Cyber Security (CS)
GTU - 3150714

Dedicated Faculty, Committed Education
Darshan
Institute of Engineering & Technology

Unit-1

Systems Vulnerability Scanning

Prof. Maulik D Trivedi
Computer Engineering Department
Darshan Institute of Engineering & Technology, Rajkot
maulik.trivedi@darshan.ac.in
+91-9998265805

Outline

- Basic Fundamental Concepts of Computer Networks
- Overview of vulnerability scanning
- Open Port / Service Identification
- Banner / Version Check, Traffic Probe
- Vulnerability Probe, Vulnerability Examples
- Networks Vulnerability Scanning
- Understanding Port and Services tools
- Network Reconnaissance
- Network Sniffers and Injection tools

Basic Fundamental Concept of Computer Networks

Section - 1

Basic Fundamental Concept

- **IP Address**
  - An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.
  - An IP address serves two principal functions: host or network interface identification and location addressing.
- Two Version of IP address:
  - IPv4
  - IPv6
- IPv4 uses 32-bit for address. Example: 192.168.1.1
- IPv6 uses 128-bit for address. Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- IP addresses are usually written and displayed in human-readable notations.

Basic Fundamental Concept – Cont.

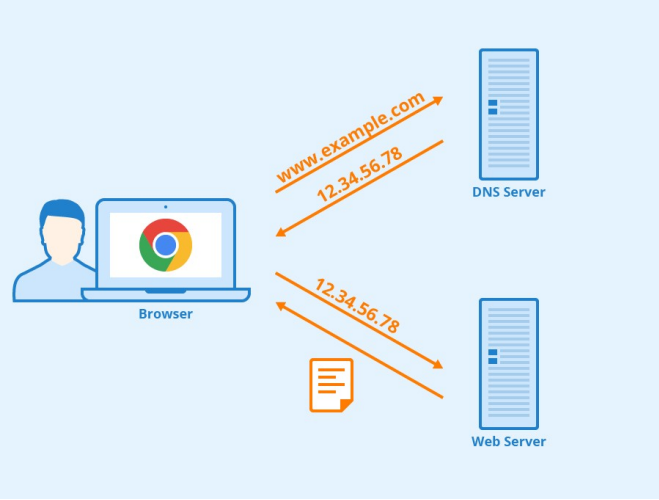
- **MAC Address**
  - A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment.
- MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet, Wi-Fi & Bluetooth.
- It is also known as physical address or hardware address.
- The MAC address is a string of usually six sets of two-digits or characters, separated by colons.
- For example, consider a network adapter with the MAC address 01:0a:95:9d:58:36.

Basic Fundamental Concept – Cont.

- Computer Network:
  - A computer network is a telecommunications network which allows computers to exchange data.
- In computer networks, networked computing devices exchange data with each other along network links (data connections).
- The connections between nodes are established using either cable media or wireless media.
- The best-known computer network is the Internet.
- Computer Port:
  - In computer hardware, a port serves as an interface between the computer and other computers or peripheral devices.
- Computer ports have many uses, to connect a monitor, webcam, speakers, or other peripheral devices.
- On the physical layer, a computer port is a specialized interface on a piece of equipment to which a plug or cable connects.

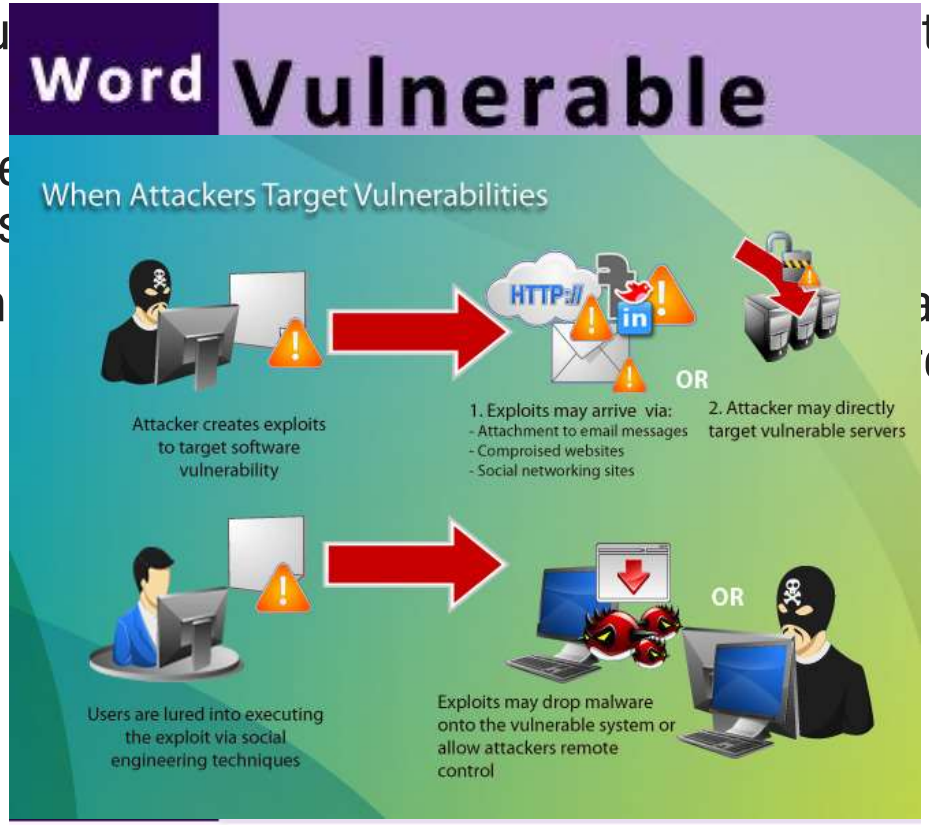
Basic Fundamental Concept – Cont.

- DNS stand for “domain name system”.
- It converting human-readable website name into computer-readable numerical IP addresses.
- For example:
  - If you want to visit Google, then open www.google.com into your web browser‘s address bar instead of IP address. However, your computer does not understand where www.google.com is located.
- Behind the scenes, the internet and other network use numerical IP addresses. www.google.com is located at the IP address 73.194.39.78 on the internet.



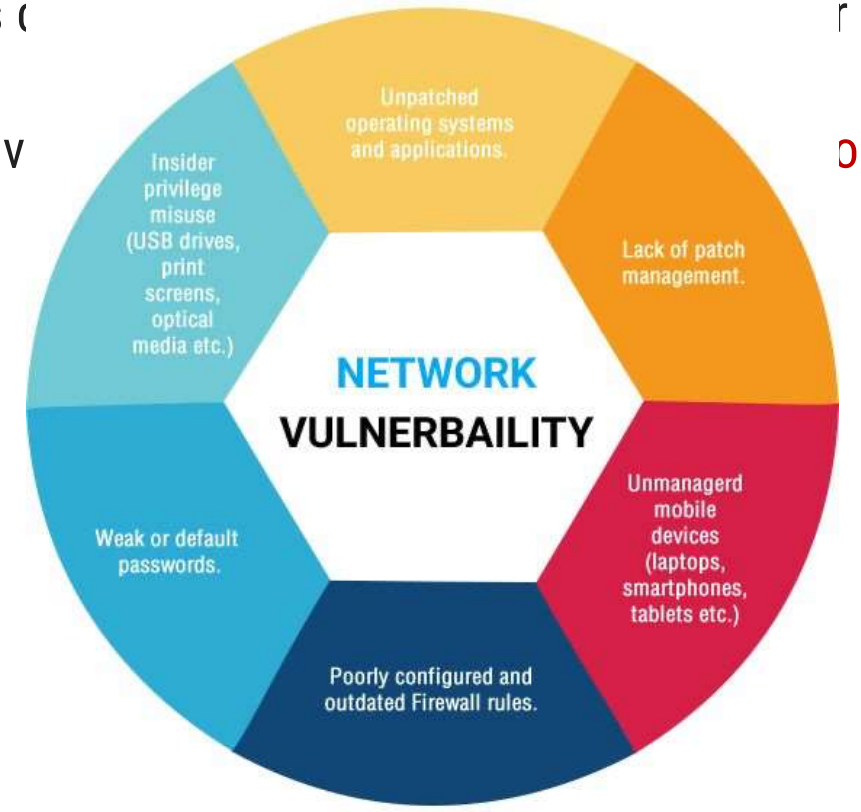
Overview of Vulnerability Scanning

- Vulnerability
  - vulnerability is a weakness which allows an attacker to reduce a system's security.
- Vulnerability scanning u… that are connected to the Internet.
- It can also refer to syste… that are not connected to the Internet in order to as…
- It is possible to know th… and managing network and websites. but it is not … reside in the network and websites.



Overview of Vulnerability Scanning – Cont.

- The vulnerability scanners provide you the automate security auditing and play an important role in your IT security.
- The vulnerability scanners (r up to thousands of different security risks.
- It produces a list of those v o overcome or reduce them.



Types of Vulnerability Scanners

- There are generally two types of vulnerability scanning tools:

1. **Network-based scanning tool:**

- Network-based scanning tools send network traffic to various network hosts and devices.
- It with the goal of gathering information that will indicate whether those systems have holes that can be exploited.
- Example: OpenVAS, Wireshark, NMAP, Nikto etc.

2. **Host-based scanning tool:**

- Host-based scanning tools are run on each host to scan for a wide range of system problems.
- It including unauthorized software, unauthorized accounts, unprotected logins, weak passwords and inappropriate access permissions.
- Example: OSSEC

Types of Vulnerability Scanners

- **Cloud-Based Vulnerability Scanners**
- Used to find vulnerabilities within cloud-based systems such as web applications, WordPress, and Joomla.
- **Host-Based Vulnerability Scanners**
- Used to find vulnerabilities on a single host or system such as an individual computer or a network device like a switch or core-router.
- **Network-Based Vulnerability Scanners**
- Used to find vulnerabilities in an internal network by scanning for open ports. Services running on open ports determined whether vulnerabilities exist or not with the help of the tool.
- **Database-Based Vulnerability Scanners**
- Used to find vulnerabilities in database management systems. Databases are the backbone of any system storing sensitive information. Vulnerability scanning is performed on database systems to prevent attacks like SQL Injection.

False Negative

- The vulnerability scanners use predefined tests to identify vulnerabilities (also called vulns).
- If the scanner has insufficient test then the scanner does not report the vulnerability exists on the system.
- It can be known as false negative.

Zero-day Vulnerability

- Zero-day vulnerability refers to a hole in software that is unknown to the vendor.
- This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it- this exploit is called a zero day attack.
- Zero-day vulnerabilities are particular dangerous because they represent a gap in knowledge between the attacker and defender.

False Positive

- If the scanner has a poorly written test then scanner reports vulnerability even if it does not exist on a system. It may produce a false positive.
- It wastes time as administrators must follow up to manually check the vulnerability that is actually vulnerable or not.
- Some of the free and very useful vulnerability scanners are:
  - Netcat
  - Socat

Open Port / Service Identification

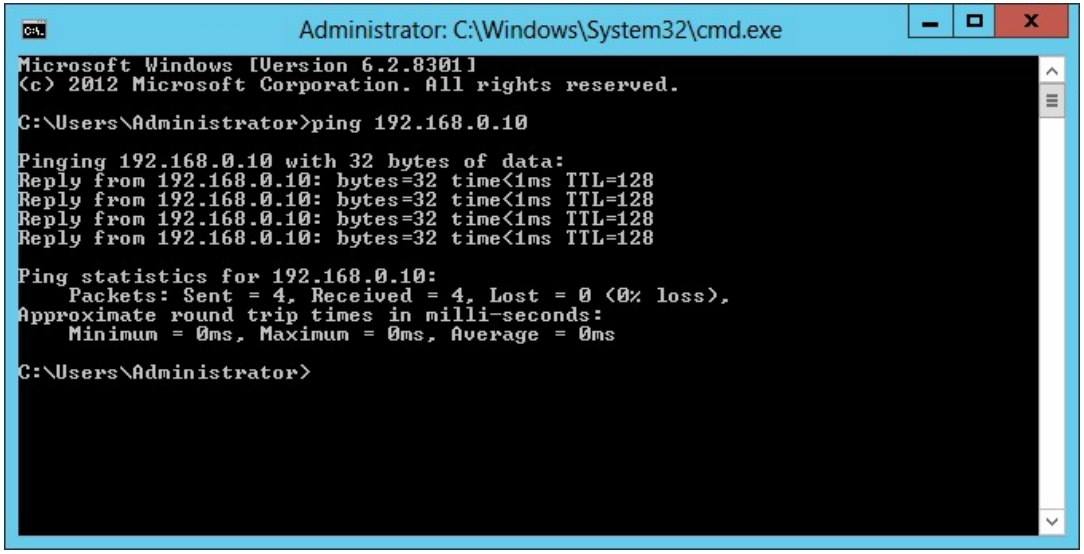
- Some services are very insecure. Telnet (port 23) is famous for its lack of encryption that leaks passwords.
- Hence Secure Shell (SSH) is widely accepted and reduced the presence of telnet on the Internet.
- Services do not always run on default ports, hence the scanner must rely on banners and "nudges" to produce a response from a listening port.
- Services do not always declare themselves. Telnet and SMTP (port 25) services return text-based banners when receives request for connection. It does not wait for particular incoming data on that connection.
- HTTP (port 80) will not respond for connection until the service receives a request that contains data.
- This way, scanners may distinguish whether an HTTP or SMTP service is listening on non-standard port.

Banner / Version Check

- Some services declare information about themselves without receiving particular data from a client.
- Banner Grabbing:
  - Banner grabbing is a technique used to gain information about a computer system on a network and the services running on its open ports.
  - Administrators can use this to take inventory of the systems and services on their network.
  - Tools commonly used to perform banner grabbing are Telnet, nmap, zmap and Netcat.
- Example:
  - SSH command
- If you know the version of SSH and target operating system then it is very easy for someone to compromise the host.
- System administrators usually remove or change banners to make them more secure, but this doesn't remove the vulnerability.

Probe

- In Computer Security, a probe is an attempt to gain access to a computer and its files through a known or probable weak point in the computer system.
- A probe is an action taken or an object used for the purpose of learning or collecting data about the state of the network.
- For example, an empty message can be sent simply to see whether the destination actually exists. Ping is a common utility for sending such a probe.



Two Type of Probe

1. Traffic Probe
2. Vulnerability Probe

Traffic Probe

- Some services declare information about themselves without receiving particular data from a client.
- But all services do not do that. However, lots of them will if you just ask.
- For example, a web service will not give response until it receives data from the client.
- A valid HTTP request using the HEAD method will provide some useful information like web server information, information about installed server operating system etc. which can be useful to compromise the host.
- Traffic probes try to use valid requests. Because valid protocol messages are less likely to crash or interrupt a service
- If a web server didn't handle the HEAD method without crashing then the chances of compromising increases. So this type of buggy service must need to be fixed to lower the chances of compromising.

Vulnerability Probe

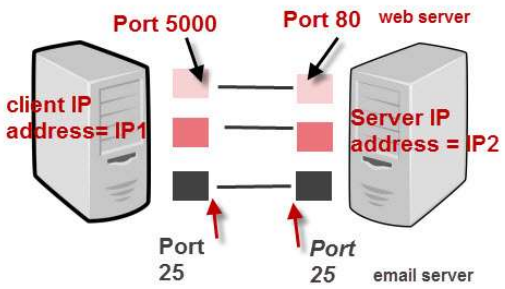
- Some security bugs cannot be identified without sending a payload that exploits (using something to one's own advantage) a suspected vulnerability.
- These types of probes are more accurate—they rely on direct observation not only on port numbers or service banners.
- But they also carry more risk of interrupting the service, because the test payload must be trying to either produce or take advantage of an error in the service's code.
- An easy-to-understand example of a vulnerability probe is an HTML injection check for a web application.
- A snippet of HTML might look like Results for 'zombies'...
- An attacker who exploits HTML injection vulnerability like this could steal data from the user or damage the web site.
- The hacker can take advantage of vulnerability to compromise the system or network.

Vulnerability Probe – Cont.

- The outcome may be to crash the software, causing a denial of service, or retrieve data, like pulling usernames and passwords from a database, or completely compromise the operating system by gaining root or administrator access.
- Exploits take many shapes. It can be simple binary shellcode or clever bits of text appended to URL parameters.
- Discovering vulnerability typically just means uncovering a software fault.
- Developing an exploit means taking advantage of that software fault to give the attacker an advantage against the system.

TCP/IP Ports and Sockets

- On a TCP/IP network every device must have an IP address.
- The **IP address identifies** the **device** e.g. computer.
- However an IP address alone is **not sufficient for running network applications**, as a computer can run multiple applications and/or services.
- Just as the IP address identifies the computer, The **network port identifies** the **application** or **service** running on the computer.
- The diagram below shows a computer to computer connection and identifies the IP addresses and ports.



IP Address + Port number = Socket

TCP/IP Ports And Sockets

- A **socket** is the **combination** of **IP address** + **port**
- A **connection between** two **computers uses** a **socket**.

Port Number Ranges and Well Known Ports

- A port number uses **16 bits** and so can therefore have a value from **0 to 65535 decimal.**
- Port numbers are divided into ranges as follows:
  - **Port numbers 0-1023 – Well known ports**.
    - These are allocated to server services by the **Internet Assigned Numbers Authority** (**IANA**).
    - e.g **Web servers** normally use **port 80** and **SMTP servers** use **port 25**.
  - **Ports 1024-49151- Registered Port**
    - These can be registered for services with the IANA and should be treated as **semi-reserved**.
    - **User written programs should not use these** ports.
  - **Ports 49152-65535**
    - These are **used by client programs** and you are **free to use** these in client programs.
    - When a Web browser connects to a web server the browser will allocate itself a port in this range.
    - Also known as **ephemeral ports**.

