Meterpreter, which enables you to do all sorts of funky stuff on the target system.

Downloaded From: https://www.rapid7.com/products/metasploit/download.jsp

# Wireshark


- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- Read/write many different capture file formats
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2

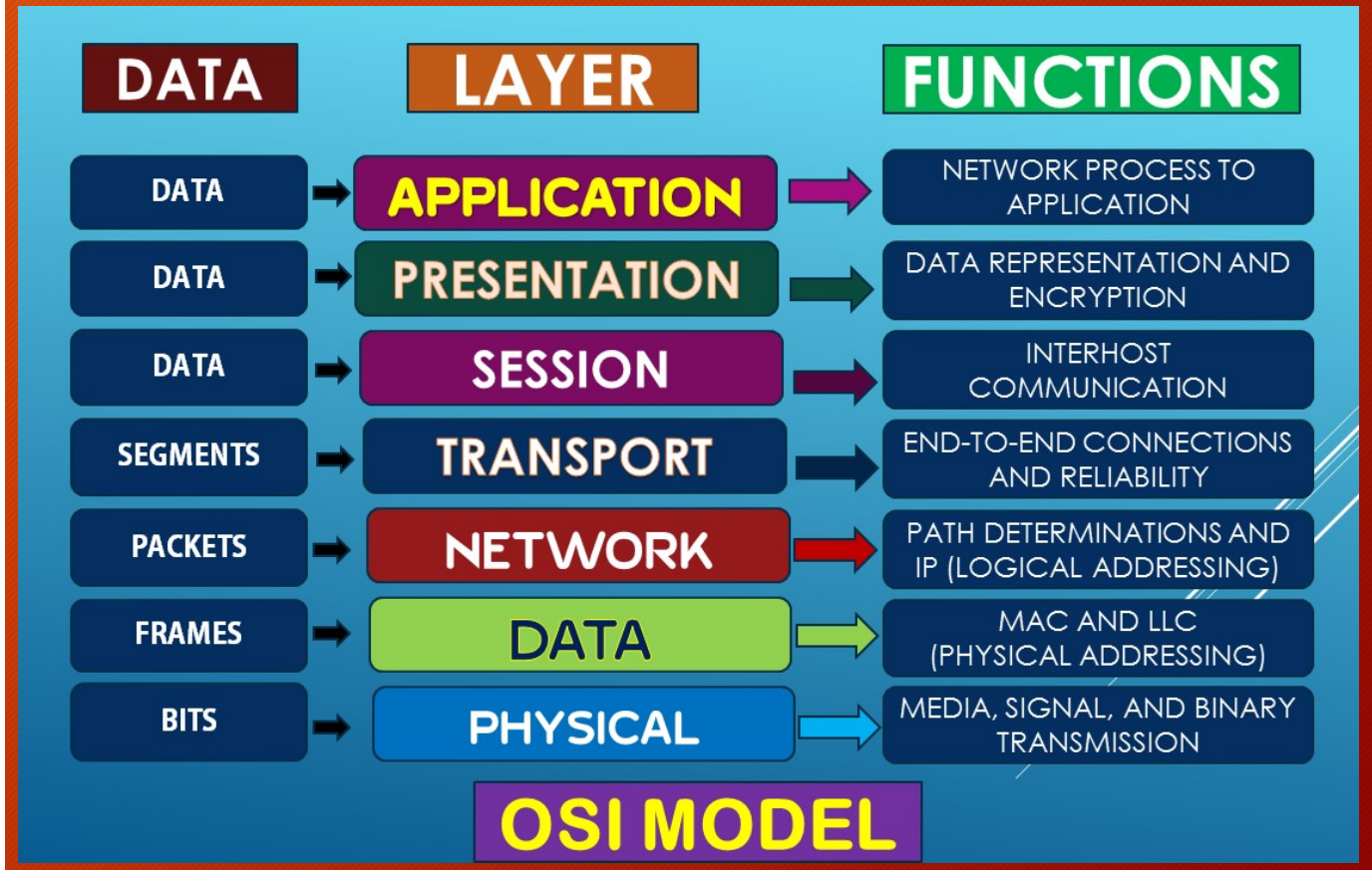
Downloaded From: https://www.wireshark.org/#download

