Denial of Service (DOS/DDOS)	A denial of service attack is any attack used to achieve the disruption of any service to legitimate users. DDOS is the 'distributed' form of such an attack where many 'Zombies' that have been taken over by hackers launch simultaneous attacks to achieve a more effective denial of service attack.
Smurf attack	Occurswhen misconfigured network devices allow packets to be sent to all hosts, on aparticular network via the broadcast address of the network.
Ping flood	Occurswhen the target system is overwhelmed with ping packets
SYN flood	Sendsa flood of TCP/SYN packets with forged sender address. causing half -openconnections and saturates available connection capacity of the target machine.

Teardrop attack	Involvessending mangled IP fragments with overlapping, oversized payloads to thelargest machine
Peer to Peer attack	Causesclients of large peer-to-peer file sharing hubs 10 disconnect from their peerto-peer network and to connect to the victim's web s ite instead, As a result,several thousand computers may aggressive ly try to connect to a target website, causing performance degrada tion.
Permanent denial-of-service'(PDoS) attack	(Alsoknown as phlashing)- Damages a system hardware to the exter nal of replacement.
Application-level flood Buffer overflow	Buffer overflow consumes available memory orCPU time,

Brute force attack	Floodsthe target with an overwhelming flux of packets, oversaturating its connectionbandwidth or depleting the target's system resources
Bandwidth-saturating flood attack	Relieson the attacker having higher bandwidth available than the victim2ml[]
Banana attack	Redirectsoutgoing messages from the client backonto the client, preventing outside access, as well as flooding the' clientwith the sent packets
Pulsing zombie	A DoSattack in which a network is subjected 10 hostile pinging by different attackercomputers over an extended lime period. This results in a degraded quality ofservice and increased workload for the network's resources.

Nuke	ADoS attack against computer networks in which fragmented or invalid ICMPpackets are sent to the target. Modified ping utility is used to repeatedlysend corrupt data, thus slowing down the affected computer to a complete stop.
Distributed denial-of-service attack (DDoS)	Occurswhen multiple compromised systems flood the bandwidth or resources of thetargeted system
Reflected attack	Involvessending forged requests to a large number of com pullers that will reply to therequests: The source IP address is spoofed to that of the targeted, victim,causing the replies 16 flood.
Unintentional attack	Website ends up denied, not due to deliberate attack by a single individual, orgroup of individuals, but simply due to a sudden enormous spike in popularity.

Botnets	Comprisea collection of compromised computers (called zombie computers) runningsoftware. Usually installed via worms. Trojan horses or back doors Examples:Denial-of-service (DoS) attacks, adware, spyware and spam
Virus	Viruses-Involvethe insertion of malicious program code into other executable code that canself-replicate and spread from computer to computer, via sharing of removablecomputer media, USB removable devices, transfer· of logic overtelecommunication lines or direct link with an infected machine/code. A viruscan harmlessly display cute messages on computer terminals, dangerously eraseor alter computer files, or simply fill computer memory with junk to a pointwhere the computer can no longer function. An added danger is that a virus maylie dormant or some time until triggered by a certain event or occurrence, suchas a date or being copied a pre-specified number of times, during which timethe virus has Silently been spreading
Worms	Destructiveprograms· that may destroy data or use up tremendous computer and communicationresources, but worms do not replicate like viruses. Such programs do not changeother programs, but can run independently and travel from machine to machineacross network connections by exploiting vulnerability and application/systemweaknesses. Worms also may have portions of themselves running on manydifferent machines.AG2.crl
Spyware/Malware	Similarto viruses. Examples are keystroke loggers and system analyzers that collectpotentially sensitive information, such as credit card numbers, bank details,etc. from the host and then transmit the information to the originator when anonline connection is detected.