Common Well Known Port Numbers

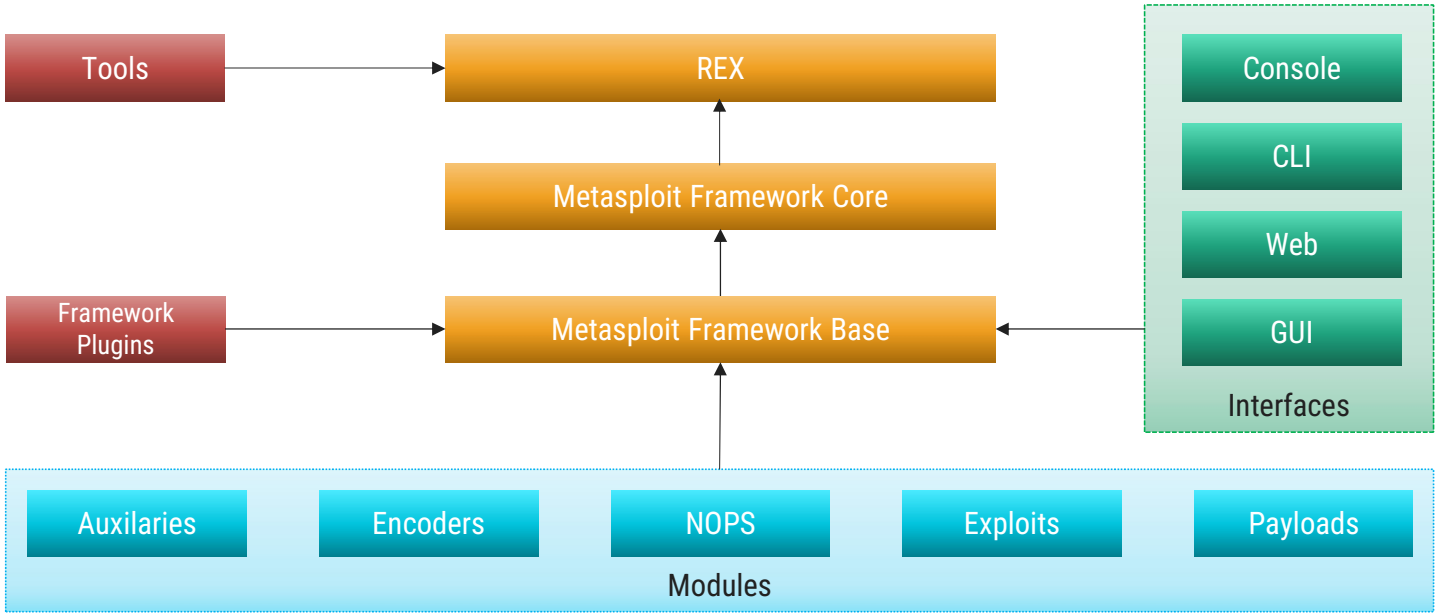
Number	Assignment
20	File Transfer Protocol (FTP) Data Transfer
21	File Transfer Protocol (FTP) Command Control
22	Secure Shell (SSH) Secure Login
23	Telnet remote login service, unencrypted text messages
25	Simple Mail Transfer Protocol (SMTP) E-mail routing
53	Domain Name System (DNS) service
67, 68	Dynamic Host Configuration Protocol (DHCP)
80	Hypertext Transfer Protocol (HTTP) used in the World Wide Web
110	Post Office Protocol (POP3)
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
143	Internet Message Access Protocol (IMAP) Management of digital mail
161	Simple Network Management Protocol (SNMP)
194	Internet Relay Chat (IRC)
443	HTTP Secure (HTTPS) HTTP over TLS/SSL

Port Scanning

- **Port scanner**: Software designed to probe server or host for Open ports.
- Used by administrator to verify security policy.
- Used by attacker to identify running services on host.
- **Port scan**: A process that sends a client request to server for finding active ports.
- **Open port**: Host sends a reply indicating port is active.
- **Close port**: Host sends a reply that connection will be denied.
- **Filtered**: There was no reply from the host.
- Vulnerability can be with **open ports** or **operating system of running host**.

Metasploit

- Metasploit is an open-source framework used for security development and testing.
- It is best tool for developing and executing exploit code against a remote target machine.



- Modules built on top of libraries, accessed via interfaces to conduct exploitation tasks. Plugins hook directly into the framework to add commands to the interface, etc.

Metasploit – Cont.

- Using the built-in tools available in Metasploit, security professionals can conduct penetration tests, verify patch installations and even perform regression testing.
- Source code of Metasploit is in ruby.
- The tool has about 500 modules, including hundreds of remote exploits that can be useful for various releases of Windows, Linux, UNIX, and the Mac OS.
- Metasploit is very easy to use even a person who can drive a mouse or a keyboard can take over a vulnerable system.
- It uses PostgresSQL database to manage data for scans, sessions, and post-hack information.

Metasploit Hacking Session Steps

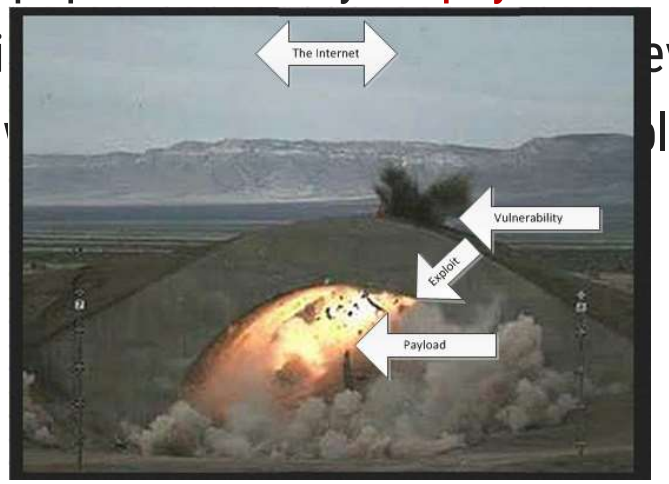
- A Metasploit hacking session progresses through several steps:
- First, you must have to identify target.
- Next, Choose an exploit to use against a vuln on the target.
- Customize the exploit to the target, which usually just requires specifying the IP address against which to run the exploit.
- Next, select a payload. Like the exploit, usually just requires specifying an IP address; in some cases you might change a TCP port number.
- Finally, launch the customized exploit and await the successful compromise of the target.

Difference between Payload and Exploits

- A payload refers to the part of malware which performs a malicious action.
- In the analysis of malicious software such as worms, viruses and Trojans, it refers to the software's harmful results.
- Examples of payloads include data destruction, messages with insulting text or spam e-mail messages sent to a large number of people.
- An exploit (meaning "using something to one's own advantage") is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability in order to cause unexpected behaviour to occur on computer software, hardware, or something electronic.
- Such behaviour includes things like gaining control of a computer system or a denial-of-service attack.
- The exploit is what delivers the payload.

Example: Payload and Exploits

- Take a missile as an analogy. You have the rocket and fuel and everything else in the rocket, and then you have the warhead that does the actual damage.
- Without the warhead, the missile doesn't do very much when it hits.
- Additionally, a warhead isn't much use if it goes off in your bunker without a rocket delivering it.
- The delivery system (missile) is the exploit and the payload (warhead) is the code that actually does something.
- Exploits give you the ability to 'pop a shell/run your payload code'.
- Example payloads are things li… …everse shells etc.
- Payloads are only referred to … …le and not when using things like denial of service exploits.



Network Vulnerability Scanning - Netcat

- The Netcat performs function with a broad application to hacking and network debugging: It reads and writes data for TCP and UDP connections.
- Netcat enables you to redirect shell commands across a network
- Netcat interacts directly with a TCP or UDP service.
- You can inspect the raw data sent by a service, manually interact with the service, or redirect network connections with stdin, stdout.
- You can connect to text-based protocols like SMTP and HTTP, UDP services like DNS, and even binary protocols.
- Netcat is often called the “Swiss Army knife” of hacking.

Uses of Netcat

- Hackers have come up with hundreds of ways to use Netcat.
- Some of the uses of Netcat are given here in detail:
  - Obtain Remote Access to a Shell
  - Perform Basic Port Scanning
  - Identify more information about ports
  - Communicate with UDP Services
  - For IP Spoofing
  - Hijack a Service
  - Create Proxies and Relays
  - Bypass Port Filters

Socat

- Socat is a clone of Netcat with extensive configuration options.
- It supports several protocols, from OpenSSL to proxies to IPv4 and IPv6.
- Socat uses word-based directives on the command line.
- Socat is part of the BSD ports collection and available as a package for most Linux OS.
- Socat's command line follows a simple format, as follows:
  - $ socat options address1 address2
- The options resemble common "dash letter" flags such as -d, -h, and -v.
- A basic address specification consists of a keyword, followed by a list of parameters and behaviour options.

Socat – Cont.

- Address specifications are not case sensitive, but we will define them in uppercase to help distinguish them on the command line.
- For example, the following command connects stdio (the first address) to TCP port 80 on a remote host (the second address):
  - $ socat STDIO TCP:deadliestwebattacks.com:80
- Since the first address is stdio, you can pipe data into the command just as you would with nc or any other shell command. Traffic is forwarded between the two addresses.
- Hence, the data piped into stdio is forwarded to the TCP host, whose response makes the round trip back through stdio.

Datapipe

- A port redirection tool passes TCP/IP traffic received by the tool on one port to another port to which the tool points.
- A port redirection tool functions as a channel for TCP/IP connections.
- For example, you could place a datapipe on a system between a browser and a web server.
- If you pointed the browser to the listening port of the system with the redirection tool, the browser would see the contents of the web server without having to directly access the web server's IP address.
- Datapipe is a Unix-based port redirection tool. It runs on the UNIX OS.
  - $ ./datapipe
  - ./datapipe localhost localport remotehost remoteport

Datapipe – Cont.

- The localhost argument indicates the IP address on which to open the listening port.
- It may be the localhost interface (i.e., 127.0.0.1) or the address of a network interface on the
- local system from which the datapipe command is being executed.
- The localport argument indicates the listening port on the local system; connections will be made to this port number.
- On UNIX systems, you must have root privileges to open a listening port below 1024.
- If you receive an error similar to “bind: Permission denied,” your account may not have privileges to open a reserved port.
- The remoteport argument indicates the port to which data is to be forwarded.
- For example, in most cases if the target is a web server, the remoteport value will be 80.
- The remotehost argument indicates the hostname or IP address of the target.
- The easiest conceptual example of port redirection is forwarding HTTP traffic.

Datapipe – Cont.

- Here we set up a datapipe to listen on a high port, 9080 in this example, that redirects to a web site of our choice:
  - $ ./datapipe my.host 9080 80 www.google.com
- Now, we enter this URL into a web browser:
  - http://my.host:9080/
  - You should see Google's home page.
- Datapipe performs a basic function, but with a little creativity you can make it a powerful tool.
- Port redirection forwards traffic between TCP ports only.
- It does not perform protocol conversion or any other data manipulation.
- Redirecting web traffic from port 80 to port 443 will not change HTTP connections to encrypted HTTPS connections.
- Use an SSL proxy instead, such as Stunnel.

FPipe

- It implement port redirection techniques natively in windows. It adds UDP protocol and outbound source port number support, which does not in datapipe.
- FPipe is a TCP source port forwarder/redirector. It can create a TCP / UDP stream with a sourse port of your choice. This is useful for getting past firwalls that allow traffic with source ports of 23, to connect with internal servers.
- Fpipe runs on windows operating system. There is no need of priviledge user account and support from dynamic link library.
- Fpipe can run on local host of the application that you are trying to use to get inside firewall.
- When you start Fpipe, it will wait for a client to connect on its listening port.
- It makes a listening connection is made a new connection to the destination machine and port with the specified local source port will be made.
- When the full connection has been established, Fpipe forwards all the data received on its inbound connection to the remote destination port beyond the firewall.

Fpipe Option

Sr No.	Option	Description
1	-? Or -h	Display Help
2	-c	Max. allows simultaneous TCP connections. Default 32 connections are allowed.
3	-i	Listening interface IP address
4	-l	Listening port number
5	-r	Remote port number
6	-s	Source port used for outbound traffic
7	-u	It support UDP mode
8	-v	For verbose mode

Winrelay

- Winrelay is windows based port redirection tool. It uses static source port for redirected traffic.
- Some antivirus software consider as malicious software.
- Online games use datapipe and fpipe tools. Port redirction tools are useful for assigning the alternative port to a service.
- Source:
  - www.ntsecurity.nu/toolbox/winrelay/

Network Reconnaissance

- Reconnaissance attack is a kind of information gathering on network system and services. This enable the attacker to discover vulnerabilities or weaknesses on the network.
- Reconnaissance attack can be active or passive.
- Tools are:
  - AMAP: Application Mapper, uses the results from Nmap to mine for more information.
  - Nessus: It is vulnerability scanner.
  - Scanrand: It is fast network scanner.
  - Paratrace: TCP traceroute that utilizes selected TTL messages.
- Intruders are increasingly making use of compromised hosts to launch reconnaissance againt target networks.

NMAP

- Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.
- Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.
- Nmap uses raw IP packets in novel ways:
  - To determine what hosts are available on the network.
  - Available services (application name and version) those hosts are offering.
  - Operating systems (and OS versions) they are running.
  - Type of packet filters/firewalls are in use.
- It was designed to rapidly scan large networks, but works fine against single hosts.

- Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.
- In addition to the classic command-line Nmap executable, the Nmap suite includes:
  - An advanced GUI and results viewer (Zenmap).
  - A flexible data transfer, redirection, and debugging tool (Ncat).
  - A utility for comparing scan results (Ndiff).
  - A packet generation and response analysis tool (Nping).
- It was even featured in twelve movies, including The Matrix Reloaded, Die Hard 4, Girl With the Dragon Tattoo, and The Bourne Ultimatum.

NMAP Characteristics and Source

- Flexible
- Powerful
- Portable
- Easy
- Free
- Well Documented
- Supported
- Acclaimed
- Popular

- Source:
  - http://nmap.org/

THC – Amap (The Hackers Choice Amap)

- Amap was the first next-generation scanning tool for pentesters.
- It attempts to identify applications even if they are running on a different port than normal.
- It also identifies non-ascii based applications.
- This is achieved by sending trigger packets, and looking up the responses in a list of response strings.
- Most of port scanners assume that if a particular port is open, then default application for that port must be present.
- Amap probes these ports to find out what is really running on that port.
- Source:
  - https://github.com/vanhauser-thc/THC-Archive/tree/master/Tools
  - http://thc.segfault.net/thc-amap/

THC – Amap Modes

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

Network Sniffers and Injection

- A packet sniffer is a wire-tap device that plugs into computer networks and eavesdrops on the network traffic.
- Sniffers are the best tools for hackers to attack computers.
- Network administrators use sniffers for network troubleshooting and security analysis.
- Many sniffing and anti-sniffing packages available on the internet for download.
- Network sniffers tools are used to watch over networks as well as collect all kinds of information including diagnostic information.

Usages of Network Sniffer tools

- Sniffing packages used for network traffic analysis to:
  1. Identify the type of network application used.
  2. Identify the hosts using network.
  3. Identify the bottlenecks.
  4. Capture data sniffing packages used for troubleshooting of network application.
  5. Create network traffic logs.

TCPdump

- TCPdump is a network debugging tools runs under command line. It allows user to intercept and display TCP/IP and other packets being transmitted or received over a network.
- It is frequently used to debug applications that generate or receive network traffic.
- TCPdump also used for debugging the network setup itself, by determining whether all necessary routing is occurring properly, allowing the user to further isolate the source of a problem.
- It is UNIX based tool.
- It is used to gather data from network, decipher the bits and display the output in a semi coherent fashion.
- TCPdump uses the libpcap library to capture packets. It can be used for intercepting and displaying the communications of another user or computer.
- Source:
  - http://www.tcpdump.org

TCPdump Commands

- TCPdump can only be used by root user. It can decode and monitor the header data of
  - Internet protocol (IP)
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
  - Internet Control Message Protocol (ICMP)
- It captures packets based on a wide range user-specified criteria, and can save the traffic in different formats.
- Syntax:
  - **tcpdump** [**-AdDefIKlLnNOpqRStuUvxX**] [**-B** *buffer_size*] [**-c** *count*]
    [**-C** *file_size*] [**-G** *rotate_seconds*] [**-F***file*][**-i** *interface*] [**-m** *module*] [**-M** *secret*][**-r** *file*] [**-s** *snaplen*] [**-T** *type*] [**-w** *file*][**-W** *filecount*][**-E** *spi@ipaddr algo:secret,...*][**-y** *datalinktype*] [**-z** *postrotate-command*] [**-Z** *user*] [*expression*]

TCPdump Commands Example

- To print all packets arriving at or departing from *sundown*:
  - **$ tcpdump host sundown**
- To print traffic between *helios* and either *hot* or *ace*:
  - **$ tcpdump host helios and \(hot or ace \)**
- To print all IP packets between *ace* and any host except *helios*:
  - **$ tcpdump ip host ace and not helios**
- To print all traffic between local hosts and hosts at Berkeley:
  - **$ tcpdump net ucb-ether**
- To print all ftp traffic through internet gateway *snup*: (note that the expression is quoted to prevent the shell from (mis-)interpreting the parentheses):
  - **$ tcpdump ip and not net** *localnet*

Output of TCPdump

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

Output of TCPdump = Frame Header + IP Header + TCP Header + TCP Data

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

Windump

- It is a free version of TCPdump for windows. Windump comes in two parts.
  1. WinPcap: It is a set of network capture drivers which uses to obtain packet-level access to network interfaces in the computer.
  2. Windump a program itself is invoked from the command line after installing the WinPcap library.
- Windump supports all TCPdump's flags, parameters and settings.
- Source:
  - https://www.winpcap.org/
- Syntax:
  - C:\> windump [-aBdDeflnNOpqRStvxX] [-c count] [-F file]
    [-I interface] [-m module] [-r file]
    [-s snaplen] [-T type] [-w file]
    [-E algo:secret] [expression]

Windump Example

- See all packets in the capture file
  - windump -n -r filename.pcap
- Show only the first 2 packets
  - windump -n -r flename.pcap -c 2
- Tracking host by source MAC address
  - windump -n -r filename.pcap -e "ether src 00:a0:cc:3b:bf:fa"
- Tracking host by destination MAC address
  - windump -n -r filename.pcap -e "ether dst 00:a0:cc:3b:bf:fa"
- Tracking host by IP, whether that IP is source or destination
  - windump -n -r filename.pcap "host 192.168.0.1"
- Track host by source IP
  - windump -n -r filename.pcap "src host 192.168.0.1"
- Track host by destination IP
  - windump -n -r filename.pcap "dst host 192.168.0.1"

Wireshark

- Wireshark is a free and open source packet analyzer.
- It is used for network troubleshooting, analysis, software and communication protocol development and education.
- It runs on Linux, UNIX, OSx, BSD, Solaris, and Microsoft windows.
- It provides following functionality:
  - Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.
  - User can see all traffic visible on that interface.
  - If a remote machine captures packets and sends the captured packets to a machine running Wireshark using the TZSP protocol. So it can analyse packets captured on a remote machine at the time they are captured.
  - It understands the structure of different networking protocols. It can parse and display the fields along with their meanings as specified by different protocols.
  - You can use it to review traffic captured by tools like tcpdump or WinDump or use it to capture traffic directly.
  - It also supports capture formats from several other commercial and open source network sniffers.