# Theory

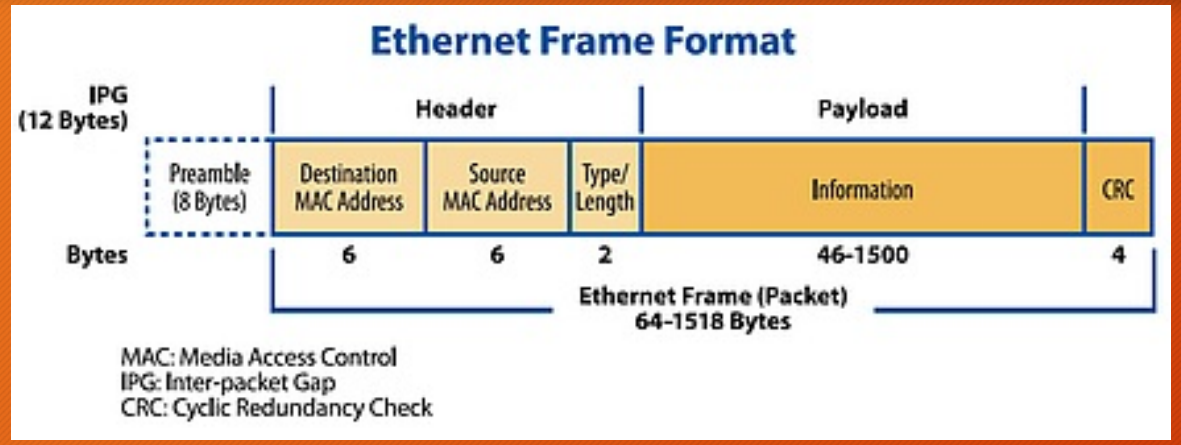
- OSI Reference Model
- IP Packet Structure
- TCP Packet Structure

