Security objective this introduction is aimed at imparting a basic understanding of what information security is all about and covers a broad spectrum of topics in the information security arena outcome at the end of this chapter you will have a clear understanding of concepts related to information security.

She security using the second word alone for now first we need to ask what information is information is nothing but processed data sounds too technical what is data then data is simply a collection of facts or values which may exist in different forms as numbers or text on pieces of paper as bits and bytes stored in electronic memory or just as facts in a person's mind now getting back on track what is information data when arranged in a convenient form for a specific purpose is known as information suppose it's in another way information maybe credit card numbers debit card numbers pin numbers Gmail passwords Facebook passwords rates of passwords and bank account pin numbers and so on an organized set of data is called information.

Peter can be classified as publicly available data confidential data and restricted or private data when data is publicly available to all it is known as publicly available data example A banks balance sheets and insurance policy details a government tender notices and job posts held by authorities when data is available only to the people involved in a process or an organization in other words it is restricted from unauthorized access it is called confidential data example a manufacturing companies market forecast data test cases and standards a banks customer data consisting of the addresses and phone numbers or government sensitive scientific and medical research data when the data is super sensitive in other words leakage mainly to serious issues it is known as restricted or private data example a company system designs and trade secrets financial account pin numbers and email password personal reports or medical reports of a person having seen the different types of data sets that are nothing but information what is the need for information security what if a credit card pin becomes available for everyone what if the number of missiles held by a nation is known worldwide what if the system design and test case for a new product of a company it's accessible by their competitors and what if a tender quotation of all the applicants is accessible by all the other applicants do you think it is good to go about without securing this information of course not let us now get into information.

security is information security information security is the means of defending information or data stored either physically or electronically from being accessed by unauthorized personnel during World War Two no one knew that EU S had nuclear weapons the then president of the USA Franklin D Roosevelt approved of the Manhattan Project that paved the way for the creation of the little boy and Feldman in 1939 itself six years from then after the demise of Roosevelt when Harry S Truman took over as president in 1945 he approved the dropping of the bombs in the Japanese cities if the Japanese or the rest of the world are known about this earlier they would have started developing their own nuclear weapons the information was kept secret but now overtime this information is available to all information gets dissipated overtime it is all about how it is being guarded at the moment information is not secured enough it becomes available to everyone this weakness or gap in the system which may allow an intruder to gain access to the information system is known as vulnerability when an intruder is able to use this vulnerability to arrive at sensitive data in the system it is termed as an exploit it has

always been a tug of war between the terms vulnerability and threat what is a threat and how does it differ from vulnerability threat is a factor that can cause harm to a system and the system has no control over it but a vulnerability is a flaw in the system itself which can definitely be treated when explain like this what are the possible threats.

Broadly into two types environmental threats and man-made threats environmental threats environmental threats can be caused due to environmental conditions or natural disasters in terms of extreme temperatures humidity power failures heavy downpour causing floods etc the environmental conditions pose a great threat to the information system in one way or the other apart from this natural disasters like earthquakes floods tornadoes or landslides pose a threat to an information system man made threats human errors and weaknesses make up most of the men made threats and employee is the greatest asset as well as the most dangerous possible threats to an organization the first category of man-made threats are caused by the employees this is also known as an insider threat this may be unintentional as well as intentional an employee may unknowingly leave his PC unlocked while going for a break which would pave the way for another disgruntled employee of the same organization to gain access to the system and steal data from the system the former is an unintentional threat while the latter falls under intentional threat the second category of man-made threats are caused intentionally by people outside the organization also called external human threats a member outside the organization attacking the information system with a malicious intent is called a hacker intentional threats are caused by individuals with motivations that can be categorized as political economic and sociocultural political motivations are aimed at destroying or taking control of the target system posting irrelevance and controversial political statements the people carrying out such activities are called hacktivists example cyber terrorism economic motivations are aimed at earning money by stealing intellectual data and selling it to the organization's competitors also called cyber espionage installing ransomware like cryptolocker and encrypting the data on a target's machine and blackmailing the target to pay a ransom in order to get the decryption Kate personal motivations are aimed at satisfying the self out of a sense of curiosity or a desire to get publicity by causing psychological damage to the target via social networking sites this is also called cyber stalking.