Unauthorized Access Through the Internet or World Wide Web	Unauthorizedaccess through the Internet or web-based services. Many Internet softwarepackages contain vulnerabilities that render systems subject to attack.Additionally, many of these systems are large and difficult to configure,resulting in a large percentage of unauthorized access incidents. Examplesinclude: • E-mail forgery (simple mail transfer protocol)• Telnet passwords transmitted in the clear (via path betweenclient and server). • Altering the binding between IP addresses and domain namesto impersonate any type of server. As long as the domain name server (DNS) isvulnerableand used to map universal resource locators (URLs) to sites,there can be no integrity on the Web. • Releasing common gateway interface (CGI) scripts asshareware. CGI scripts often run with privileges that give them completecontrol of a server. • Client-side execution of scripts (via JAVA in JAVA Applets), which pr
Traffic Analysis	Aninference attack technique that studies the communication patterns betweenentities in a system and deduces information. This typically is used whenmessages are encrypted and eavesdropping would not yield meaningful results.Traffic analysis can be performed in the context of military intelligence orcounter-intelligence, and is a concern in computer security
Spam	Also knownas unsolicited commercial e-mail (UCE) or junk e-mail. Usually sent asmass-mailed messages and considered invasive by recipients. • Spamcauses inconveniences and has severe impacts on productivity and thus isconsidered a business risk. • When spamis responded to, the e-mail address or the recipient is validated and givesaway information. • Spam ismanaged using Sender Permitted Form (SPF) protocol and with the help toolssuch as Bayesian filtering and grey listing.
War Dialing	Thepractice of driving around businesses or residential neighborhoods whilescanning with a notebook computer, hacking tool software and sometimes. with aglobal positioning system (GPS) to search for wireless network names. Whiledriving around the vicinity of a wireless network, an attacker might be able tosee the wireless network ' name, but the use of wireless security will determinewhether the attacker can do anything beyond viewing the wireless network name. With wireless security enabled and properly configured, war drivers cannot see the network name and are unable to send data, interpret data sent on the wireless network, access the shared resources of the wireless or wired network (shared files, private web sites), or use the Internet connection. Without wireless security enabled and properly configured, war drivers can send data, interpret data sent on the wireless network, access the shared resources of the wireless or wired network (shared files, private web sites), install viruses, m

War Driving	Similar towar driving, but a vehicle is not used. The potential hacke r walks around thevicinity with a hand held device or a PDA. Curren tly, there are several freehacking tools that lit in these mini devices . The process of using an attack tool to penetrate wireless systems fr om outside the facility where the wireless system sits. A wireless Ethernet card set to work in promiscuous mode is neede d to War drive, and you will also need a powerful antenna if you ar e going to remain at a distances
War Chalking	Thepractice of marking a series of symbols (outward facing crescen ts) on sidewalksand walls to indicate nearby wireless access points. These markings are used toidentify hotspots, where other computer users can connect to the Internetwirelessly and at no cost. War chal king was inspired by the practice ofunemployed migrant workers, d uring the Great Depression in the US, using chalkmarks to indicate which 110mes were friendly.
Salami Attack	Involvesslicing small amounts of money from a computerized trans action or account.Similar to the rounding down technique. The differ ence between the roundingdown technique and the salami techniqu e is that, in rounding down, the programrounds off by the smallest money fraction. For example, in the rounding downtechnique, a US $1 ,235,954.39 transaction may be rounded to US $1 ,235,954.35.O n the other hand, the salami technique truncates the last few digits from thetransaction amount, so US $1 ,235,954.39 becomes US $i , 235,954.30 or $1,235,954.00, depending on the algorithm/formula built into the program. In fact, other variations ofthe same techniqu e are applied to rates and percentages,
Resource Enumeration and Browsing	Whenthe a hacker lists the various resources (names, directories, p rivileges,shares, policies) on targeted hosts and networks Browsing attack-A form of aresource enumeration attack and is performed by a manual search, frequentlyaided with commands and tools availabl e in software, operating systems oradd-on utilities.