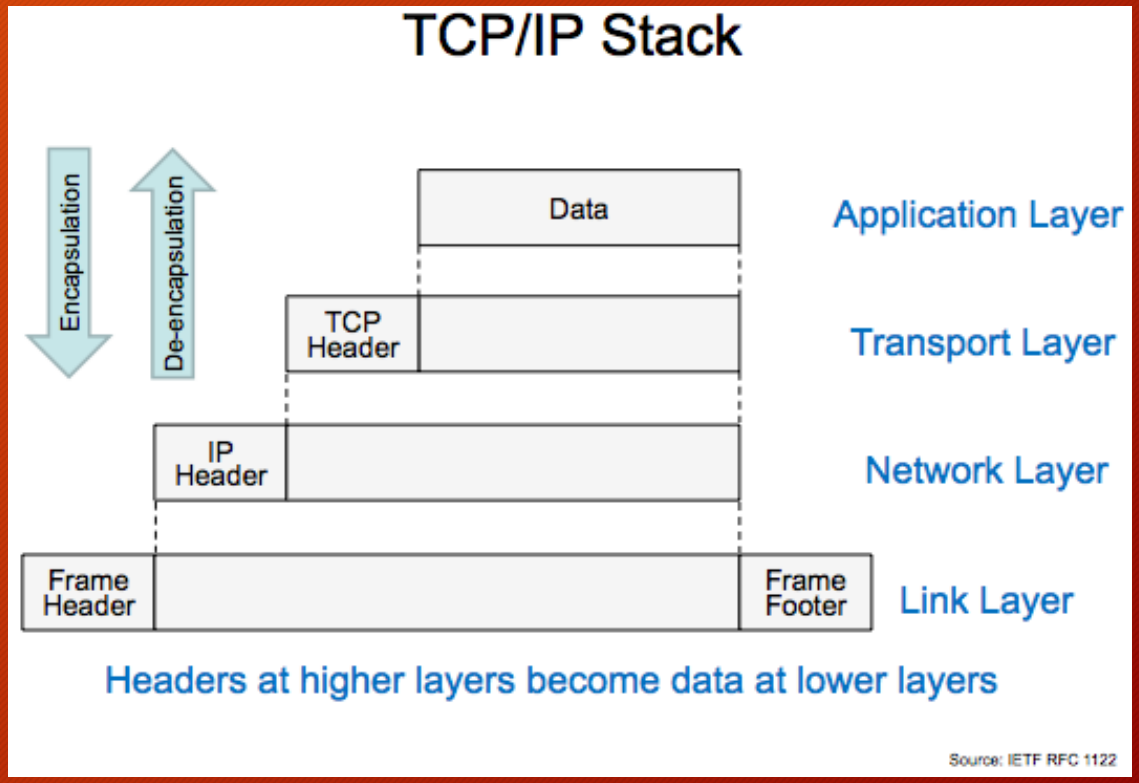
# OSI Reference Model

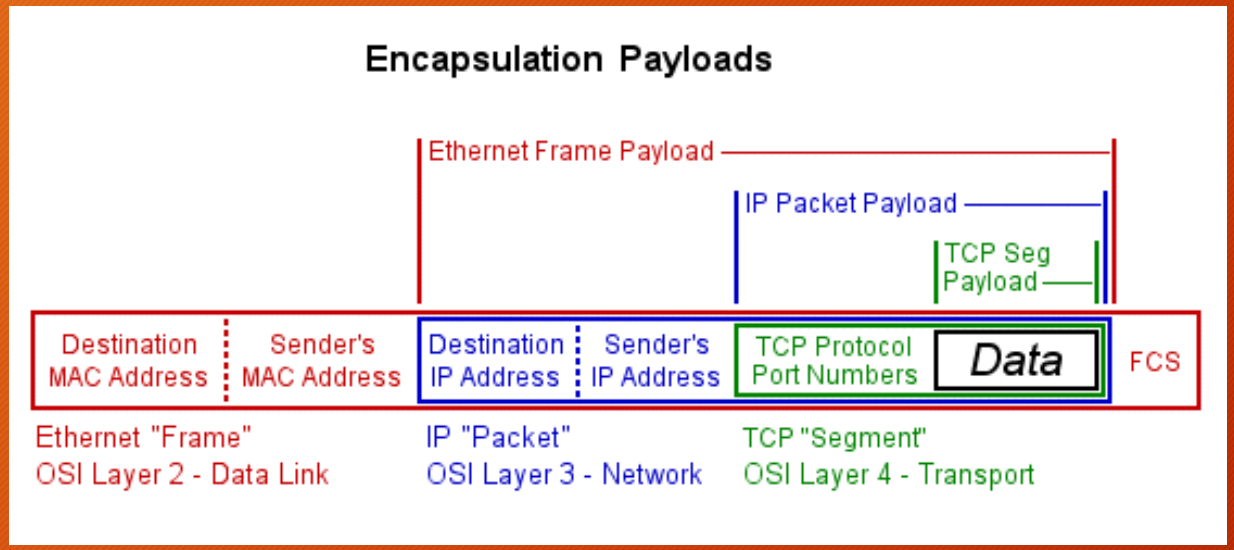
| Layer | Function | Example |
|---|---|---|
| **Application (7)** | Services that are used with end user applications | SMTP, |
| **Presentation (6)** | Formats the data so that it can be viewed by the user<br><br>Encrypt and decrypt | JPG, GIF, HTTPS, SSL, TLS |
| **Session (5)** | Establishes/ends connections between two hosts | NetBIOS, PPTP |