A hacker intentionally exploiting a vulnerability in a system with authorization but without a malicious intent is known as a white hat hacker these are actual security guys deployed as security admins a hacker who intentionally attacks a system with a malicious intent is called a Black Hat hacker or a cracker apart from these two types of hackers there are Gray hat hackers who exhibit the traits from both the white and black hats for example if a white hat hacker found a vulnerability in his system and exploited it with authorization but revealed it publicly instead of reporting it to the organization who had authorized him he would be exhibiting a trait of a Black Hat hacker so then he would be called a Gray hat hacker when an amateur hacker breaks into systems using pre packaged automated scripts tools and software written by real hackers he is called a script kiddie.

Curity breach occurs when sensitive or confidential data is leaked stolen or destroyed by an unauthorized individual a hacker this security breach can be avoided in general by concentrating on the elements of information security what are the elements of information security let us take this scenario of an online purchase of a T shirt usually one logs into the shopping website and adds it to the cart for purchase when it comes to the payment part the control is transferred to a third party application that connects to the bank what if an attacker is able to sniff your bank account password at this point the confidentiality of the data is lost here which is the first element of information security let's say you have placed your order and paid for it but in the bill you find the delivery address to be a different 10 what happened and it's hacker pushing himself between you and the server has tampered with the data and made the delivery address data point to his own address the integrity of the data is lost here which is the second element of information security if an attacker is not able to fiddle with the first two elements of information security they execute attacks like denial of service that would bring down the server making the website unavailable to legitimate users the availability of the data is lost here which forms the third elements of information security these three elements form the CIA triad apart from these elements of the information security system there were two more concepts that security relies on they are authentication and non repudiation in the very same example of the online purchase the authentication of a trusted user can be ensured by issuing an OTP to the user's mobile number it ensures the conformity of a trusted source non repudiation is a byproduct of authentication which ensures that the data is sent to and fro between the communicating parties originated only from the parties involved in the communication.

To ensure the security of its information conducts a security audit that involves calculating the risk factors what is a risk risk is nothing but the possibility of losing a valuable asset to identify the loopholes or danger in an information security asset risk assessment involves classifying the risks into two categories namely inherent risks and residual risks inherent risk this is the risk that is faced when no controls or other mitigating factors are in place to guard the information for example in an organization the lack of physical security measures such as CCTV door access control mechanisms etc poses a higher risk of vital information theft residual risk the risk that remains after the implementation of all control measures for example an organization can control the physical access to its premises either by having a security guard or by using electronic access control when the organization seems to have nothing to be guarded physically there is no need for it to protect its premises with either of the securing methodologies this is where the organization conducts a cost benefit analysis of its assets against its safety measures irrespective of the results of the cost benefit analysis there are certain standards and compliance is an organization is supposed to follow these include ISO international organization for standardization 27,001 and 27,002 ITIL information technology infrastructure cobit control objectives for information and related technology PCI SSC payment card industry security standards council and PCI DSS payment card industry data security standard having seen what information security is and how information security is ensured by following standard practices it's time to get to know how the attackers are able to get into the system.

In an information system to gain unauthorized access of data is called hacking hacking involves 3 phases information gathering gaining access and anti forensics information gathering this is the phase where a hacker tries to collect as much information as possible about the target gaining access using the information collected the attacker designs a blueprints of the target and executes attacks against them to gain access to the system anti forensics the final phase is to erase the tracks that would eventually lead a forensic investigation back to the hacker who executed the attack on the target.