Ettercap

- Ettercap is a free and open source network security tool for man-in-the-middle attacks on LAN.
- It can be used for computer network protocol analysis and security auditing.
- It runs on various UNIX- like operating systems including Linux, mac os x, BSD and Solaris, and on Microsoft windows.
- It is capable of intercepting traffic on a network segment, capturing passwords and conducting active eavesdropping against a number of common protocols.
- Ettercap works by putting the network interface into promiscuous mode and by ARP poisoning the target machines.
- Thereby it can act as a 'man in the middle' and unleash various attacks on the victims.
- Ettercap supports active and passive dissection of many protocols and provides many features for network and host analysis.

Ettercap - Modes of Operation

- Ettercap offers four modes of operation.
- These are as follows:
  - IP-based: packets are filtered based on IP source and destination.
  - MAC-based: packets are filtered based on MAC address, useful for sniffing connections through a gateway.
  - ARP-based: uses ARP poisoning to sniff on a switched LAN between two hosts.
  - PublicARP-based: uses ARP poisoning to sniff on a switched LAN from a victim host to all other hosts.

Features of Ettercap

- Character injection into an established connection. Characters can be injected into a server or to a client while maintaining a live connection.
- It supports sniffing of a password and username and even the data of an SSH1 connection.
- It supports sniffing of HTTP SSL secured data-even when the connection is made through a proxy.
- It supports in setting up a filter that searches for a particular string in the TCP or UDP payload and replaces it with a custom string or drops the entire packet.
- It can determine the OS of the victim host and its network adapter.
- It can kill connections of choices from the connection-list.
- It can hijack DNS requests.
- It can also find other poisoners on the LAN actively or passively.

Hping

- Hping is a free packet generator and analyzer for the TCP/IP protocol. It is one of the tools for security auditing and testing of firewalls and networks.
- It was used to exploit the idle scan scanning technique and now implemented in the NMAP security scanner.
- The new version of hping, hping3, is scriptable using the tcl language and implements an engine for string based, human readable description of TCP/IP packets, so that the programmer can write scripts related to low level TCP/IP packet manipulation and analysis in very short time.
- Hping also has a listen mode, enabling it to be used as an unsophisticated backdoor for covert remote access or file transfers.
- Hping's "listen" mode can be used for receiving data.
- When hping is in listen mode, it monitors traffic for a special "signature" that indicates it should capture the data to follow.

Use of Hping

- Determining a Host's Status When Ping Doesn't Work.
- Testing Firewall Rules.
- Stealth Port Scanning.
- Remote OS Fingerprinting.

Kismet

- Kismet is a free software and it is network detector, packet sniffer and intrusion detection system for 802.11 wireless LANs.
- Kismet will work with any wireless card which supports raw monitoring mode and can sniff 802.11a, 802.11b, 802.11g and 802.11n traffic.
- This runs under Linux, FreeBSD, NetBSD, openBSD, and mac OS X, Microsoft windows.
- Kismet has three separate parts.
- These are as follows:
  - A drone: it can be used to collect packets and then pass them on to a server for interpretation.
  - A server: it can either be used in conjunction with a drone or on its own, interpreting packet data and extrapolating wireless information and organizing it.
  - The client: it communicates with the server and displays the information the server collects.

Features of Kismet

- Kismet differs from other wireless network detector in working passively.
- It is able to detect the presence of both wireless access and wireless client.
- Kismet also includes basic wireless IDS features such as detecting active wireless sniffing programs including NetStumbler, as well as a number of wireless network attacks.
- It has the ability to log all sniffed packets and save them in a tcpdump/wireshark compatible file format.
- Kismet can also capture “per-packet information” headers.
- It has ability to detect default or not configured networks, probe requests, and determine what level of wireless encryption is used on a given access point.

Features of Kismet – Cont.

- Kismet supports channel hoping.
- This means that it is constantly changes from channel to channel non-sequentially, in a user defined sequence with a default value that leaves big holes between channels.
- The advantage with this method is that it will capture more packets because adjacent channels overlap.
- Kismet also supports logging of the geographical coordinates of the network if the input from a GPS receiver is additionally available.

Cyber Security (CS)
GTU - 3150714

Dedicated Faculty, Committed Education
Darshan
Institute of Engineering & Technology

Thank You

Prof. Maulik D Trivedi
Computer Engineering Department
Darshan Institute of Engineering & Technology, Rajkot
maulik.trivedi@darshan.ac.in
+91-9998265805

Cyber Security (CS)
GTU # 3150714

Dedicated Faculty, Committed Education
Darshan
Institute of Engineering & Technology

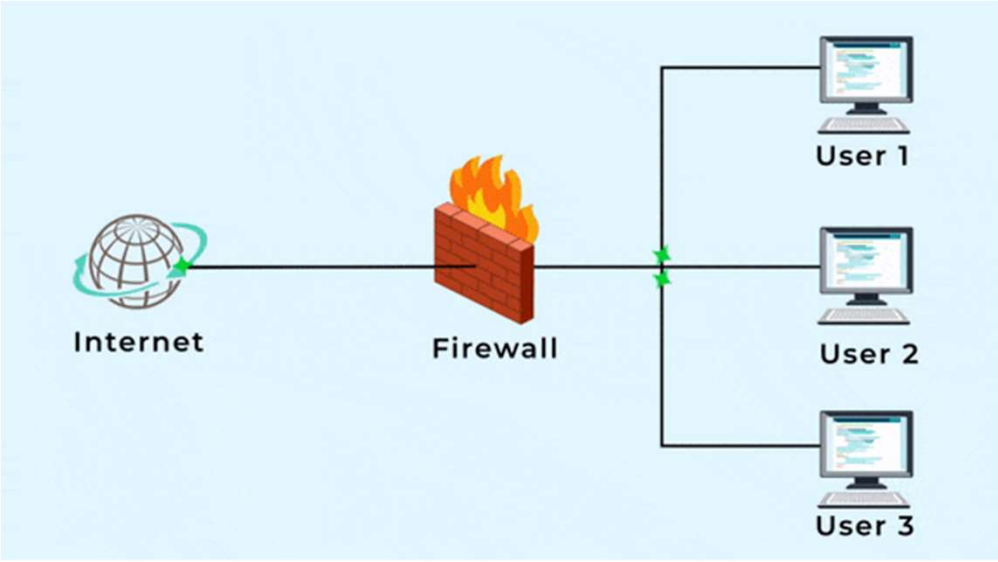
Unit-2

Network Defense Tools

Prof. Kalpesh H Surati
Computer Engineering Department
Darshan Institute of Engineering & Technology, Rajkot
Kalpesh.surati@darshan.ac.in
9925010033

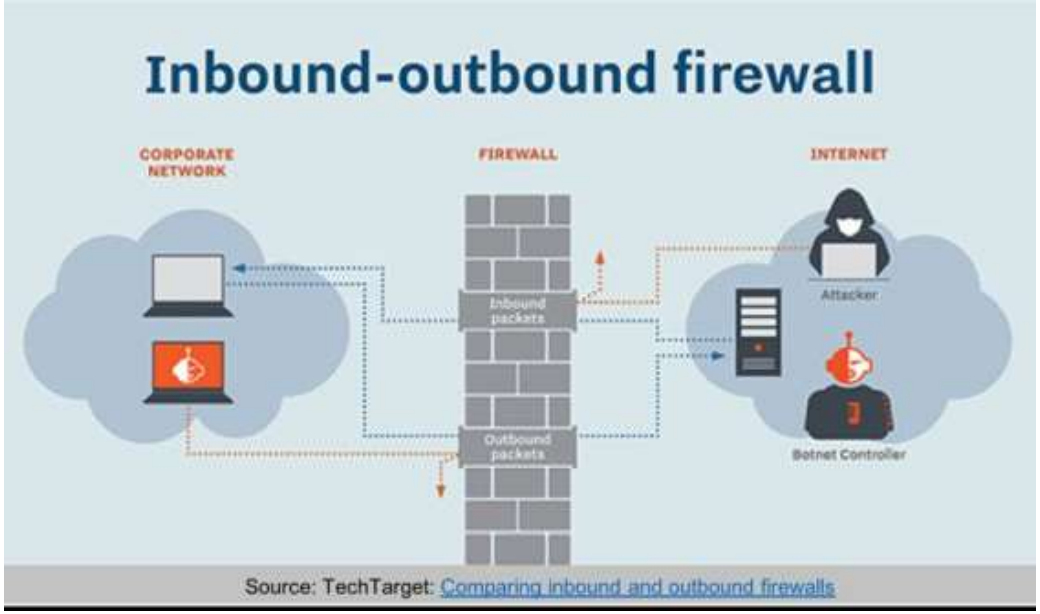
Firewall Basics

- A **firewall** is a device which is used to **control** the **flow of traffic** into and out-of network. In other words, it is a **security device** which **installed between** two networks, **internal network** to **outside network** (more often the internet).
- **Based on** the **rule define** in the firewall **data will be passed** to one network to other network.
- The primary job of a firewall is to **secure the inside network from the internet**.
- Systems on one side of the firewall are protected from systems on the other side.



Firewall Basics

- For example:
  - Consider **LAN** is corporate or our campus network and **WAN** is internet.
  - If we place firewall between the two networks then it will control the flow of the whole traffic and based on rule define into firewall.
  - It will **allow or deny** the traffic.
- Firewalls generally **filter** traffic based on **two methodologies**:
  1. A firewall can **allow any traffic** except what is specified as restricted part. It depends on the type of firewall used, the source, the destination addresses, and the ports.
  2. A firewall can **deny any traffic** that does not meet the specific criteria based on the network layer on which the firewall operates.



Source: TechTarget: Comparing inbound and outbound firewalls

Firewall Types

- Firewall is the first destination for the traffic coming to your internal network.
- So, **anything** which **comes** to your **internal network passes through** the **firewall** and any outgoing traffic will also pass through the firewall before leaving your network completely.
- This is the reason that sometimes this type of firewall filter is also called **screening routers**.
- Firewall types the way a firewall provides greater protection relies on the firewall itself, and on the policies that are configured on it.
- The Following types of firewall are:

1. Packet-Filter Firewall
2. Circuit-Level Gateways
3. Stateful Packet-Inspection (SPI)
4. Proxy Firewall
5. Application Gateways
6. Next-Gen firewalls
7. Software Firewall
8. Hardware Firewall
9. Cloud Firewall

Packet Filtering Firewall

- As the most “basic” and oldest type of firewall architecture,
- **Packet-filtering** firewalls basically **create** a **checkpoint** at a traffic router or switch.
- The firewall performs a simple **check** of the **data packets** coming through the router—inspecting information such as the **destination** and **origination IP address**, **packet type**, **port number**, and other surface-level information **without opening** up the **packet** to inspect its contents.
- If the information **packet doesn’t pass** the **inspection**, it is **dropped**.
- The **good thing** about these firewalls is that they **aren’t very resource-intensive**.
- This means they don’t have a **huge impact** on **system performance** and are **relatively simple**.
- However, they’re also **relatively easy** to **bypass** compared to firewalls with more robust inspection capabilities.

Circuit-Level Gateways

- As another simplistic firewall type that is meant to quickly and easily approve or deny traffic without consuming significant computing resources.
- Circuit-level gateways work by **verifying** the **transmission control protocol** (TCP) **handshake**.
- This TCP handshake check is designed to **make sure** that the session the **packet** is **from legitimate**.
- While **extremely resource-efficient**, these firewalls **does** not **check the packet** itself.
- So, if a **packet held malware**, but had the right TCP handshake, it **would pass** right through.
- This is why circuit-level gateways are **not enough** to **protect** your **business** by themselves.

Stateful Inspection Firewalls

- These firewalls **combine both packet inspection technology** and **TCP handshake** verification to create a level of protection greater than either of the previous two architectures could provide alone.
- However, these firewalls do put **more** of a strain on **computing resources** as well. This may **slow down** the **transfer** of legitimate packets compared to the other solutions.

Proxy Firewalls

- **Proxy** firewalls operate at the **application layer** to **filter incoming traffic** between your network and the traffic source—hence, the name "**application-level gateway**."
- Rather than letting traffic connect directly, the proxy firewall first establishes a connection to the source of the traffic and **inspects** the **incoming data packet**.
- This check is similar to the stateful inspection firewall in that it looks at both the packet and at the TCP handshake protocol.
- However, proxy **firewalls** may also **perform deep-layer packet inspections**, **checking** the **actual contents** of the information packet to **verify** that it contains **no malware**.
- Once the check is complete, and the packet is approved to connect to the destination, the proxy sends it off.
- This creates an extra layer of separation between the "client" (the system where the packet originated) and the individual devices on your network—obscuring them to **create additional anonymity** and **protection** for your network.
- It's that they can create **significant slowdown** because of the extra steps.

Application Level Firewall

- These firewalls operate at the application level.
- In other words, they filter the **traffic only** with regards to the **application** (or **service**) for which they are intended.
- For example, a firewall for monitoring traffic to all the web applications your network uses.

Next-Generation Firewalls

- Many of the **most recently-released** firewall products are being advertised as "**next-generation**" architectures.
- Some common features of next-generation firewall architectures **include deep-packet inspection** (checking the actual contents of the data packet), **TCP handshake checks**, and **surface-level packet inspection**.
- Next-generation firewalls may include other technologies as well, such as **intrusion prevention systems** (**IPSs**) that work to **automatically stop attacks** against your network.
- The issue is that there is no one definition of a next-generation firewall, so it's important to verify what specific capabilities such firewalls have before any conclusion.

Software Firewalls

- **Software firewalls** include any type of firewall that is **installed** on a **local device rather than** a **separate** piece of **hardware**.
- The big benefit of a software firewall is that it's highly useful for creating defense in depth by **isolating individual network endpoints** from one another.
- However, **maintaining** individual software firewalls on different devices can be **difficult** and **time-consuming**.
- Furthermore, not every device on a network may be compatible with a single software firewall, which may mean having to use several different software firewalls to cover every asset.

Hardware Firewalls

- **Hardware firewalls** use a **physical appliance** that acts in a manner similar to a traffic router to **intercept data packets** and **traffic requests** before they're connected to the network's servers.
- Physical appliance-based firewalls like this excel at perimeter security by **making sure malicious traffic** from outside the network is **stopped before** the company's **network endpoints** are **exposed** to risk.
- The actual **capabilities** of a hardware firewall **may vary depending** on the **manufacturer—some** may have a more limited capacity to handle simultaneous connections than others.

Cloud Firewalls

- Whenever a cloud solution is used to deliver a firewall, it can be called a cloud firewall, or **firewall-as-a-service** (**FaaS**).
- **Cloud** firewalls are considered **synonymous** with **proxy** firewalls by many, since a cloud server is often used in a proxy firewall setup.
- The **big benefit** of having cloud-based firewalls is that they are **very easy** to **scale** with your organization. As your needs grow, you can **add additional capacity** to the cloud server to filter larger traffic loads.
- Cloud firewalls, like hardware firewalls, excel at perimeter security.

Firewall vs Packet Filters

- A firewall is a computer connected to both a private (protected) network and a public (unprotected) network, which receives and resubmits specific kinds of network requests on behalf of network clients on either the private or public network.
- **Firewalls involve proxies**. A proxy **acts as** a **middle-man** in a network transaction.
- Rather than allowing a client to speak directly to a server, the proxy server receives the request from the client, and then resubmits the request, on behalf of the client, to the target server.
- Each protocol or type of network transaction typically requires its own proxy program, and an administrator enables or installs specific proxies to determine what kinds of services will be allowed between the two networks.
- **Firewalls are not routers** or address translators.
- The internal network uses private address space. **Neither side of** the **firewall knows** about the **address space on** the **other side** of the firewall, and does not know how to route data to the other side of the firewall.

Firewall vs Packet Filters

- A **packet filter** is a **set of rules**, applied to a stream of data packets, which is used to **decide** whether to **permit** or **deny** the **forwarding** of each **packet**.
- These rules are usually on a router or in the routing layer of a computer's network protocol stack.
- Using a packet filter, an administrator can **dictate what types** of **packets** are **allowed** into or out of a network or computer.
- **Prevents** the **outside network** from having knowledge of the address space on the protected network.
- However, aside from translating the addresses of the internal network, **packets are forwarded as received** through the unit, and **no proxies** are **involved**.
- Any **good firewall** will also **employ packet filtering**.
- This is done to protect the firewall itself from intrusion and to isolate intruders from the internal network.