Remote Maintenance Tools.	Ifnot securely configured and controlled, can be used as an attack method bymalicious hackers to remotely gain elevated access and cause damage to thetarget systemm
Race Condition	Also knownas Time of Check [TOC] Time of Use [TOU] attacks. Expl oit a small window oftime between the time that the security contro l is applied and the time thatthe service is used. The exposure to a race, condition increases in proportionto the time difference betwee n TOC and TOU. Interference occurs when a deviceor system .atte mpts to perform two or more operations at the same time; but then ature of the device or system requires the operations to happen in propersequence Race conditions occur due to interferences caused by the following conditions: Sequence or non-atomic-These conditio ns are caused by untrusted processes. such as those invoked by an attacker, that may get in between the steps of the secure program. Deadlock, livelock, or locking failure- These conditions are caused b y trusted processes running the same program. Since .these differe nt processes may have the same privileges, they may interfere wit h each other, if not properly controlled. **Careful programming and**
Piggybacking	Theact of following an authorized person through a secured door or electronicallyattaching to an authorized telecommunications link to i ntercept and possiblyalter transmissions. Piggybacking is considere d a physical access exposure.
Phishing	Thecriminally fraudulent process of attempting to acquire sensitive informationsuch as usernames, passwords and credit card details b y masquerading as atrustworthy entity in an electronic communicati on.

Spear Phishing	Apinpoint attack against a subset of people (users of a web site or product,employees of a company. members of an organization) to undermine that companyor organization. Phishing techniquesinclude social engineering. Link manipulation and web site forgery.
Pharming	Anattack that aims to redirect the traffic of a web site lo bogus web site. Pharming can conducted either by changing the host file ona victims computer or by exploit a vulnerability in DNS server software. DNSservers are computers responsible to resolving Internet names into the realaddresses—they are the signposts of the internet, Compromised DN servers aresometimes referred to as “poisoned”. In recent years, both pharming andphishing have been used to steal identity information. Pharming has become amajor concern to businesses hosting e-Commerce and to online banking web sites.Sophisticated measure known as anti-pharming are required to protect againstthis serious threat Antivirus software and spyware removal software cannotprotect against pharming.
Social engineering	Thehuman side of breaking into a computersystem. Organizations with strong technical security computer measures (such asauthentication processes firewalls and encryption) may still fail to protectthier information systems. This situation may happen if an employee unknowinglygives away confidential information (e.g., passwords and IP addresses) byanswering questions over the phone with someone they do not knower replying toan email message from an unknown person. Some examples of social engineeringinclude impersonation through a telephone call, dumpster diving and shouldersurfing. The best means at defense for social engineering is an ongoingsecurity awareness program. wherein all employees and third parties (who haveaccess to the organization’s facilities) ale educated about the risks involvedin falling prey to social engineering attacks.Ri4 9
Network Analysis	Anintruder applies a systematic and methodical approach known as foot-printing tocreate a complete profile of an organization's network security infrastructure.During this initial reconnaissance phase. the intruder uses a combination oftools and techniques to build a repository of information about a particularcompany's internal network. This probably would include information aboutsystem aliases, functions, internal addresses, and potential gateways andfirewalls. Next. the intruder focuses on systems within the targeted address space thatresponded to these network queries. Once a system has been targeted; theintruder scans the system's ports to determine what services and operatingsystem are running on the targeted system, possibly revealing vulnerableservices that could be exploited

Message Modification	Involvesthe capturing of a message and making unauthorized changes or deletions (offull streams or parts of the message) changing the sequence or delayingtransmission of captured messages. This attack can have disastrous effects if.for example, the message is an instruction to a bank to make a Payment.
Masquerading	Anactive attack in which the intruder presents an identity other than theoriginal identity. The purpose is to gain access to sensitive data orcomputing/network resources to which access is not allowed under the originalidentity. Masquerading also attacks the authentication attribute by letting agenuine session authentication take place and subsequently enters theinformation flow, masquerading as one of the authenticated users of thesession. **Since a masquerading attack is anattempt to gain access to a computer system by posing as an authorized user. Amore effective approach is where" The system informs the user about theirlast-time login information (date and time accessed). This will alert the userif their account has been compromised.**
Impersonation	Impersonation both by people and machines fallsunder this category. Masquerading by machines (also known as IP spoofing)-Aforged IP address is presented. This form of attack is often used as a means ofbreaking a firewall. Forgery is one of the ways impersonation is achieved.Forgery is attempting to guess or otherwise fabricate evidence that theimpersonator knows or possesses the authenticating information (the secret).
Packet replay	Packet replayisone of the most common security threats to network systems, similar toimpersonation and eavesdropping. Packet replay refers to the recording andretransmission of message packets in the network and is not consideredimpersonatione