| **Transport (4)** | Responsible for the transport protocol and error handling | TCP, UDP |
| **Network (3)** | Reads the IP address form the packet. | Routers, Layer 3 Switches |
| **Data Link (2)** | Reads the MAC address from the data packet | Switches |
| **Physical (1)** | Send data on to the physical wire. | Hubs, NICS, Cable |



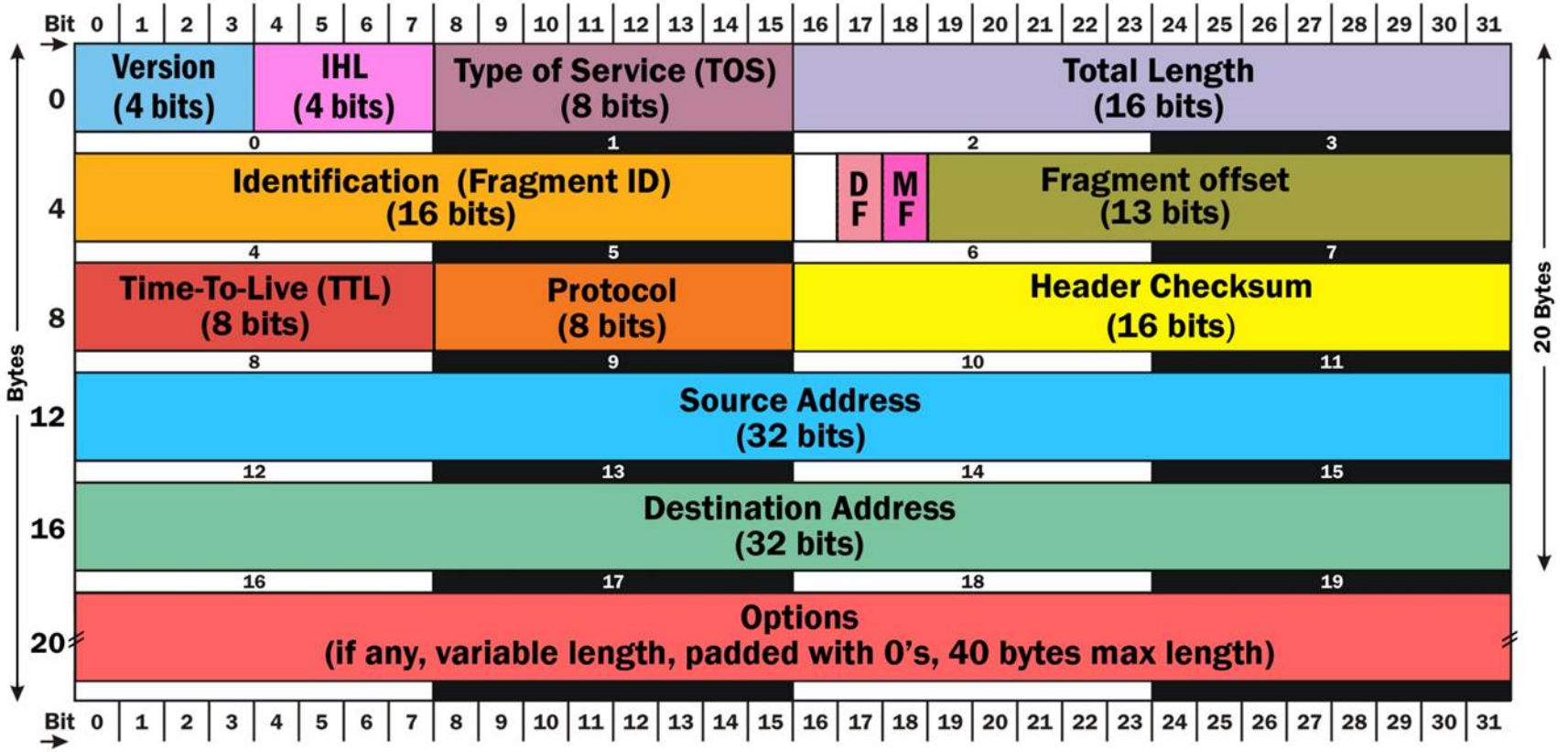
# Network Packet – Ethernet Packet/Frame