Packet Characteristic to Filter

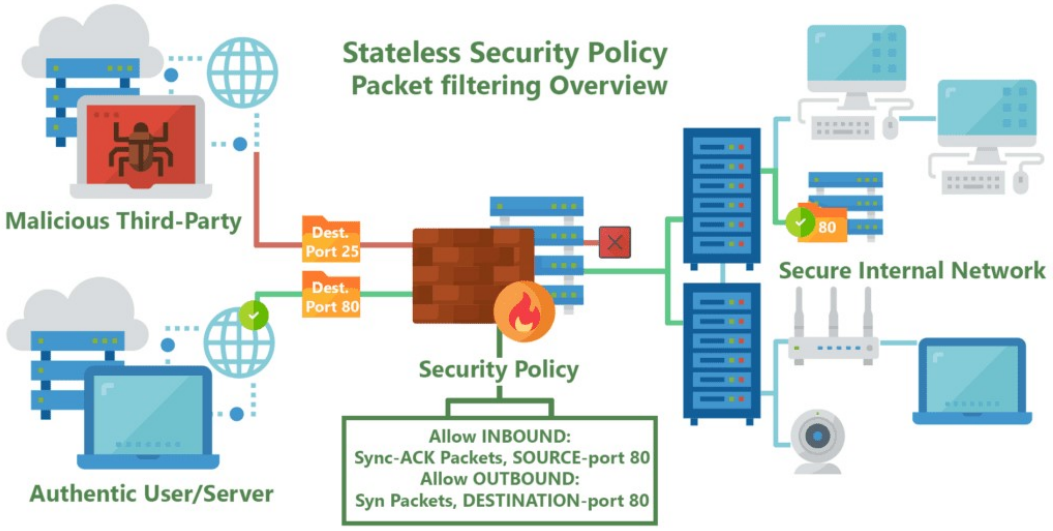
- By using Packet filtering, firewall will create rule and based on rule it will allow or block incoming packet.
- Most firewalls and packet filters have the ability to examine the following characteristics of network traffic:
  - **Type of protocol (IP, TCP, UDP, ICMP, IPsec, etc.)**
  - **Source IP address and port**
  - **Destination IP addresses and port**
  - **ICMP message type**
  - **TCP flags (ACK, FIN, SYN, etc.)**
  - **Network interface on which the packet arrives**

Packet Characteristic to Filter

- For example, if you wanted to **block incoming ping packets** (ICMP echo requests) to your home network of 192.168.1.0/24, you could write something like the following rule.
- The important components of the rule are the action (deny), the packet attributes (ICMP protocol, specifically "ping" types), the direction of the rule (packets "from" one source "to" another), and the type of source (a network address range like 192.168.1.0/24).
  - **deny proto icmp type 8:0 from any to 192.168.1.0/24**
- Other way that is if you wanted to allow incoming web traffic to 192.168.1.50 but deny everything else, you would create two rules. The first one would specify the direction of web traffic to a specific TCP ***port*** on a specific host. The second one would make sure all other traffic is denied. Those rules would
- look like the following:
  - **For allow: allow proto tcp from any to 192.168.1.50:80**
  - **For block: deny proto all from any to 192.168.1.0/24**

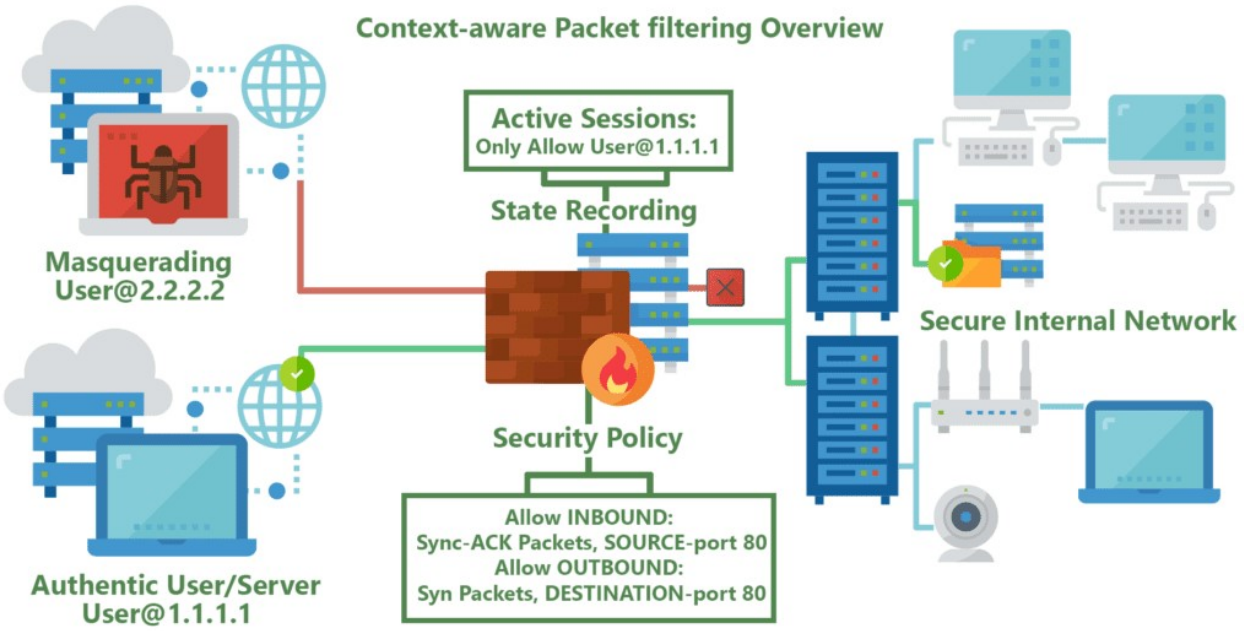
Stateless Firewalls

- If the information about the **passing packets is not remembered** by the firewall, then this type of filtering is called **stateless packet filtering**.
- **These types** of firewalls **are not smart enough** and can be **fooled** very **easily by** the **hackers**.
- These are especially **dangerous for UDP** type of data packets.
- The reason is that, the allow/deny decisions are taken on packet by packet basis and these are not related to the previous allowed/denied packets



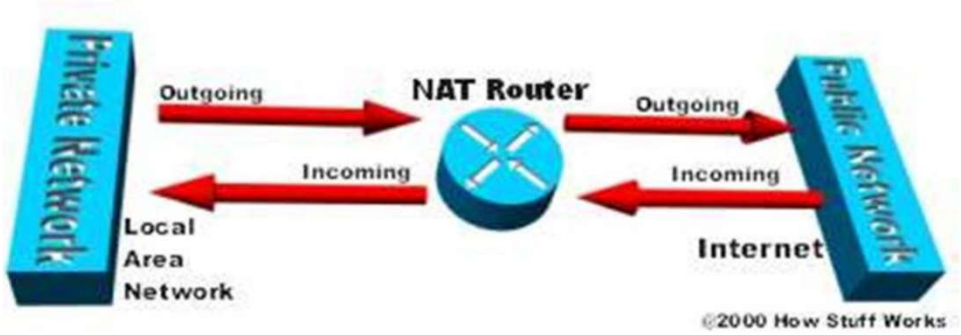
Stateful Firewalls

- If the firewall **remembers** the **information about** the **previously passed packets**, then that type of filtering is **Stateful packet filtering**.
- These can be termed as **smart firewalls**. This type of **filtering** is also **known** as **Dynamic packet filtering**.



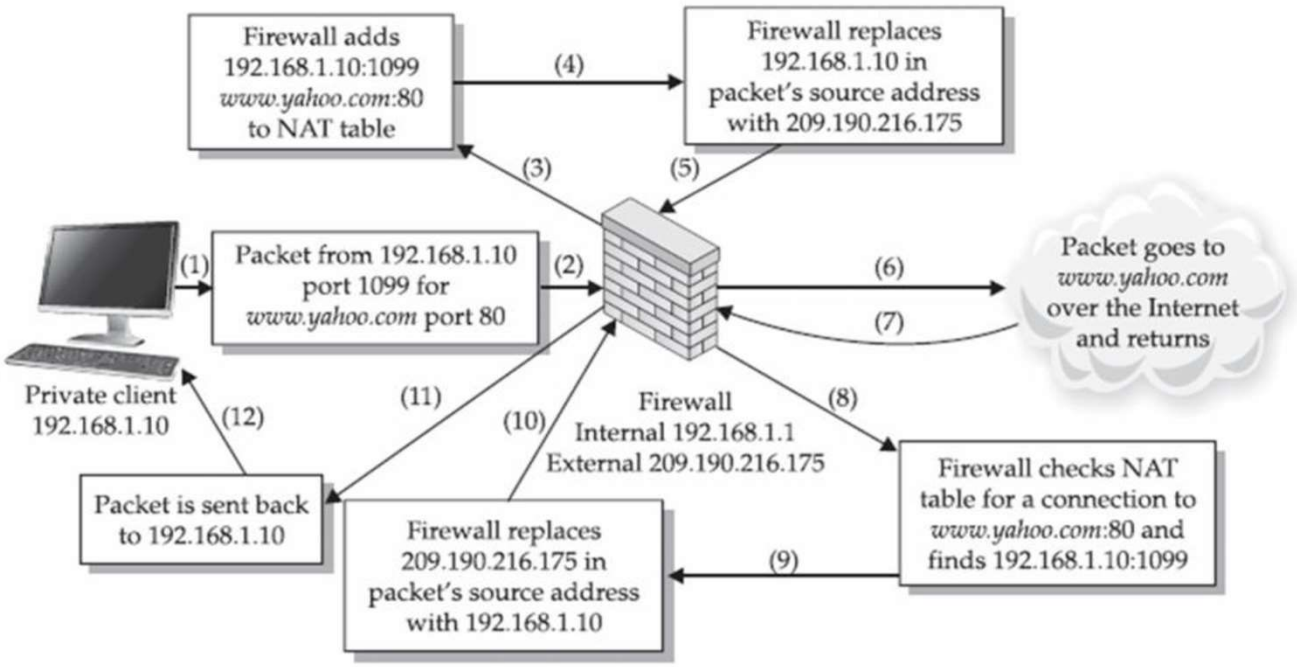
Network Address Translation (NAT)

- Network Address Translation (NAT) is **designed for IP** address **conservation**.
- **Network Address Translation** (NAT) is method of **connecting multiple computers** to the Internet **using one IP address**.
- It enables **private IP networks** that use unregistered IP addresses to **connect to the Internet**.
- **NAT operates on** a **router**, usually connecting two networks together, and **translates** the **private addresses** in the internal network **into legal addresses**, **before** packets are **forwarded to another network**.
- Here in figure we see that NAT router operate between internal networks to Public network. By using NAT router when traffic come from the private network after that NAT router convert private network IP to other IP before transfer packet to another network.



Network Address Translation (NAT)

- Here in below figure, we can easily understand flow of each step one by one.
- Here we see that **Firewall** that work **as NAT device** for IP converting and transfer packet to other network.

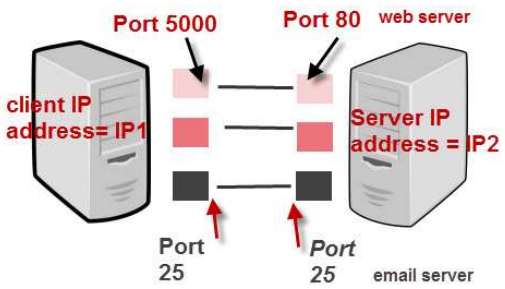


Port Forwarding

- **Port forwarding** or **port mapping** is an application of network address translation (NAT) that redirects a communication request from **one address and port number combination to another** while the packets are crossing a network gateway, such as a router or firewall.
- Port **forwarding allows computers of different network** (Internet) **to connect** to a **specific computer** or **service** within a **private local-area network** (LAN).
- Ports can be "opened" and "closed" in the firewall, which determines which types of traffic are allowed in or out.

TCP/IP Ports and Sockets

- On a TCP/IP network every device must have an IP address.
- The **IP address identifies** the **device** e.g. computer.
- However an IP address alone is **not sufficient for running network applications**, as a computer can run multiple applications and/or services.
- Just as the IP address identifies the computer, The **network port identifies** the **application** or **service** running on the computer.
- The diagram below shows a computer to computer connection and identifies the IP addresses and ports.



IP Address + Port number = Socket

TCP/IP Ports And Sockets

- A **socket** is the **combination** of **IP address** + **port**
- A **connection between** two **computers uses** a **socket**.

Snort : Intrusion Prevention System (IPS)

- Snort is an open source network Intrusion Prevention System (IPS) and Intrusion Detection System (IDS).
- It can perform real time traffic analysis and packet-logging on IP networks.
- Also perform protocol analysis, content searching/matching.
- It can be used to detect a variety of attacks, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more.
- Snort can be configured to run in three modes:
  - **Sniffer mode**, which simply reads the packets off of the network and displays them on the screen.
  - **Packet Logger mode**, which logs the packets to disk.
  - **Network Intrusion Detection System (NIDS) mode**,
    - Performs detection and analysis on network traffic.
    - The program will monitor network traffic and analyze it against a rule set defined by the user.
    - The program will then perform a specific action based on what has been identified.
- With increasing in the growth of internet, it is important task to manage security of network. For this purpose Snort is very useful in term of security.

Cyber Security (CS)
GTU - 3150714

Dedicated Faculty, Committed Education
Darshan
Institute of Engineering & Technology

Unit-3
Web Application Tools

Prof. Maulik D Trivedi
Computer Engineering Department
Darshan Institute of Engineering & Technology, Rajkot
maulik.trivedi@darshan.ac.in
+91-9998265805

Outline

- Scanning for Web Vulnerabilities Tools
  - Nikto
  - W3af
- HTTP Utilities
  - Curl
  - OpenSSL
  - Stunnel
- Application Inspection Tools
  - Zed Attack Proxy
  - SQLmap
  - DVWA
  - Webgoat
- Password Cracking and Brute-Force Tools
  - John the Ripper
  - L0htcrack
  - Pwdump
  - HTC-Hydra

Basic Fundamental Concept of Computer Networks

Section - 1

Scanning for Web Vulnerabilities Tools

- A vulnerability scanner is a computer program designed to assess computer system, network or application for weaknesses.
- A web application security scanner is a program which communicates with a web application in order to identify potential security vulnerabilities. It performs a black-box test.
- Unlike source code scanners, web application scanners don't have access to the source code and therefore detect vulnerabilities by actually performing attacks.
- Web applications are highly popular to give an interactive experience on the Internet for user. Provides not only static web pages but able to create personal accounts, add content, query databases and complete transactions.
- In the process of providing an interactive experience web applications frequently collect, store and use sensitive personal data to deliver their service.
- OpenVAS and Metasploit, which are scanners that check for the presence of known vulnerabilities in web sites in addition to vulns in network devices and operating systems.

Nikto

- Nikto is a Web server scanner that tests web servers for dangerous files, outdated server software and other problems. Also known as a web server assessment tool.
- It preforms generic and server type specific checks.
- It is designed to find various default and insecure files, configurations and programs on any type of web server.
- Nikto is used for assessing the security of a web application's deployment.
- It focuses on identifying vulns in commercial and open source web application frameworks.
- It won't be as helpful for assessing the security of a custom web application.
- For example, it may tell you that a site uses an outdated (and insecure) version of WordPress, but it won't be able to tell you if the blogging application you wrote from scratch is secure or not.

Nikto – Cont.

- Examine a web server to find potential problems and security vulnerabilities, including:
  - Server and software misconfigurations
  - Default files and programs
  - Insecure files and programs

Nikto - Features

- SSL Support(Unix with OpenSSL or maybe Windows with ActiveState's Perl/NetSSL)
- Full HTTP proxy support
- Checks for outdated server components
- Save reports in plain text, XML, HTML, NBE or CSV
- Template engine to easily customize reports
- Scan multiple ports on a server, or multiple servers via input file (including nmap output)
- Easily updated via command line
- Identifies installed software via headers, favicons and files
- Host authentication with Basic and NTLM
- Subdomain guessing
- Scan tuning to include or exclude entire classes of vulnerability checks
- Guess credentials for authorization (including many default id/pw combos)

Nikto - Implemenatation

- Nikto is written in Perl, so it will run on any platform that Perl runs on. Like Windows and any of the Unix-based operating systems.
- Source:
  - https://github.com/sullo/nikto.git
- You shouldn't need to install any Perl libraries that aren't already present in a default installation.
- Scanning:
  - Nikto is uncomplicated, but not unsophisticated.
  - We can use the -host option to start scanning a single target for the presence of default files, pages that might expose sensitive information, or pages with known vulnerabilities.

Nikto - Options

Options	Description
-host	Specifies the target host IP address or name
-port	Specifies an arbitrary port
-output	Logs output to file
-display	Control the output that Nikto shows
-dbcheck	Check the scan database for syntax errors
-format	Save the output file specified with –o (output) option in this format
-nossl	Do not use SSL to connect to the server
--nolookup	Do not perform name lookups on IP addresses

W3af - Web Application Attack and Audit Framework

- w3af is an open-source web application security scanner.
- The project provides a vulnerability scanner and exploitation tool for Web applications.
- It provides information about security vulnerabilities and aids in penetration testing efforts.
- This cross-platform tool is available in all of the popular operating systems such as Microsoft Windows, Linux, Mac OS X, FreeBSD and OpenBSD and is written in the Python programming language.
- Users have the choice between a graphic user interface and a command-line interface.
- We can use w3af to identify more than 200 vulnerabilities and reduce your site's overall ris exposure.
- Identify vulnerabilities like SQL Injection, Cross-Site Scripting, Guessable credentials
- w3af is fully written in Python, and very well documented.
- For Linux user we recommend you download the source from out GitHub repository:
  - https://github.com/andresriancho/w3af.git

W3af - Features

- It has plugins that communicate with each other
- It removes some of the headaches involved in Manual web application testing through its Fuzzy and Manual request generator feature.
- It can also be configured to run as a MITM proxy.
- The requests intercepted can be sent to the request generator and then manual web application testing can be performed using variable parameters.
- It also has features to exploit the vulnerabilities that it finds.