Wiretapping and sniffing	Wiretapping and sniffing are ways to gather information needed to impersonate, but are not impersonation attacks by themselves.
Alteration attack	Occurswhen unauthorized modifications affect the integrity of the data or code
Back Door	Any opening left in a functional piece of software that allows 'unknown' entry into the system / or application without the owners knowledge. Many times, back doors are left in by the software creators.
Spoofing	Spoofing is a technique used to gain unauthorized access to computers. A hacker must first find an IP address of a trusted host. Once this information is gotten, then the hacker can use this information to make the recipient think that the hacker is the trusted sender.

Man in the Middle#1	Theattacker actively establishes a connection to two devices. The attacker connects to both devices and pretends to eachof them to be the other device. Should the attacker's 'device be required to authenticate itself to one of the devices, itpasses the authentication request to the other device t and then sends theresponse back to the first device. Having authenticated himself/herself in thisway, the attacker can then interact with the device as he/she wishes. Tosuccessfully execute this attack, both devices have to be connectable.
Man in the Middle#2	The attacker interferes while the devices are establishing aconnection. During this process, the devices have to synchronize the hopsequence that is to be used. The aggressor can prevent this synchronization sothat both devices use the same sequence but a different offset within thesequence. A Man in the Middle attack is when an attacker is able to intercept traffic by placing themselves in the middle of the conversation. Man in the Middle attacks involve a malicious attacker intercepting communications and fooling both parties into believing they are communicating with each other when they are really being watched. The attacker can then do anything to the transmission they are now apart of to include eavesdropping or planting information. Wireless systems are very susceptible to this form of attack.
Trojan horses (often called Trojans)	Programsthat are disguised as useful programssuch as operating system patches, software packages or games. Once executed,however. Trojans perform actions that the user did not intend, such as openingcertain ports for subsequent access by the intruder.
Trap doors	Commonlycalled back doors. Bits of code embedded in programs by programmers to quicklygain access during the testing or debugging phase an unscrupulous programmerpurposely leaves in this code (or simply forgets to remove it), a potentialsecurity hole is introduced. Hackers often plant a back door on previouslycompromised systems to gain subsequent access. Threat Vector Analysis (a typeof defense-in-depth architecture), separation of duties and code audits help todefend against logic bombs and trap/back doors.

Logic bomb	Aprogram or a section of a program that is triggered when a certain condition,time or event occurs. Logic bombs typically result in sabotage of computersystems and are commonly deployed by disgruntled insiders who have access toprograms. For example, when terminated from an organization, a disgruntledsoftware programmer could devise a logical bomb to delete critical files ordatabases. Logic bombs can also be used against attackers. Administratorssometimes intentionally install pseudo flaws, also called honey tokens, thatlook vulnerable to attack but really act as alarms or triggers of automaticactions when the intruder attempts to exploit the flaw.& .+qC
Interrupt Attack	Occurswhen a malicious action is performed by invoking the operating system toexecute a particular system call. Example: A boot sector virus typically issuesan interrupt to execute a write to the boot sector.
Flooding	Adenial of service (DoS) attack that brings down a network or service byflooding it with large amounts of traffic. The host's memory buffer is filledby flooding it with connections that cannot be completed.
E-mail Bombing and Spamming	Characterizedby abusers repeatedly sending an identical e-mail message to a particularaddress. E-mail spamming is a variant ofbombing and refers to sending e-mail to hundreds or thousands 01 users (or tolists that expand to that many users). E-mail spamming can be made worse ifrecipients reply to the message, causing all of the original addressee toreceive the reply. It may also occur innocently as a results of sending amessage to mailing lists and not realizing that the list explodes to thousandsof users or as a result of using a responder message, such as a vacation alert,that is not set up correctly. May be combined with e-mail spooling, whichalters the identity of the account sending the message making if more difficultto determine from whom the e-mail is coming.