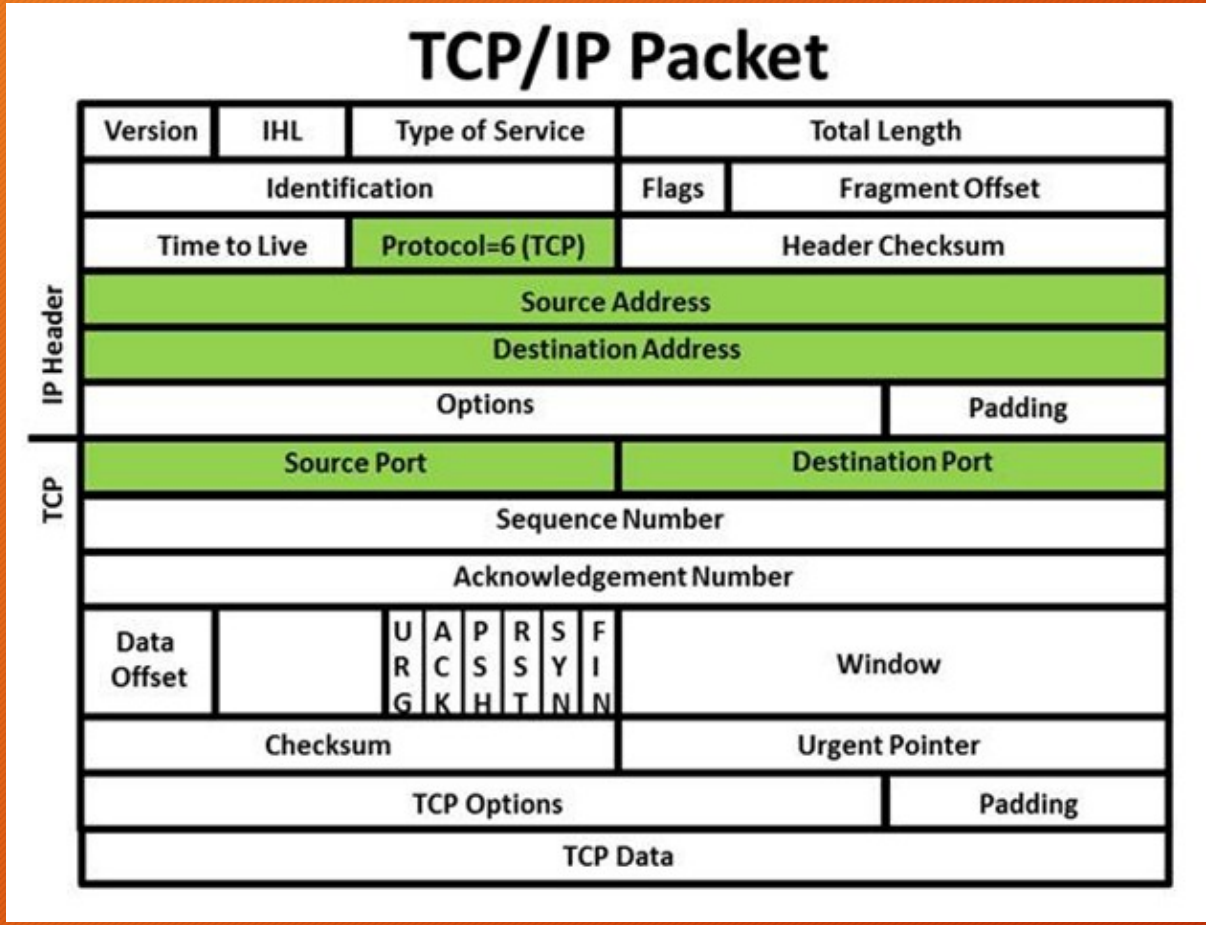



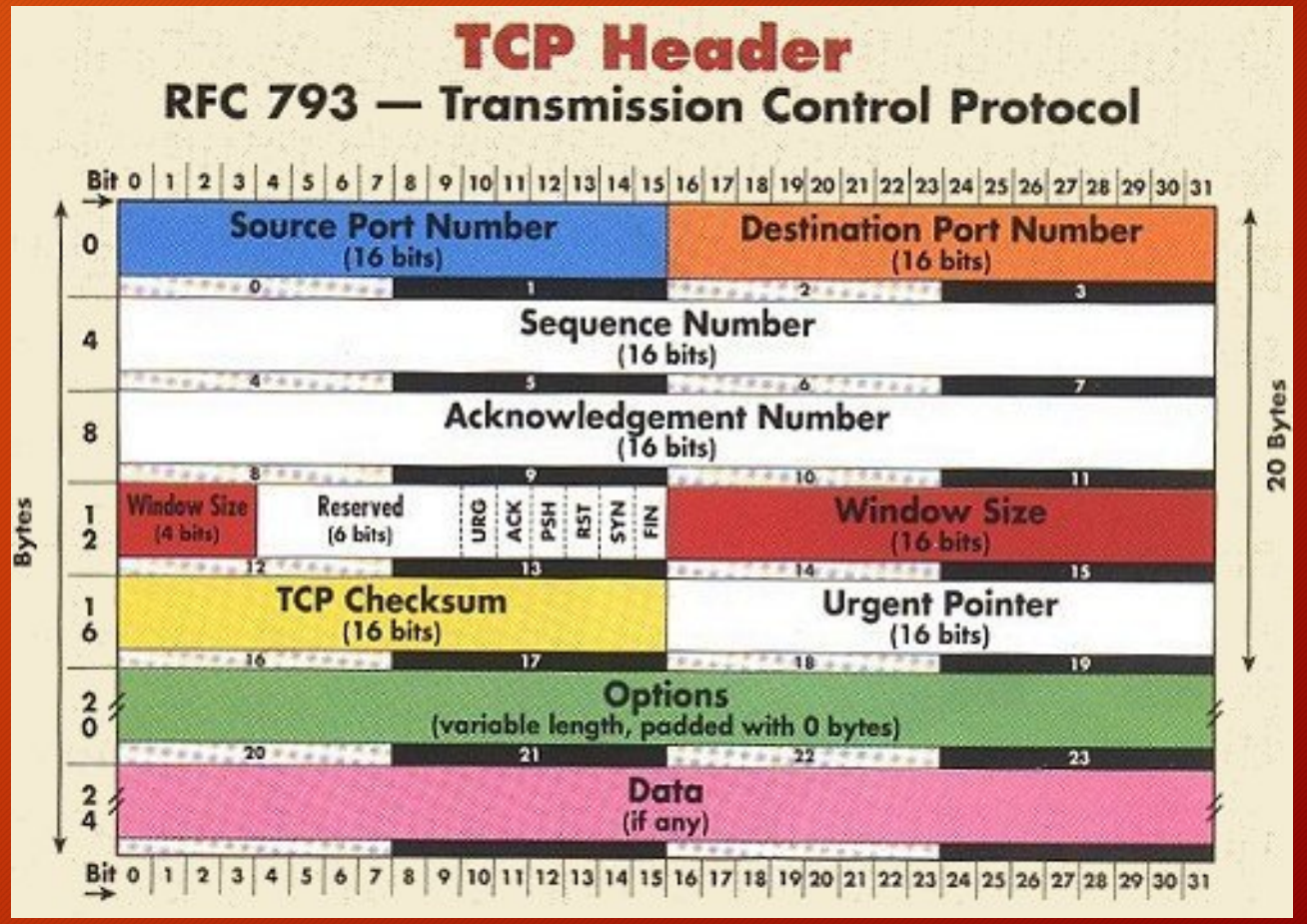



# Network Packet – IP Packet Structure

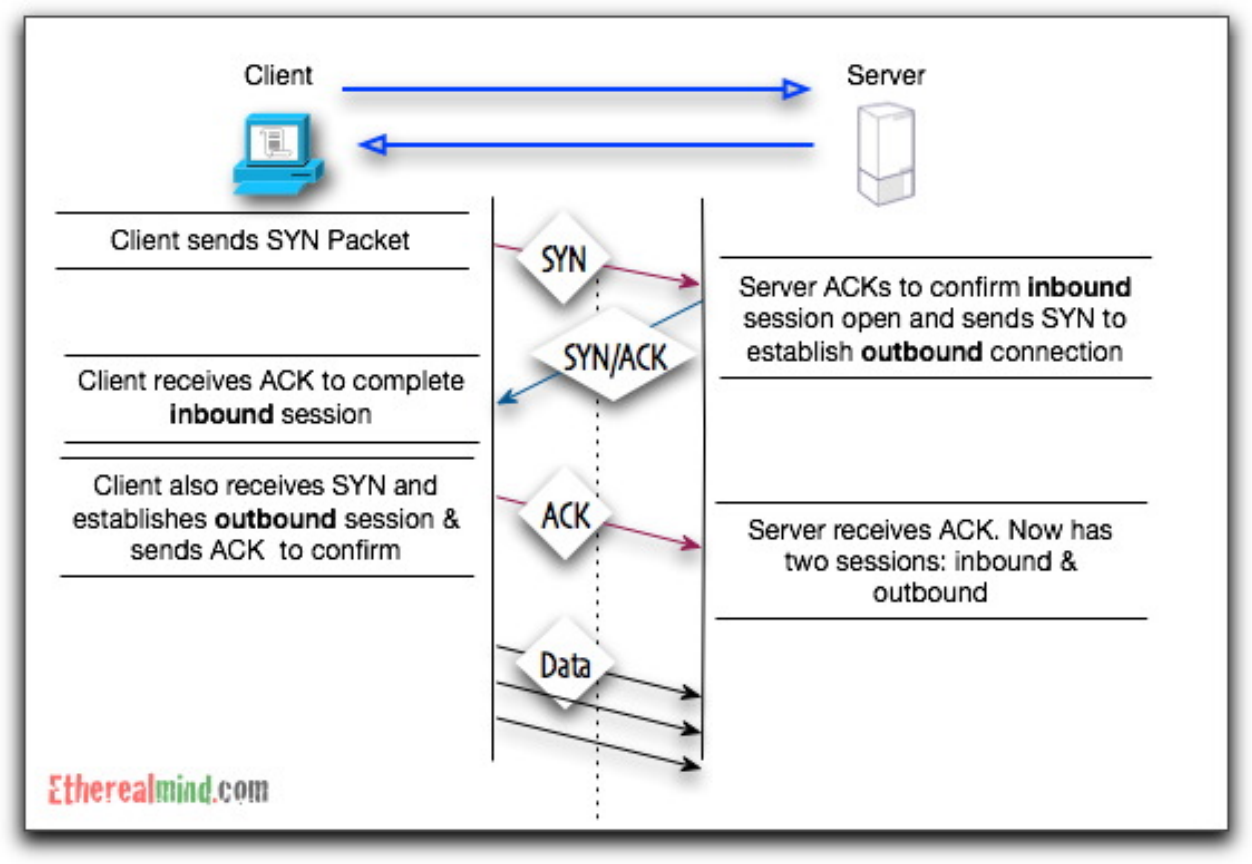


# Network Packet – TCP Packet Structure



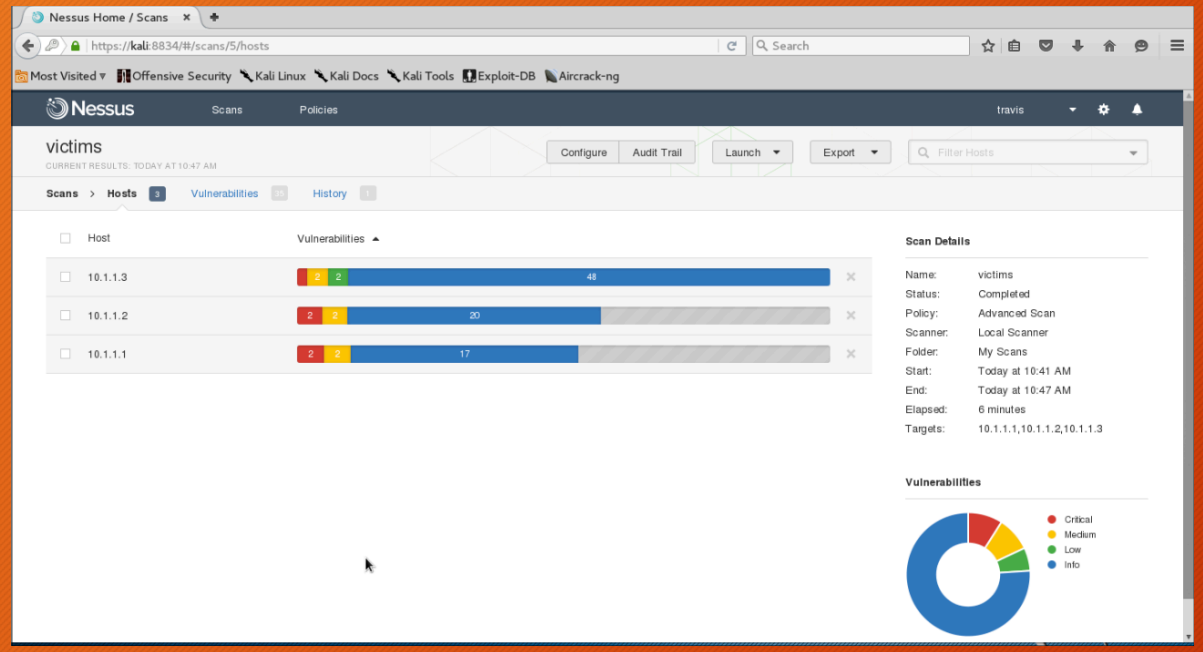
# TCP 3-Way Handshake

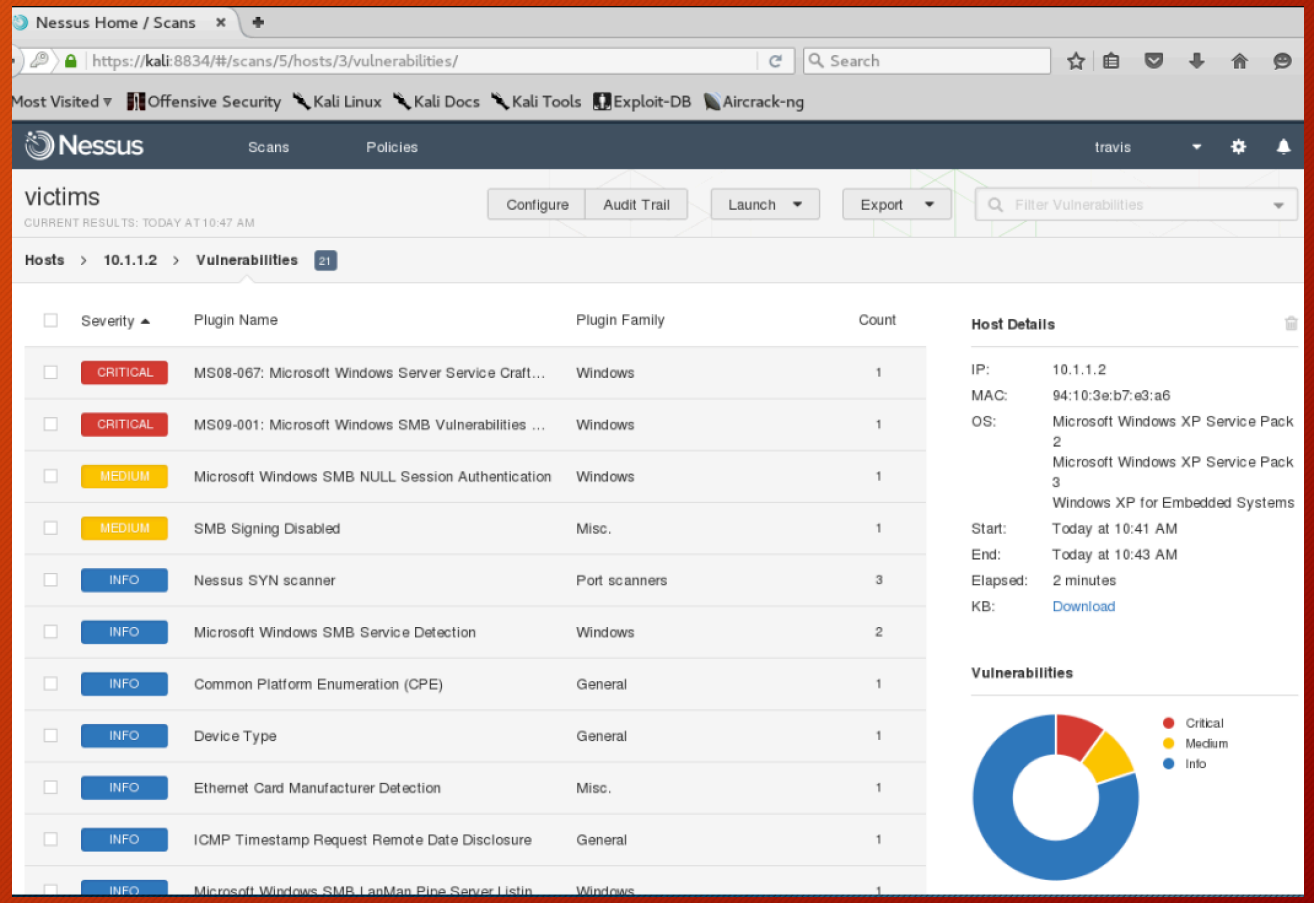