W3af - Implementation

- To open up w3af console, type in the command as shown in the figure below.

```
root@bt:~/w3af# ./w3af_console
w3af>>>
```

Commands	Description
help	List of available commands
keys	To look at the various shortcuts keys available
plugins	Console output change to w3af/plugins.
Help pluginName	To know information about a specific plugins.

- Plugin:
  - Discovery
  - Audit
  - Grep
  - Brute force
  - Output

HTTP Utilities

- The following tools serve as workhorses for making connections over HTTP or HTTPS.
- Alone, they do not find vulnerabilities or secure a system, but their functionality can be put to use to extend the abilities of a web vulnerability scanner, peek into SSL traffic, or encrypt client/server communication to protect it from network sniffers.

Curl

- curl is an open source command line tool and library for transferring data with URL syntax, supporting FILE, FTP, FTPS, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S etc.
- Curl supports SSL certificates, HTTP POST, HTTP PUT, FTP uploading and more.
- It normally displays a progress meter during operations, indicating the amount to transferred data, transfer speeds and estimated time left, etc.
- Curl is used in command lines or scripts to transfer data.
- It is also used in cars, television sets, routers, printers, audio equipment, mobile phones, tablets, set-top boxes, media players, etc.
- Source:
  - http://curl.haxx.se

Implementation

- It is available on Unix, Linux Mac OS X and Windows platforms.
- The curl command is a default tool on most Unix-based systems.
- If it's not present, then it's likely available as a package for your system or you can install it from source.
- To connect to a web site, specify the URL on the command line, like the following example:
  - To retrieve the antihackertoolkit.com homepage
  - Type $ curl http://antihackertoolkit.com

OpenSSL

- OpenSSL is an open-source implementation of the SSL and TLS protocols.
- The OpenSSL library is the most commonly used open source library for establishing encrypted connections.
- The OpenSSL command is present by default on most Unix-based systems. Under Windows, you can use the command as provided by the Cygwin environment or you can build OpenSSL from source.
- The core library, written in the C programming language, implements basic cryptographic.
- SSL establishes confidentiality by preventing view of plaintext traffic and provides integrity by establishing a trusted identity of the web server to prevent intermediation attacks that try to manipulate traffic without being detected.
- The SSL and TLS protocols also establish the identity of a web site.
- This (mostly) prevents an attacker from spoofing web sites or performing intermediation attacks in which a hacker intercepts, modifies, and forwards a victim's traffic without their knowledge.

OpenSSL – Cont.

- It is used for:
  - Creating key for RSA, DSA
  - Creating X.509 certificate
  - Message digest calculation
  - Handling of S/MIME signed
  - SSL / TLS client and server tests
  - Encryption and decryption with ciphers
- Syntax:
  - $ openssl command [command options] [command arguments]
  - Example: $ openssl list-cipher-commands
  - It will give output in the form of algorithm name, key size and blockoption of algorithm.
- Source:
  - https://www.openssl.org

Stunnel

- Stunnel is open source multi platform program, used to provide universal TLS/SSL tunnelling service.
- It can be used to provide secure encrypted connections for clients or servers.
- You can also use stunnel to wrap SSL around any network service.
- OpenSSL is excellent for one-way SSL conversions.
- Unfortunately, you can run into situations in which the client sends out HTTPS connections and cannot be downgraded to HTTP.
- In these cases, you need a tool that can either decrypt SSL or sit between the client and server and watch traffic in clear text.
- Stunnel provides this functionality, Install this tool with your system's package manager or download it from https://www.stunnel.org

Stunnel – Cont.

- It runs on a variety of operating systems, including most Unix-like operating systems and Windows.
- Stunnel relies on a separate library, such as OpenSSL or SSLeay, to implement the underlying TLS or SSL protocol.
- Source:
  - https://www.stunnel.org

Application Inspection tools

- Application Inspection tools which assist with the manual analysis of and interaction with a web application.
- We care much less about whether the application is running on Apache or IIS, or whether the source code is Ruby or Java. Knowing those details informs some of the attacks that we might try against the web application.
- But, we care more about how the web application handles cookie values, or how it responds to different values for a URL parameter, or what kinds of data it accepts from a form submission.
- Tools:
  - Zed Attack Proxy
  - SQLmap
  - DVWA
  - Webgoat

Zed Attack Proxy

- Many web application attacks require a knowledge of HTML and no other tool than a browser's address bar.
- Zed Attack Proxy (ZAP) is example of an interactive proxy.
- An interactive proxy provides the means to inspect, alter, and manipulate web traffic in order to probe a web application for the presence of vulns.
- It is able to passively inspect traffic for security practices.
- ZAP Principles
  - Free, Open source
  - Cross platform
  - Easy to use
  - Easy to install
  - Internationalized
  - Fully documented

Zed Attack Proxy - Installation

- The easiest way to get started with ZAP is to download an installer for your operating system of choice.
- ZAP is written in Java, so your experience in using it doesn't noticeably change between systems. Note that you'll need to set up your environment correctly for building Java source code (e.g., class files).
- ZAP requires a JDK (available from www.java.com) and the ant command.
  - $ svn co https://zaproxy.googlecode.com/svn/trunk zap
  - $ cd zap
  - $ cd build
  - $ ant
  - $ cd zap
  - $ sh zap.sh

SQLmap

- It is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.
- It comes with a powerful detection engine, many niche features for the ultimate penetration:
  - Database fingerprinting
  - Over data fetching from the database
  - To accessing the underlying file system and executing commands on the operating system
- Sqlmap automates the detection and exploitation of SQL injection vulns.
- The following examples demonstrate the basic way that SQL injection vulns occur within a web app and a simple way they can be exploited.
- https://web.site/search?q=tardis+repair
- Source:
  - http://sqlmap.org

SQLmap – Cont.

- **SQLmap can be used for the following:**
  - Scan web apps against SQL injection vulnerability.
  - Exploit SQL injection vulnerability.
  - Extract databases and database user detail entirely.
  - Bypass Web Application Firewall (WAF) by using tamper scripts.
  - Own the underlying operating system.

SQLmap – Cont.

- **Key Features of SQLmap Testing Tool**
- Supports MySQL, Oracle, PostgreSQL, Microsoft Access, Microsoft SQL Server, IBM DB2, SQLite, Firebird, Sybase and SAP MaxDB DBMSs.
- Fully supports six SQL injection procedures:
  - Boolean-based blind
  - error-based
  - UNION query
  - Time-based blind
  - Stacked queries
- Supports cracking password hash formats using a dictionary-based attack.
- Allows enumeration of users, password hashes, privileges, roles, databases, tables an columns.

DVWA - Damn Vulnerable Web App

- It is a PHP/MYSQL web application which is considered as damn vulnerable.
- The main goal of DVWA is to be an aid for security professionals that are to test their skills an their tools in legal environment.
- It helps web developers to proper understand the process of securing its web application an also to teach or even learned by teachers or student for the security in web application that to in class environment.

WebGoat

- WebGoat is a deliberately insecure application that allows interested developers just like you to test vulnerabilities commonly found in Java-based applications that use common and popular open source components.
- The primary goal of the WebGoat project is simple: create an interactive teaching environment for web application security.
- The WebGoatv5 Application provides a testing platform for a typical application security assessment and this testing is black-box testing.
- All of this needs to happen in a safe and legal environment. Even if your intentions are good, we believe you should never attempt to find vulnerabilities without permission.

WebGoat - Installation

- Source:
  - https://github.com/WebGoat/WebGoat
- Unzip WebGoat-OWASP_Standard-x.x.zip to your working directory.
- Change "1.5" on lines 17, 19, and 23 of webgoat.sh to "1.6".
- Since the latest version runs on a privileged port, you will need to start/stop WebGoat & Tomcat:
- On port 80 as root:
  - $ sudo sh webgoat.sh start80
  - $ sudo sh webgoat.sh stop

Password Cracking and Brute-Force Tools

- Password cracking is the process of recovering passwords from data that have been stored.
- A common approach (brute-force attack) is to try guesses repeatedly for the password and check them against correct password.
- Password cracking is an old technique that is successful mostly because humans are not very good random-sequence generators.
- Brute-force guessing techniques against password hashes take advantage of rising hardware performance combined with falling hardware cost.

John the Ripper

- John the Ripper remains one of the fastest, most versatile, and most popular password crackers available
- Currently available for many flavours of Unix, Windows, DOS, BeOS, and OpenVMS.
- Its primary purpose is to detect weak Unix passwords.
- Auto detects password hash types, and includes a customizable cracker.
- It can be run against various encrypted password formats including several crypt password hash types most commonly found on various Unix versions.

John the Ripper - Implementation

- It is compiled on any Unix-based system with make command.
  - $ tar zxvf john-1.7.9-jumbo-7.tar.gz
  - $ cd john-1.7.9-jumbo-7
  - $ cd src
  - $ make
- The make step configures and compiles John for Unix-based system.
- When this step has finished, the binaries and configuration files will be placed in the ./run directory relative to the ./src directory in which you executed the make command.

```
$ ./john –test
Benchmarking: Traditional DES [128/128 BS SSE2-16]... DONE
Many salts: 2041K c/s real, 2041K c/s virtual
Only one salt: 1954K c/s real, 1935K c/s virtual
...
Benchmarking: FreeBSD MD5 [128/128 SSE2 intrinsics 20x]... DONE
Raw: 15780 c/s real, 15780 c/s virtual
Benchmarking: OpenBSD Blowfish (x32) [32/64 X2]... DONE
Raw: 430 c/s real, 462 c/s virtual
...
Benchmarking: LM DES [128/128 BS SSE2-16]... DONE
Raw: 22740K c/s real, 27397K c/s virtual
Benchmarking: dynamic_0: md5($p) (raw-md5) [128/128 SSE2 intrinsics
6x4x5]... DONE
Raw: 9750K c/s real, 10714K c/s virtual
```

L0phtcrack

- It is a Smart tool for Windows password recovery.
- Just like OphCrack tool L0phtCrack is also a Windows passwords recovery tool uses hashes to crack passwords, with extra features of Brute force and dictionary attacks.
- The L0pht hacking group discovered serious weaknesses in the generation of these hashes and released a tool, L0phtcrack.
- It normally gains access to these hashes from directories, network servers, or domain controllers.
- It is capable of doing hash extraction from 32 & 64 bit Windows systems, multiprocessor algorithms, scheduling, and can also perform decoding and monitoring networks.
- It is the easiest to use password auditing and recovery software available.

L0phtCrack - Feature

- It is available for Windows XP, NT, 2000, Server 2003,and Server 2008.
- It can work in both 32- and 64-bit environments.
- Extra feature of schedule routine auditing on daily, weekly, monthly bases.
- After run it provide complete Audit Summary in report page.
- Source:
  - http://www.l0phtcrack.com

Pwdump

- Pwdump is actually different Windows programs that are used to provide LM and NTML hashes of system user accounts.
- Pwdump password cracker is capable of extracting LM, NTLM and LanMan hashes from the target in Windows, in case if Syskey is disabled, software has the ability to extract in this condition.

Screenshot of the Syskey utility on the Windows XP operating system requesting for the user to enter a password

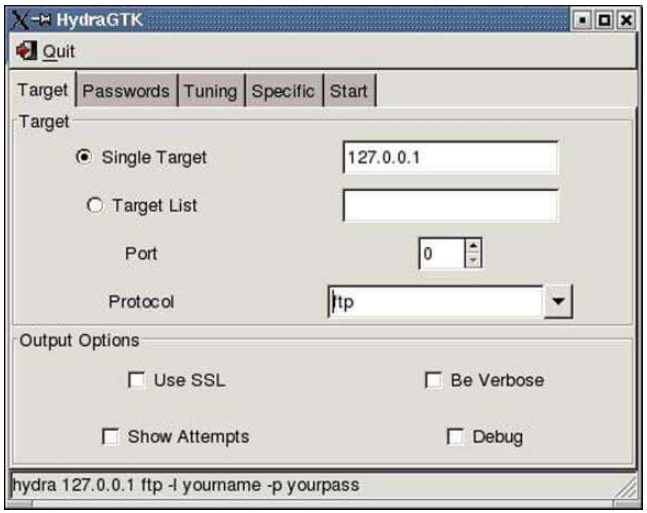
- Software is update with extra feature of password histories display if history is available. Extracted data will be available in form that is compatible with L0phtcrack.
- Recently software is updated to new version called Fgdump as Pwdump not work fine when any antivirus program is running.

Pwdump - Feature

- It is available for Windows XP, 2000.
- A powerful extra feature are available in new version of Pwdump.
- Ability to run multithreaded.
- It can perform cachedump (Crashed credentials dump) and pstgdump (Protected storage dump).
- Source:
  - http://www.darknet.org.uk/

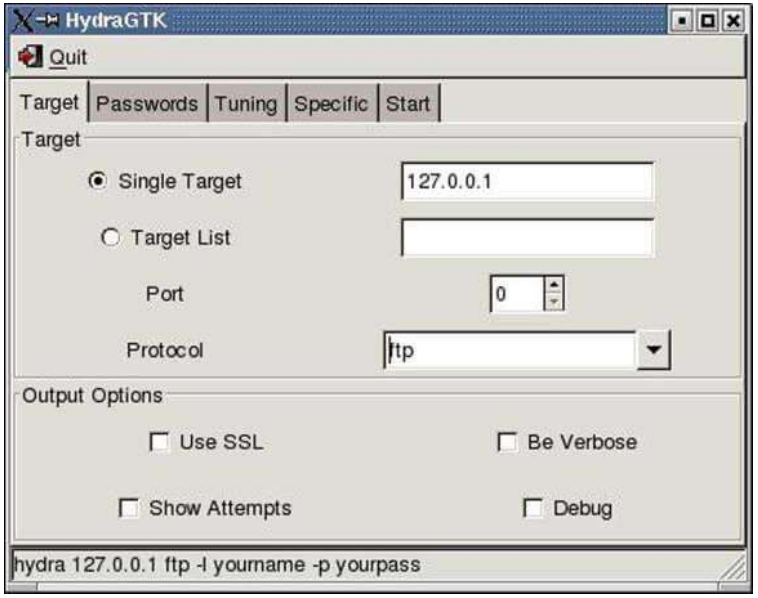
HTC-Hydra

- It is multiple services supportive and network authentication cracker.
- THC Hydra is a supper fast network password cracking tool. It uses network to crack remote systems passwords.
- It can be used to crack passwords of different protocols including HTTPS, HTTP, FTP, SMTP, Cisco, CVS, SQL, SMTP etc.
- It will give you option that you may supply a dictionary file that contains list of possible passwords. It's best when we use it in Linux environment.



THC Hydra - Feature

- Fast cracking speed.
- Available for Windows, Linux ,Solaris and OS X.
- New modules can be added easily to enhance features.
- Supportive with Brute force and dictionary attacks.
- Source:
  - https://www.thc.org/thc-hydra



Cyber Security (CS)
GTU - 3150714

Dedicated Faculty, Committed Education
Darshan
Institute of Engineering & Technology

Thank You

Prof. Maulik D Trivedi
Computer Engineering Department
Darshan Institute of Engineering & Technology, Rajkot
maulik.trivedi@darshan.ac.in
+91-9998265805

Cyber Security (CS)
GTU # 3150714

Dedicated Faculty, Committed Education
Darshan
Institute of Engineering & Technology

Unit-4

Introduction to Cyber Crime and Cyber Law

Prof. Kalpesh H Surati
Computer Engineering Department
Darshan Institute of Engineering & Technology, Rajkot
kalpesh.surati@darshan.ac.in
9925010033

Cyber Crime

- **Cyber-crime** is simply defined as **crimes** that are **directly** or **indirectly related** to **computers**, **mobile**, **network**, **communication** or **storage devices** and using all or any of them.
- A **crime conducted** in which a **computer** was **directly** and **significantly instrumental**.
- Cyber crime in more detail, "**Offences** that are committed **against individuals** or **groups** of individuals with a **criminal motive** to **harm** the **reputation** of the victim or cause **physical** or **mental** or **economical** harm, or **loss** to the victim **directly** or **indirectly**, **using** modern **telecommunication networks** such as **Internet** (networks including but not limited to Chat rooms, emails, notice boards and groups) and **mobile phones** (Bluetooth/SMS/MMS)".

Cyber Law

- **Cyber Law** is a **framework** created to give **legal recognition** to all risks arising out of the usage of computers, computer network or related technology.
- "Cyber Law" is a term used to describe the legal issues related to use of **Computer and Communications Technology**.
- The Indian Parliament passed the Information Technology Bill on 17th May 2000, known as the **ITA 2000**, aimed at providing legal infrastructure for E-Commerce in India.

Cyber Security

- **Cyber Security** means **protecting information**, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.
- Cyber security also refers to the body of technologies, processes, and practices designed to protect computer, networks, communication devices, programs, and data from attack, damage, or unauthorized access
- Effective cyber security reduces the risk of cyber attacks, and protects organizations and individuals from the unauthorized exploitation of systems, networks and technologies

Cyber Crime Classification

- We can categorize Cyber crimes in two ways
  - The **Computer as a Target** :- using a computer to attack other computers. e.g. Hacking, Virus/Worm attacks, DOS attack etc.
  - The **Computer as a Weapon** :- using a computer to commit real world crimes. e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.
- Types of Cybercrime
  1. Cybercrime against individual
  2. Cybercrime against property
  3. Cybercrime against organization
  4. Cybercrime against society
  5. Crimes originating from Usenet newsgroup

Cybercrime against individual

Email Spoofing

- A spoofed email is one in which e-mail header is forged so that mail appears to originate from one source but actually has been sent from another source.
- Email spoofing is the creation of email messages with a forged sender address.

Spamming

- Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.
- In context of “search engine spamming”, spamming is alternation or creation of a document with the intent to deceive an electronic catalog or filing system

Cybercrime against individual

Cyber Defamation

- This occurs when defamation takes place with the help of computers and / or the Internet.
- E.g. someonepublishes defamatory matter about someone on a website or sends emails containing defamatory information.

Harassment & Cyber Stalking

- Cyber Stalking Means following the moves of an individual's activity over internet.
- It can be done with the help of many protocols available such at e- mail, chat rooms, user net groups.

Phishing

- A deception designed link to steal valuable personal data, such as credit card numbers, passwords, account data, or other information.
- Phishing is the fraudulent attempt to obtain sensitive information (such as usernames, passwords, and credit card details) by masking as a trustworthy entity.
- For example : please reset your facebook password www.facebook.com

Cybercrime against property

- **Intellectual Property crimes**
  - These include Software **piracy**, **illegal copying** of programs, **distribution** of copies of software, Copyright violation, **Trademarks** violations, **Theft** of computer **source code**.
- **Credit Card Fraud**
  - An **unauthorized taking** of victim's credit card information for the purpose of purchases from credit card or **transferring funds** from it.
  - Credit card fraud is a form of identity theft
- **Internet Time Theft**
  - The **usage** of the **Internet** hours by an **unauthorized** person which is actually **paid by another person**.

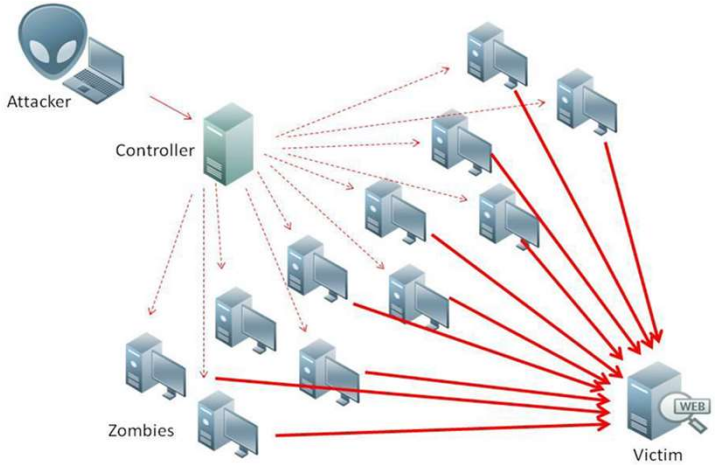
Cybercrime against organization

Unauthorized Accessing of Computer

- **Accessing** the computer/network **without permission** from the owner.
- it can be of 2 forms:
  - **a. Changing/deleting data:** Unauthorized changing of data.
  - **b. Computer observe:** The criminal reads or copies confidential or proprietary information, but the data is neither deleted nor changed.

Denial of Service (DoS) or DDos Attack

- When Internet **server** is **flooded** with **continuous bogus requests** so as to denying legitimate users to use the server or to crash the server.



Cybercrime against organization

- **Computer Virus / Contamination**
  - A computer virus is a computer program that can **infect** other **computer programs** by **modifying** them in such a way as to include a (possibly evolved) copy of it.

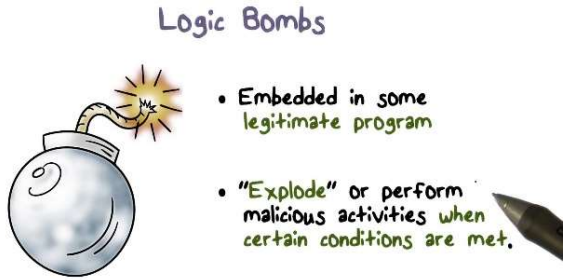
- **Email Bombing**
  - **Sending large numbers** of **mails** to the individual or company or mail servers thereby ultimately resulting into crashing.

- **Salami Attack**
  - When **negligible amounts** are **removed** & accumulated in to something larger. These attacks are used for the commission of **financial crimes**.

Cybercrime against organization

Logic Bomb

- It is an **event dependent** program, as soon as the designated event occurs, it crashes the computer, **release** a **virus** or any other harmful possibilities.

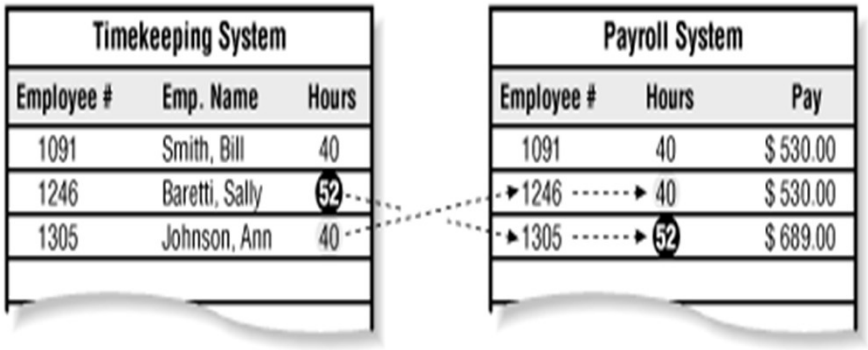


Trojan Horse

- An **unauthorized program** which functions from inside what **seems to be an authorized program**, thereby concealing what it is actually doing.

Data diddling

- This kind of an **attack** involves **altering raw data** just before it is processed by a computer and then changing it back after the processing is completed.



Cybercrime against Society

Forgery

- Currency notes, revenue stamps, mark sheets etc can be **forged using computers** and high quality scanners and printers.

Cyber Terrorism

- Using **computer resources** to **threaten** or force others.

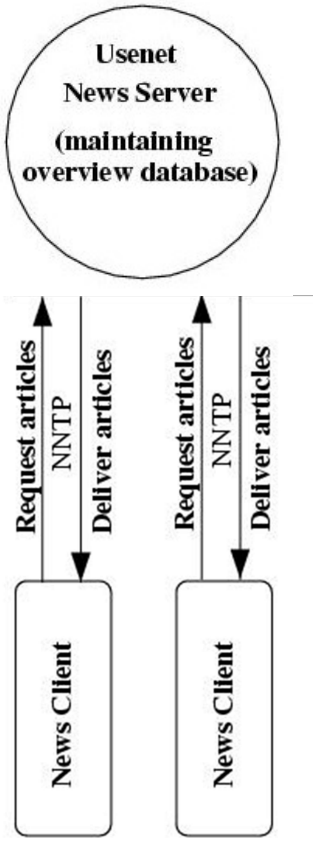
Web Jacking

- Hackers **gain access** and **control** over the **website** of another, even they change the content of website for fulfilling political objective or for money.

Crimes originating from Usenet newsgroup

Usenet

- Usenet is a popular means of **sharing** and **distributing information** on the web with respect to specific subjects or topic.
- Usenet group may carry very offensive, harmful, inaccurate or otherwise **inappropriate material** or **postings** that have been improper or are dishonest in another way.



Following criminal use Usenet

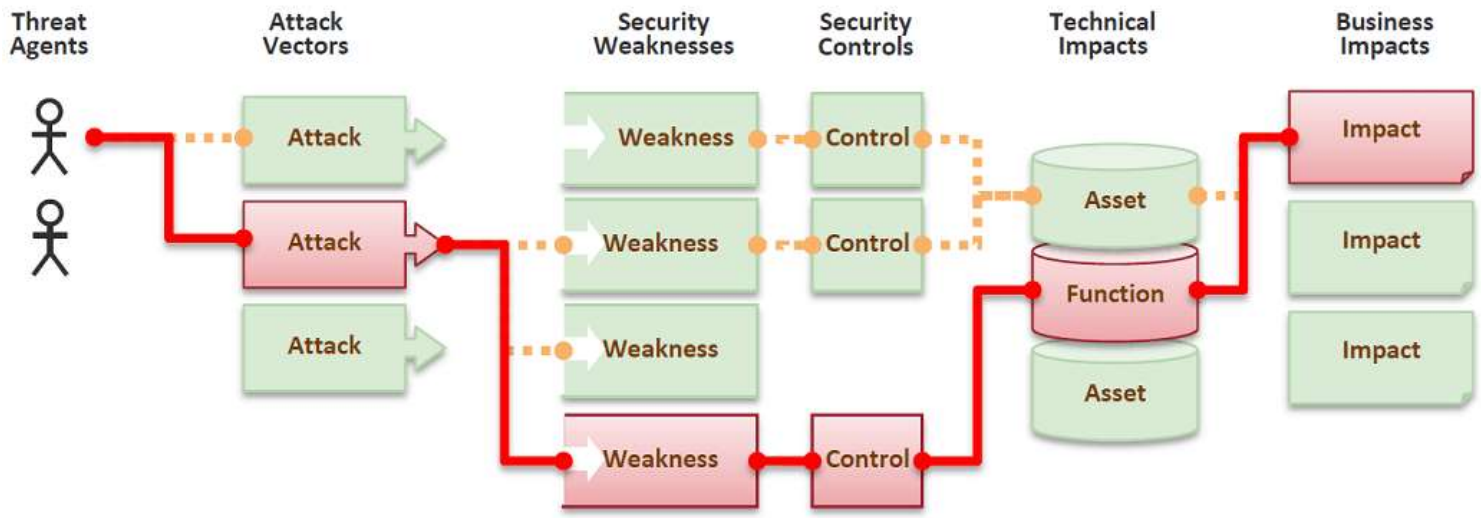
- Distribution/sale of **pirated software** package
- Distribution of **hacking software**
- Distribution/sale of **pornographic material**
- Sale of stolen **credit card number**
- Sale of **stolen data/stolen property**

Hacking

- **Purpose of Hacking**
  - Greed
  - Power
  - Publicity
  - Revenge
  - Adventure
  - Desire to access forbidden information
  - Destructive mindset

- The term **hacker** was originally a term of respect for **computer experts** who knew all about computers, and could do cool things with them
- The person **who** is able to **discover weakness** in a **system** and managed to exploit it to **accomplish** his **goal** referred as a **Hacker**, and the **process is** referred as **Hacking**
- Some hackers crossed over to the **dark side**, and these **villains** were more properly known as "**crackers**"
- A hacker is an **unauthorized user** who attempts tor gains access tan information system

Attack vector



- An **attack vector** is a **path** or means by which a hacker (or cracker) can **gain access** to a computer or network server in order to deliver a payload or **malicious outcome**.
- Attack vectors are **routes** or **methods** used to get into computer systems, usually for **malicious purposes**.
- They take advantage of known **weak spots** to **gain entry**. Many attack vectors take advantage of the **human element** in the system, because that's often the **weakest link**.

Types of Attack Vector

- **Email as an Attack Vector**
  - **Email attacks** continue to advance in sophistication.
  - **Millions** of **messages** can be **sent** out in the hope that a large number of people will be **duped**.
- **Attachments (and other files)**
  - **Malicious attachments** install **malicious** computer **code**. Attachments attempt to install their payload as soon as you open them.
  - The code could be a **Virus**, **Trojan horse** or any other kind of malware.
- **Attack by deception**
  - Deception is aimed at the **user/operator** as the **vulnerable entry point**.
  - It's **not** just malicious **computer code** that you need to watch out for.
- **Viruses**
  - These are **malicious** computer **code** that **makes** them a **payload**.
  - The main attack vector for viruses was originally **infected USB drive**, but now the vectors include **email attachments**, **downloaded files**, worms and more.

Types of Attack Vector

- **Heedless guests (attack by WebPages)**
  - **Fake Web sites** are used extract personal information, like your address, credit card number and expiration date from people.
  - The Fake websites **look** very **much like** the **genuine websites** they imitate.
- **Attacks of the worms**
  - Most worms are delivered **as attachments**
  - These worms **spread without** the need for **humans** to open attachments.
- **Foist ware (sneak ware)**
  - **Foist ware** is a new term for software that **secretly adds hidden components** to your system.
  - **Spyware** is the most common form of foist ware.
  - **It diverts** you to some "**revenue opportunity**" that the foister has going.
- **Malicious macros**
  - Microsoft **Word** and Microsoft **Excel** are some of the examples that **allow macros**.
  - The **macros** can also be used for **malicious purposes**.

Cyberspace and Criminal Behavior

- **Cyberspace** is **worldwide network** of computer networks for **communication** and **exchange** of **data** using **TCP/IP**.
- Cyberspace is most definitely a **place** where you **chat**, **explore**, **research** and **play**.
- The Information or **Digital Revolution** has **created** a new forum for both **terrorist activity** and **criminal behavior**.
- The cybercriminals are categorized based on motive into following groups:
- Cybercriminals- **hungry for recognition**
  - Hobby hackers, IT professionals, Politically motivated hackers, Terrorist organizations
- Cybercriminals- **not interested in recognition**
  - Psychological perverts, Financially motivated hackers, State-sponsored hacking, Organized criminals
- Cybercriminals- **the insiders**
  - Former employees seeking revenge
  - Competing companies using employees to gain economic advantage through damage and/or theft

Criminal Behavior

- The **advent of the computer** has changed the way individuals behave.
- A similar point can be made about **Criminal behavior**; namely, a **significant** amount of **crimes are connected** to **technology**.
- In common fraud scams the **criminals gathers** the **information** by phishing and spoofing leading to identity theft.
- Crimes related to **health care**, **insurances** are also performed by hacking and **forging identities**.
- Cyber **harassment** and **defamation** especially the cases of pedophiles' and **stalkers** use false identities to **trap** the **children** and **teenagers**.
- **spamming** and unsolicited **bulk messages** leads to **lost productivity**.
- The criminal **steals** this **information** from certain **unsecured websites** or by identity theft and doing frauds like **auction frauds**, **non-delivery** of existent/non-existent **merchandize**.
- **Forgery** is often achieved by hacking wherein the hacker attack the target computer and **retrieve personal information** of the victims and use it for their personal **monetary gains**.
- The **Industrial** espionage are achieved through "**spying**".

Clarification of Terms

- **Computer crime**
  - A general term that has been used to denote any **criminal act** which has been **facilitated by computer** use.
  - **Included** both Internet and **non-Internet activity**. Examples include theft of components, forging, digital piracy or copyright infringement, hacking, and child pornography.
- **Computer-related crime**
  - A broad term used to encompass those **criminal activities** in which a **computer** was **peripherally involved**. Examples include traditional bookmaking and theft.
- **Cybercrime**
  - A specific term used to refer to any **criminal activity** which has been committed **through** or facilitated by **the Internet**.
- **Digital-crime**
  - A term used to refer to any **criminal activity** which involves the **unauthorized access**, dissemination, **manipulation**, **destruction**, or **corruption** of electronically **stored data**.

Traditional Problems

- **Criminals** adapt **changing technologies** while **law enforcement agencies** and government institutions, **bounded** by **traditional system**
- The law enforcement agencies are **struggling** to keep up with **criminal innovations**.
- Computer crime has proven and significant challenge to Law Enforcement personnel
- Indeed, the law-enforcement community has often **failed** to **recognize**.
- Many computer-related crime involves non-specialist users (e.g., child pornography, drug dealers, harassment, etc.).

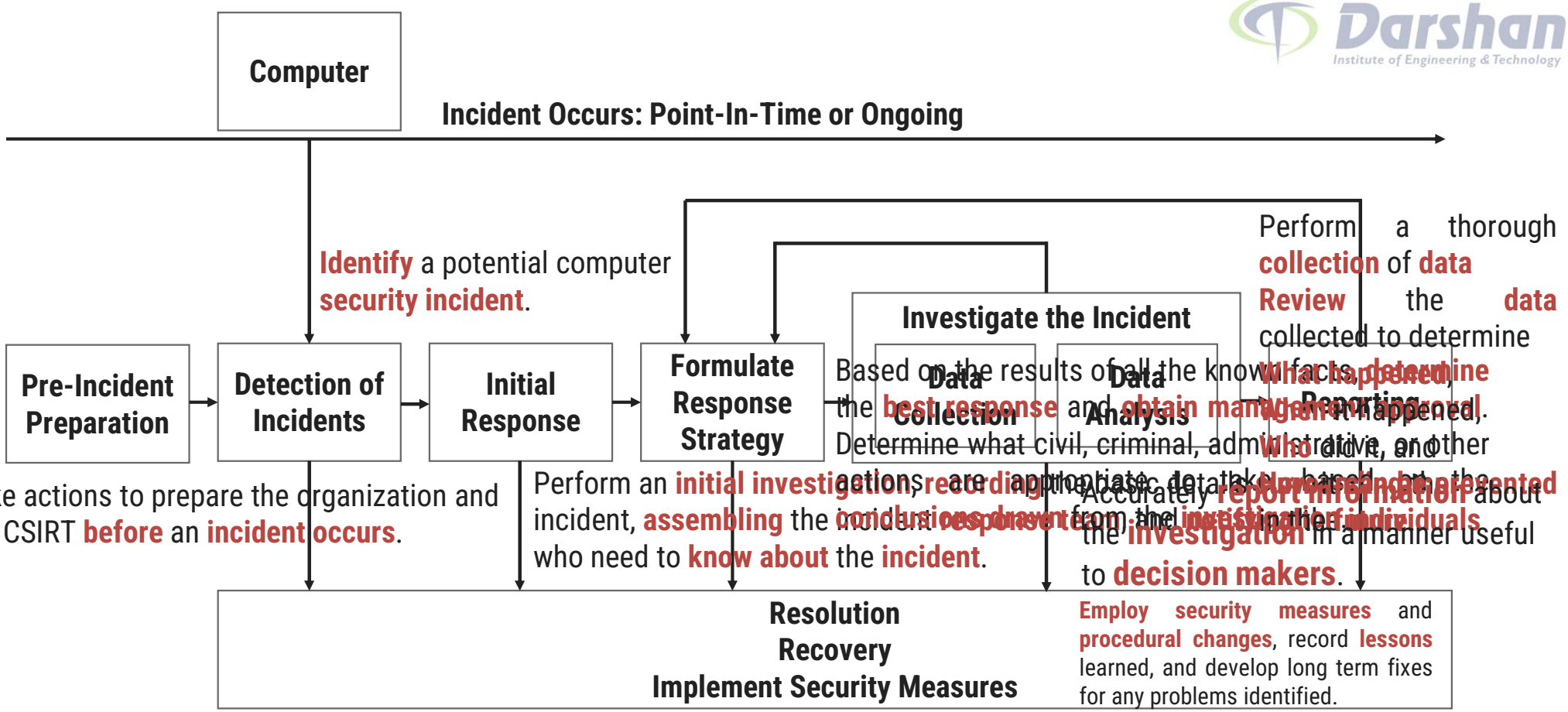
Types of Traditional Problems

1. Physicality and Jurisdictional Concerns
2. Perceived Insignificance, Stereotypes, and Incompetence
3. Prosecutorial Reluctance
4. Lack of Reporting
5. Lack of Resources
6. Jurisprudential Inconsistency