# Demo

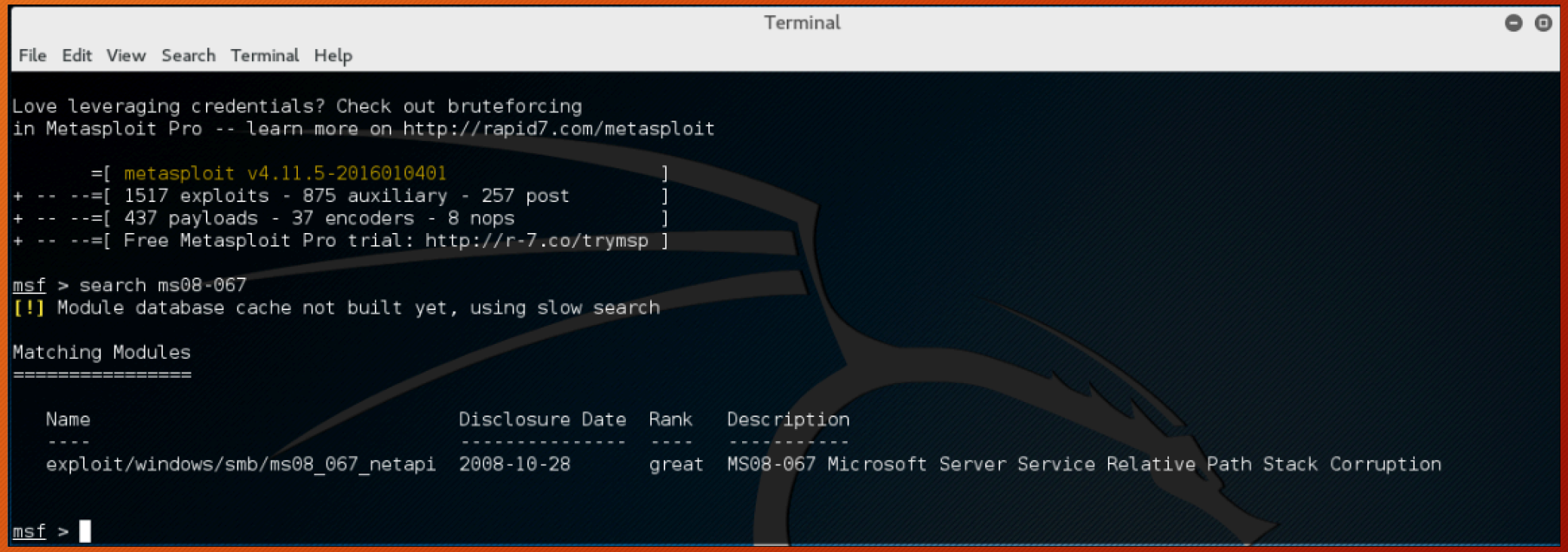
- Nessus and Metasploit
  - Nessus to perform system vulnerability scan
  - Metasploit to exploit and control system
    - Taking over webcom
    - Process takeover and keyboard scans
- Wireshark (Packet Captures)
  - FTP Capture Demo and Walk-Through