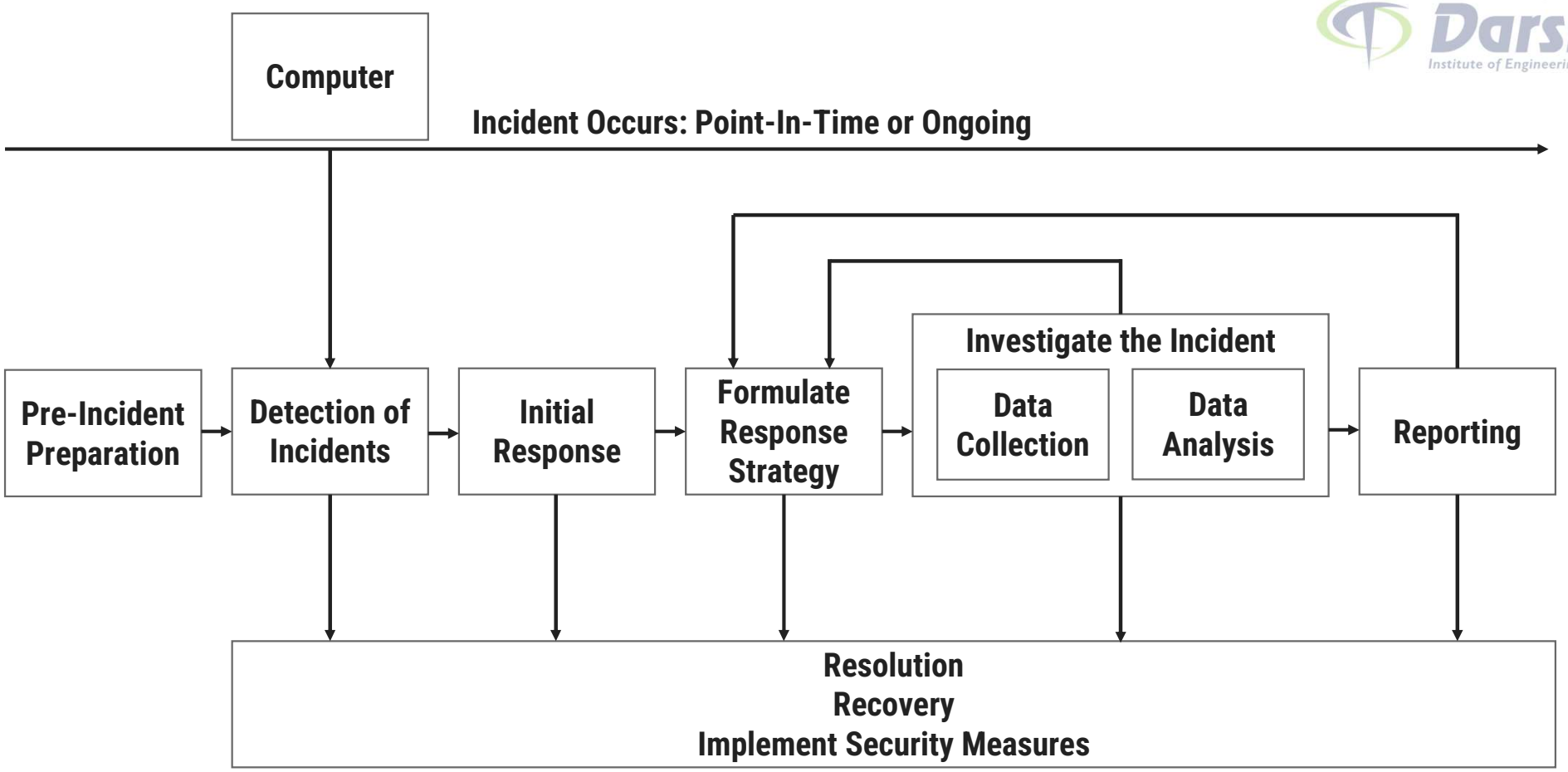
Introduction to Incident Response

- Incident response is the **response to** a **computer crime**, **security policy violation**, or similar event.
- **Digital evidence** is secured, preserved, and **documented** in this phase.
- The **incident responder** is **not necessarily** the **forensic specialist** who will conduct the analysis of the digital evidence.
- In a **large corporate** setting, the incident responder might be a **technician-level employee** in security or information technology.
- In a **smaller company**, the **network administrator** or security officer might also be the incident responder in addition to performing several other duties.
- In the case of a **criminal investigation**, a sworn **law enforcement officer** or "crime lab" technician typically has incident responder **responsibilities**.

Introduction to Incident Response



Introduction to Incident Response



Introduction to Incident Response

- **Pre-incident preparation**
  - Take actions to prepare the organization and the CSIRT **before** an **incident occurs**.
- **Detection of incidents**
  - **Identify** a potential computer **security incident**.
- **Initial response**
  - Perform an **initial investigation**, **recording** the basic details **surrounding** the incident, **assembling** the incident **response team**, and **notifying** the **individuals** who need to **know about** the **incident**.
- **Formulate response strategy**
  - Based on the results of all the known facts, **manage** the **best response** and **get management approval**. Determine what civil, criminal, administrative, or other **actions** are appropriate to **take**, **based on** the **conclusions drawn** from the **investigation**.

Introduction to Incident Response

- **Investigate the incident**
  - Perform a thorough **collection** of **data**
  - **Review** the **data** collected to determine
  - **What happened**,
  - **When** it happened,
  - **Who** did it, and
  - **How** it **can be prevented** in the **future**.
- **Reporting**
  - Accurately **report information** about the **investigation** in a manner useful to **decision makers**.
- **Resolution**
  - **Employ security measures** and **procedural changes**, record **lessons** learned, and develop long term fixes for any problems identified.

Digital Forensics

- **Digital forensics** is a fairly **novel science**.
- Digital forensics is as “the collection of **techniques**, proven **methods** and **tools used** to **find digital evidence** derived **from digital sources** ”.
- Computer forensics generally focuses on particular methods for extracting evidence from a specific platform, whereas digital forensics needs to be formed in such a way that it **covers all types** of **digital devices**, including future digital technologies.
- Regrettably, there is **no regular** or consistent **digital forensic methodology**.
- However there are a number of **procedures and tools based on experiences** of law enforcement, system administrators and hackers.
- Gather evidence by applying approved methods that will reliably extract and **analyze evidence without bias** or **modification** is **challenging task**.

Realms of the Cyber world

- Basically, there are three different levels of networked systems: **intranets**, **internets**, and **the Internet**.
- Intranets are small, local networks connecting computers which are within one organization and which are controlled by a common system administrator.
- internets, on the other hand, connect several networks, and are distinguished in the literature by a lower case (i.e., internet as opposed to Internet).
- These networks are usually located in a small geographic area, and share a common protocol (usually TCP-Transmission Control Protocol/ IP-Internet Protocol).
- The Internet, on the other hand, is the largest network in the world, an international connection of all types and sizes of computer systems and networks. It is a system of small networks of computers linked with other networks via routers and software protocols.

Recognizing and Defining Computer Crime

- It is unclear exactly when and where the first “computer crime” actually occurred.
- Contextually, theft of an abacus or a simple adding machine would constitute a computer crime.
- It is safe to assume that these types of activities occurred long before written or formal documentation was in vogue.
- However, the first documented instance of computer disruption occurred in the **early Nineteenth Century**, when a textile manufacturer named Joseph Jacquard developed what would soon become the **precursor to the computer card**.
- His invention, which allowed **repetitive automation** of a **series of steps** in **the weaving** of special fabrics, was not popular among his workers, who feared for their continued employment. Thus, they dismantled his invention.

Contemporary Crime (Modern Crime)

- **Legislative bodies** have been **slow to respond** to the potentiality of **contemporary** computer **crime** in the Twenty-first Century.
- In fact, the steps made in electronic communications and **point-and-click platforms** have **enabled** a variety of **criminally minded people** to **expand their limits**.
- Actually, promise of **anonymity** has **encouraged criminal activity** among the masses.
- who would never walk into an adult **book store** in **search of photographs** or **videos**, download those same **materials** in the **privacy of their home** from web.
- Instead of **looting bank with** a **gun** criminal **may feel comfortable altering bank records** or manipulating stock records using cyber technology.
- **Revenge through traditional avenues**, may feel completely confident in **posting** embarrassing or **compromising information** on the web.

Contaminants and Destruction of Data

- **Data destruction** is the process of **destroying data** stored on tapes, hard disks and other forms of electronic media so that it is completely unreadable and cannot be accessed or used for unauthorized purposes.
- **Data contamination** The **alteration**, **maliciously** or **accidentally**, **of data** in a computer system.
- **Environment** surrounding of **data storage** area may affect on the stored data. Like environment polluted with **Ferrous metal** particles, **Corrosive gases**, **Chlorides/salts**, **Electrostatic dust**, electricity generation,
- five most commonly experienced culprits of data loss
  1. Power Outage
  2. Virus, Malware, or Attack
  3. Natural Disaster
  4. Human Error
  5. Equipment Failure or Malfunction

Indian IT ACT 2000

- **IT Act: Aim and Objectives**
- The Information Technology Act,2000, is an important law relating to Indian cyber laws. It aims
- at promoting E-Commerce and facilitating E-Governance. The Act strives to achieve the following objectives:
  - To give legal recognition to transactions done by electronic way or by use of the internet.
  - To grant legal recognition to digital signature for accepting any agreement via computer.
  - To provide facility of filling documents online.
  - To authorize any undertaking to store their data in electronic storage.
  - To prevent cyber-crime by imposing high penalty for such crimes and protect privacy of internet users.
  - To give legal recognition for keeping books of account by bankers and other undertaking in electronic form.

Amendments - Indian IT ACT 2008

- **Notable features of the ITAA 2008 are:**
  - Focusing on data privacy
  - Focusing on Information Security
  - Defining cyber café
  - Making digital signature technology neutral
  - Defining reasonable security practices to be followed by corporate
  - Redefining the role of intermediaries
  - Recognizing the role of Indian Computer Emergency Response Team
  - Inclusion of some additional cyber-crimes like child pornography and cyber terrorism
  - Authorizing an Inspector to investigate cyber offences (as against the DSP earlier)

Cyber-Crime Scenarios and Applicability of Legal Sections

- Let us look into some common cyber-crime scenarios which can attract prosecution as per the penalties and offences prescribed in IT Act 2000 (amended via 2008) Act.

1. **Harassment via fake public profile on social networking site**
   - A fake profile of a person is created on a social networking site with the correct address, residential information or contact details but he/she is labeled as 'prostitute' or a person of 'loose character'. This leads to harassment of the victim.
   - **Provisions Applicable**: Sections 66A, 67 of IT Act and Section 509 of the Indian Penal Code.
2. **Online Hate Community**
   - Online hate community is created inciting a religious group to act or pass objectionable remarks against a country, national figures etc.
   - **Provisions Applicable**: Section 66A of IT Act and 153A & 153B of the Indian Penal Code.
3. **Email Account Hacking**
   - If victim's email account is hacked and obscene emails are sent to people in victim's address book.
   - **Provisions Applicable**: Sections 43, 66, 66A, 66C, 67, 67A and 67B of IT Act.

Cyber-Crime Scenarios and Applicability of Legal Sections

4. Credit Card Fraud

- Unsuspecting victims would use infected computers to make online transactions.
- **Provisions Applicable**: Sections 43, 66, 66C, 66D of IT Act and section 420 of the IPC.

5. Web Defacement

- The homepage of a website is replaced with a pornographic or defamatory page. Government sites generally face the wrath of hackers on symbolic days.
- **Provisions Applicable**: Sections 43 and 66 of IT Act and Sections 66F, 67 and 70 of IT Act also apply in some cases.

6. Introducing Viruses, Worms, Backdoors, Rootkits, Trojans, Bugs

- All of the above are some sort of malicious programs which are used to destroy or gain access to some electronic information.
- **Provisions Applicable**: Sections 43, 66, 66A of IT Act and Section 426 of Indian Penal Code.

7. Cyber Terrorism

- Many terrorists are use virtual (GDrive, FTP sites) and physical storage media(USB's, hard drives) for hiding information and records of their illicit business.
- **Provisions Applicable**: Conventional terrorism laws may apply along with Section 69 of IT Act.

Cyber-Crime Scenarios and Applicability of Legal Sections

8. Online sale of illegal Articles

- Where sale of narcotics, drugs weapons and wildlife is facilitated by the Internet.
- **Provisions Applicable**: Generally conventional laws apply in these cases.

9. Cyber Pornography

- Among the largest businesses on Internet. Pornography may not be illegal in many countries, but child pornography is.
- **Provisions Applicable**: Sections 67, 67A and 67B of the IT Act.

10. Phishing and Email Scams

- Phishing involves fraudulently acquiring sensitive information through masquerading a site as a trusted entity. (E.g. Passwords, credit card information).
- **Provisions Applicable**: Section 66, 66A and 66D of IT Act and Section 420 of IPC.

11. Theft of Confidential Information

- Many business organizations store their confidential information in computer systems. This information is targeted by rivals, criminals and disgruntled employees.
- **Provisions Applicable**: Sections 43, 66, 66B of IT Act and Section 426 of Indian Penal Code.

Cyber-Crime Scenarios and Applicability of Legal Sections

12. Source Code Theft

- A Source code generally is the most coveted and important "crown jewel" asset of a company.
- **Provisions applicable**: Sections 43, 66, 66B of IT Act and Section 63 of Copyright Act.

13. Tax Evasion and Money Laundering

- Money launderers and people doing illegal business activities hide their information in virtual as well as physical activities.
- **Provisions Applicable**: Income Tax Act and Prevention of Money Laundering Act. IT Act may apply case-wise.

14. Online Share Trading Fraud

- It has become mandatory for investors to have their demat accounts linked with their online banking accounts which are generally accessed unauthorized, thereby leading to share trading frauds.
- **Provisions Applicable**: Sections 43, 66, 66C, 66D of IT Act and Section 420 of IPC

Cyber Security (CS)
GTU # 3150714

Dedicated Faculty, Committed Education
Darshan
Institute of Engineering & Technology

Unit-5

Attacks and Techniques used in Cyber Crime

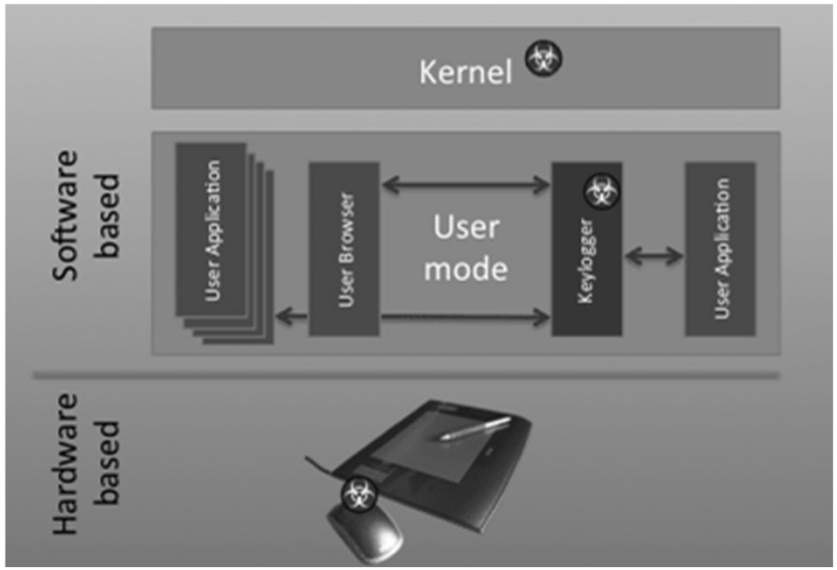
Prof. Kalpesh H Surati
Computer Engineering Department
Darshan Institute of Engineering & Technology, Rajkot
Kalpesh.surati@darshan.ac.in
9925010033

Keyloggers

- Keylogger is a piece of code that logs keystrokes.
- **Keylogger captures the keystrokes** typed on your keyboard and saves these keystrokes in a file, including the details like the usernames and passwords you entered, credit card details, websites you have visited, the applications you opened, and so on.
- The file may stores locally or periodically send it over the network to the owner of the program.
- keylogger is quicker and easier way of capturing and monitoring victims' keyboard activities.

Types of Keyloggers

- It can be classified as **software keyloggers** and **hardware keyloggers**.
- **Software keyloggers** are programs installed in the computer which usually are located between the OS and the keyboard. Or it may at the **kernel level** so receives data directly from the input device
- The software keyloggers are installed on computer system by Trojan or Viruses without the knowledge of the user.
- **Hardware keyloggers** are small hardware devices connected to the PC or keyboard.
- It save every keystork into a file or in the memory of the hardware device.
- To install hardware keylogger, physical access to the computer is required.



Countermeasure of Keyloggers

- **Antikeylogger** is a tool that can detect the keylogger installed on the computer and remove it.
- Never login to your bank account or do some very important work from cyber cafe or someone else computer.
- Use on-screen or virtual keyboard while typing the login credential.
- Use latest anti-virus software and keep them updated.
- AntiViruses do not provide 100% security from keyloggers. An antivirus works on the basis of known signatures, and so if the new keylogger signature is unknown, the antivirus will not report it.