# Using Nessus to Scan a System



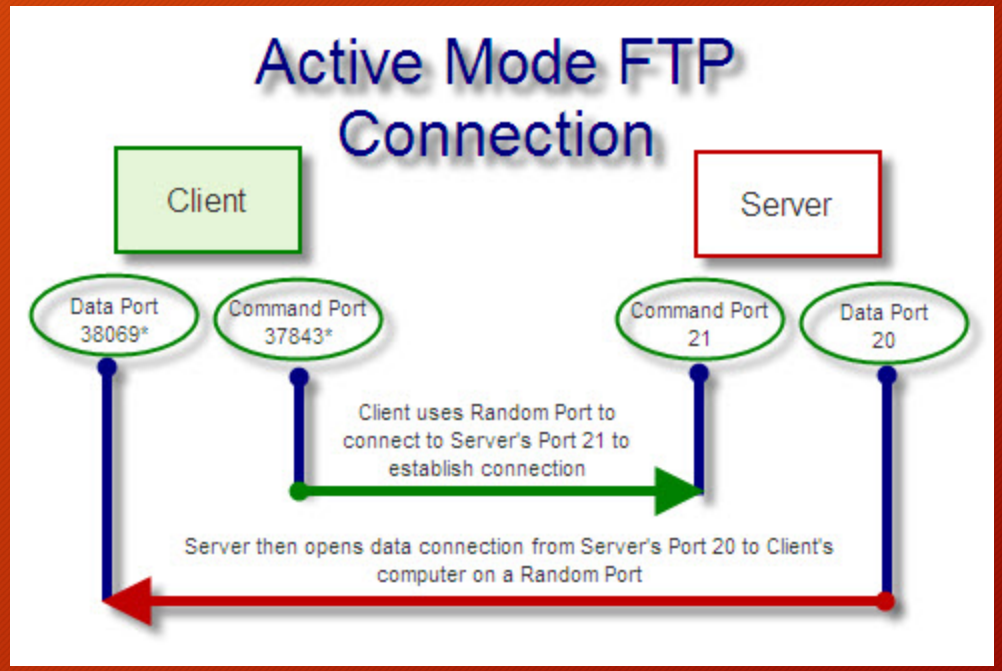
# Using Metasploit to Exploit a System



# Packet Captures with Wireshark

## FTP

File Transfer Protocol. Establishes a TCP connection between FTP client and FTP server using TCP ports 20/21. Standard FTP protocol does not use encryption and transmits all packets in clear text. FTP can be setup to use a UserName/Password combination, however, it is recommended to use SFTP or some other type of secure file transfer protocols to protect the security and integrity of the connection.



# Tracing an FTP Connection – Wireshark Demo