Spyware

- **Spyware** is a type of malware that is installed on computers which collects information about the victim without their knowledge or permission
- It is installed on infected computer and silently sends the collected information to the hackers' computer
- it may seems relatively harmless but it may disturbing your privacy
- Spyware such as keyloggers are installed by the owner of a shared, corporate or public computer on purpose to secretly monitor other users
- It may slow down the victim's computer performance
- **Anti-spyware** gives protection against it

Computer Viruses and Worms

- **Computer Virus and Worms** both are malicious software program that is designed to interfere computer operation or it may damage victim's hardware, software, data or annoyance them.

- Virus needs host program to spread. It can start on **event-driven** or **time-driven** effects or random on both.
- It is **attached** to an **executable** file, which means the virus may exist on your computer but it actually cannot infect your computer unless you run or open the malicious program.
- **Stealth** virus, **self-modified** virus, **polymorphic** and **metamorphic** virus, encryption with variable key virus.

- Worm is **Self-replicating** in nature.
- It can **spread through network** with or without user intervention.
- The biggest danger with a worm is its **capability** to **replicate itself** on your system, so rather than computer sending out a single worm, it **sends out thousands** of **copies**, creating a huge devastating effect.
- **E-mail** worms, **instant messaging** worm, **file-sharing network** worm are types of worms.

Trojan Horse

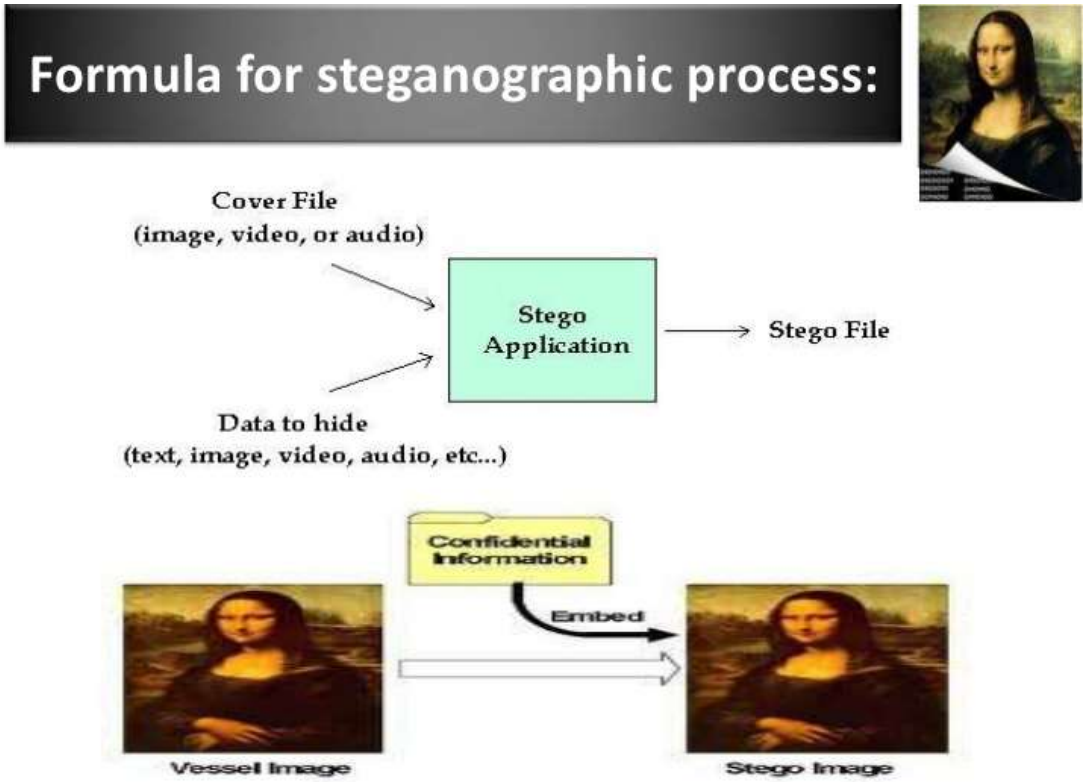
- **Trojan horse** is a harmful code embedded inside a seemingly harmless program.
- The term Trojan Horse comes from the Greek mythology about the Trojan War.
- Unlike viruses and worms, Trojans **do not replicate themselves** but they can be equally destructive.
- The Trojan horse can **create backdoor**.
- Trojan is **designed to spy** on the victims computer, access files or to extract sensitive data.
- It allows remote access to victim's computer, doing malicious activities **without the owner** of the computer.

Backdoor

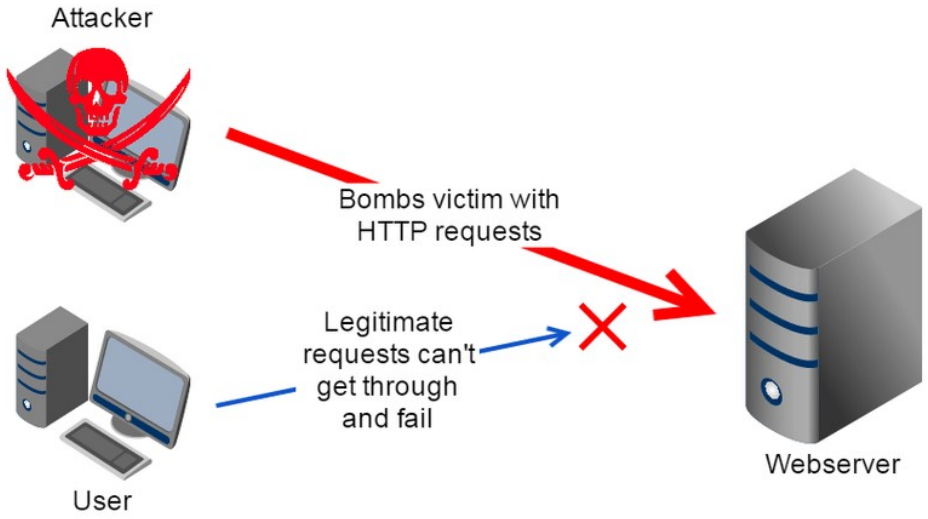
- A **backdoor**, is a **secret entry point** into a program or operating system that allows someone that is aware of the backdoor to gain access without going through the usual security access procedures.
- During the development of operating system or application, programmers **add backdoors** for maintenance hooks and **troubleshooting**. Backdoors allow them to examine operations inside the code while the code is running.
- Backdoor works in background and hides from the user.
- The backdoors are stripped out of the code when it's moved to production.
- When a software manufacturer discovers a hook that hasn't been removed, it releases a maintenance upgrade or patch to close the backdoor.

Steganography

- **Steganography** is the art and science of **writing hidden messages** in such a way that no one can get or knows the existence of the message except the intended user.
- **Steganography** is a **method** that attempts to **hide** the **existence** of message or **communication**.

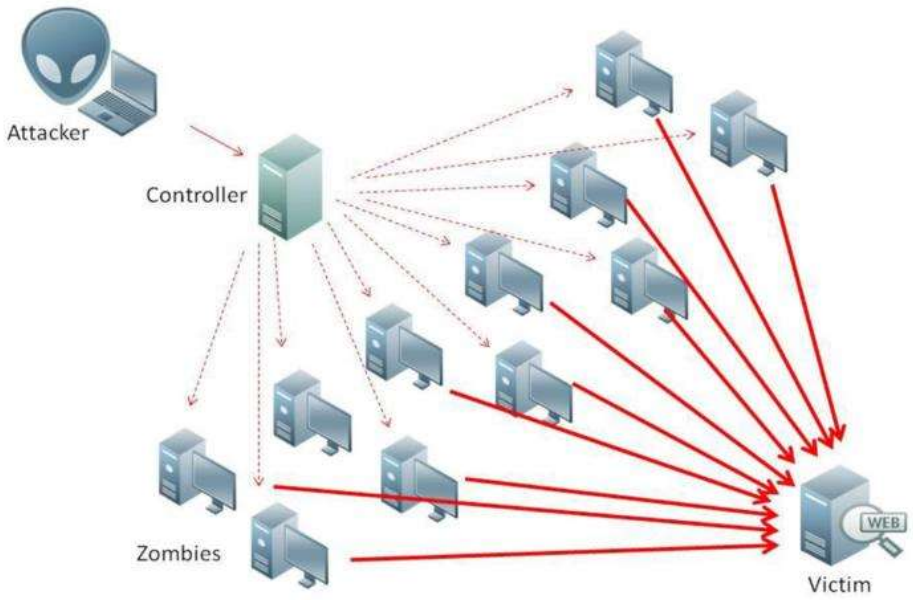


DoS (Denial-of-Service) Attacks



- A **DoS attack** is an attempt to **make computer resources unavailable** and deny to give service to its legitimate users.
- In this attack, the attacker **floods** the **bandwidth** of the victims' **network** by **sending** constant **multiple request** to the victims' server and **make** it **busy** for giving response of the multiple request.
- It is the actual reason for **preventing access** to a service to the **genuine users**.
- DoS attacks often last for days, weeks and even months at a time, making them **extremely destructive to** any **online organization**.
- They can **cause loss of revenues**, consumer **trust**, force businesses to suffer long-term **reputation damage**.

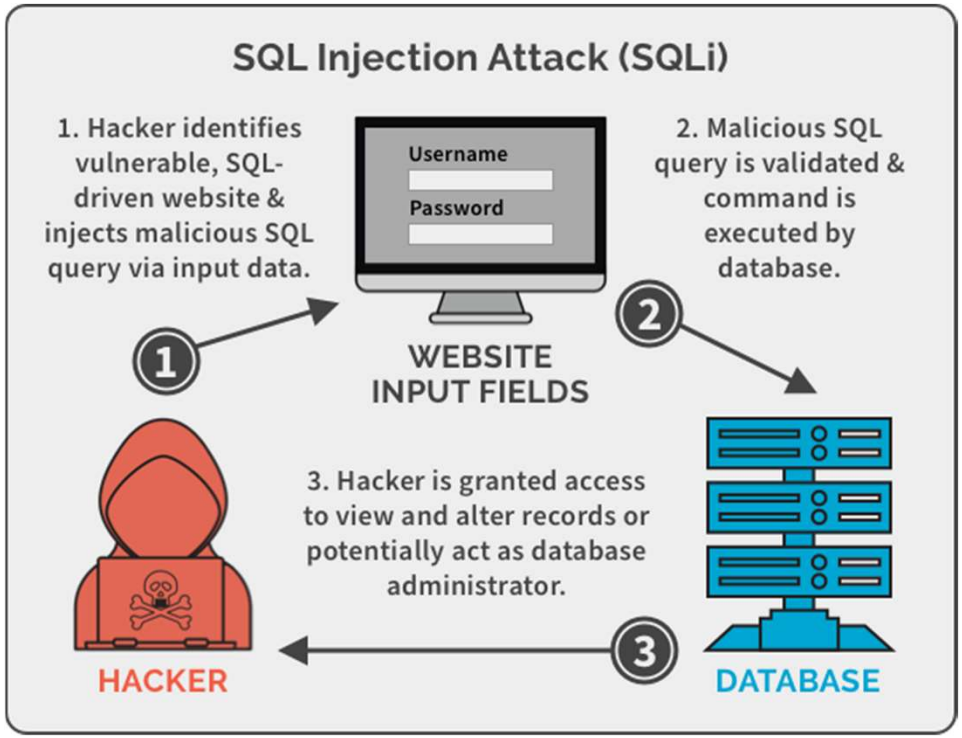
DDoS (Distributed Denial-of-Service) Attacks



- A **DDoS** attack means **Distributed DoS attack**, **DoS attacks from multiple computer** for the same victim is Distributed DoS attack.
- A large numbers of **zombie systems** are **synchronized to attack** a particular system. The zombies are infected by the attackers and it is also victims in the DDoS attack.
- The **zombie** systems are called "**Secondary Victims**" and the **main target** is called "**Primary Victim**".
- **Malware carries** the DDoS attack mechanisms.
- **Botnet** is the **popular medium** to lunch DDoS attack.

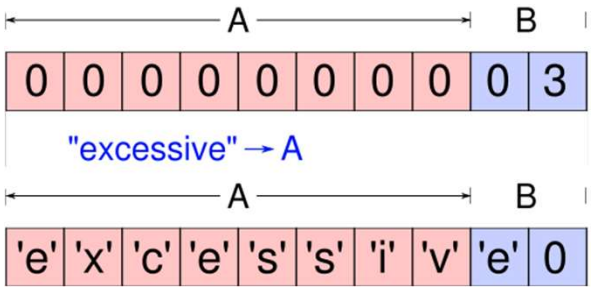
SQL Injection

- SQL injection is a **code injection technique** that **exploits** a **security vulnerability** occurring **in** the **database** layer of an application.
- Using escape character along with single quote **(\') embedded in SQL statement** .
- User input is not strongly typed and thereby unexpectedly executed.
- The main **objective is** to **obtain information** of the victims while **accessing database**.
- **Malicious code** is **inserted** into a web **form field** in the SQL injection



Buffer Overflow

- **Buffers are memory** storage regions that **temporarily hold data** while it is being transferred from one location to another.
- A buffer **overflow** (or buffer overrun) **occurs** when the volume of **data exceeds** the **storage capacity** of the **memory buffer**.
- As a result, the program attempting to write the data to the buffer **overwrites adjacent memory** locations.
- Buffers are created to **contain** a **limited amount** of **data**.
- If data is **more than** the buffer **limit**, it can **overflow into the nearby buffer** and **overwrite** the **valid data** stored in it.
- Buffer overflow is an increasingly common type of **security attack** on **data integrity/reliability**



For example:

```
void main()
{
    char bufferA[50];
    char bufferB[16];

    printf("What is your name?\n");

    gets(bufferA);

    strcpy(bufferB, bufferA);

    return;
}
```

Attack on wireless Networks

- Standard wireless communication occurs when the end user and the wireless access point are able to communication on a point-to-point basis without interruptions.
- There are many **attack** variations in existence **against wireless networks that breaks** the **standard communication** format.

- These attacks includes
  - Denial of Service (DoS) attacks
  - Man-in-the-middle attacks
  - War driving
  - Encryption cracking
  - Spoofing
  - Sniffing

Attack on wireless Networks

Denial of Service (DoS) attacks

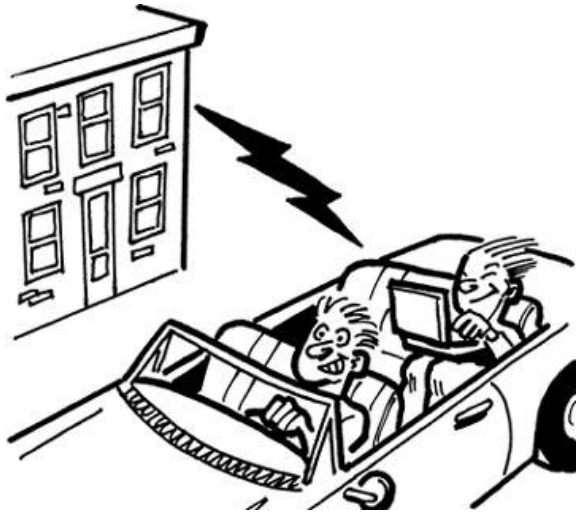
- The objective of a Denial of Service (DoS) attack is to prevent authorized users access to legitimate network resources by denying them service.
- A DoS occurs when the malicious attacker sends an abundant of garbage data to the wireless access point choking all other communications to legitimate users.

Man-in-the-middle attacks

- A man-in-the-middle attack consists of a **malicious** user (**hacker**) **inserting themselves into the data path** between the client and the AP (Access Point).
- In such a position, the malicious attacker can delete, add, or modify data.
- The man-in-the middle attack also enables the malicious attacker **access** to **sensitive information** about legitimate users such as username and passwords, credit card numbers and social security.

Wardriving

- Wardriving is the act of searching for Wi-Fi wireless networks, usually from a moving vehicle, using a laptop or smartphone.
- Wardriving is the **mapping of wireless access points** (WAP) by driving or **walking through populated areas** carrying wireless equipment such as a laptop or a PDA to detect active wireless access points.
- Once the malicious attacker **located vulnerable wireless access points**, they are able to **mount attacks** to other locations under the cover the compromised network.



Steps to Protect Your Wireless Network

Put up a firewall

- A good rule of thumb is to protect your wireless network with a **firewall** to **keep intruders from sniffing your data**.
- While these components often come included within wireless routers, they work best in the form of standalone applications or as a feature of anti-virus software.

Be careful where you roam

- In all honesty, there is **no need to trade stock from** the **Wi-Fi hotspot provided** by the local library. **Wait until** you return to a **trusted network** to conduct such **sensitivity activity**.
- **Disable** your **wireless connection**.

Limit online communications to SSL protected sites

- **SSL** (Secure Sockets Layer) is the **protocol that ensures** the **privacy** of the conversation between you and another party. If you must pay for airline tickets or trade stock from the local café, be sure to **look for** "**HTTPS**" in the URL rather than "HTTP".

Steps to Protect Your Wireless Network

- **Watch out for the Evil Twin**
  - **Malicious** individuals **often create Wi-Fi hotspots** beside legitimate access points. When sitting down to make a connection, you may unknowingly select the evil twin from the list of available access points, giving the malicious individual access to anything you transmit.
- **Encryption**
  - No matter how hard you try, a hacker will eventually try to latch onto your wireless signal. You can **apply** additional **security by implementing encryption protocols** to transform your sensitive data into characters that are only readable by intended receivers.
- **Trust no one**
  - Always keep **your back against the wall** and remain suspicious against all that come encounter with your network. The **enemy could be looking right over your shoulder** seeking usernames and passwords as your fingers tap the keyboard.
- Although **no wireless solution is 100% effective**, taking a few preventive steps will make an intruder's task of breaking into your network much more difficult.