Course map this course on information security is aimed at imparting the end users with the knowledge starting right from the basics of information systems the security measures being implemented and the Ways and Means they get disrupted by hackers the course map starts with imparting knowledge on how hackers gather information about a target information gathering and information system is comprised of individual systems which when connected become a network and when they start rendering services they are known as a web even though information gathering and system based cracking seem to be a good place to start it really all starts with executing malicious software on the target system or malware and it would be unjust if it was not dealt with as the first step revising the flow the course map starts with malware followed by information gathering and the rest this module covers ways in which a system can be attacked to gain information system based cracking while this one deals with attacks pertaining to wired and wireless infrastructure offer group of systems known as network based cracking following this is the web based cracking module by now you would have noticed that all the topics are covered from a hacker's point of view and you will be wondering why this is not dealt with from a security officers point of view to be the best placement one should think about crime from a thieves perspective in the same right in order to be a good security specialist one must think from a hacker's perspective this module vulnerability assessment and penetration testing deals with the prospects of evaluating an information system and its security state from a hackers perspective

Even now what will the defending mechanism be there since the course is designed to cover topics from a hacker's perspective a clear idea of how the hacker works is imparted defining a single defending mechanism will do no good for example to arrive at the number 91 person multiplies three by three while I'm not other may add five to four on the 3rd may simply start counting number's from one and ascending order to arrive at 9 in the very same way a single fix will overtime be easily exploited by hackers and it is left to the audience to come up with their own defense mechanisms having finished with the introduction for information security let's us start deep into ethical cracking.

Malwares

It's a malware getting started with the introduction what is malware Simply put malware is the blend of two distinct words malicious plus software malware can be classified as well as categorized beginning with the classification malware can be classified into two types namely user mode malware and kernel mode malware this can be further explained with the help of protection rings which are nothing but the layers of privileges within the architecture of the computer system protection rings are organized in a hierarchical form starting from ring 0 which is the most privileged layer to ring 3 which is the least privileged layer the intermediary rings one and ring two are comprised of the drivers that facilitate communication between ring zero and three the one targeting rings 0 is termed as kernel mode malware for instance let us have a look on this system that consists of applications such as VLC notepad and Ms office etc on top of OS when the kernel mode malware corrupts the kernel program that controls the Ms office application the link between the application and the OS is broken none of the existing files or any new instances related to the Ms office application that is word excel PowerPoint is cetera can be accessed the one targeting ring three is called user mode malware when this malware effects a word application file it results in corruption only of those infected files this clearly means that an existing word file can be accessed or a new instance of the same office application can be created without any interest having learns about how malware is classified let us move into categorizing malware categorization of malware malware can be categorized into four groups namely virus worm Trojan and backdoor.

Malware the objective here is to study the characteristics behavior and purpose of malware now the architecture of malware learn how to create malware learn how to remove malware learn how an antivirus detects malware and learn how to bypass an antivirus at the end of this episode one would be able to create malware differentiate between the types of malware based on their characteristics behavior purpose and architecture and defend against malware.

Stepping into action the first category of malware virus is the most prevalent 1 what is a virus virus stands for vital information resource under siege virus is nothing but a piece of code affecting the normal behavior of a system components and virus virus comprises of the following components namely Concealer payload and replicator as the name suggests this component concealer helps in anti detection by concealing itself to look like a benign application the payload is the actual Mal code holding the executable instructions and the final component the replicator is there one which helps the virus to craft duplicate copies of itself now let us have a look at the characteristics of virus with respect to each component the component concealer is responsible for making the virus appear stealthy which allows it to implement its intent in secrecy and to evade the antivirus the next component payload allows the virus to carry another virus affecting a specific individual host meaning it is host specific one may think formatting one system helps to get rid of the virus if present however viruses remain even after assistive format this is accomplished with the help of the replicator and payload components.

Such as characteristics and components of a virus if you ever wondered how to create one such virus to create a virus one must know the life cycle that is phases of a virus these involves 6 stages starting from origination transmission triggering infection identification and removal the first phase origination it's the place where a virus is born normally a virus can only be created when one thinks from the attackers POV tech geeks will always love to build a virus by coding a program the basic requirements to code a virus

include an OS notepad application and a programming language which you are familiar with from the wide range of programming languages available we have opted for DOS commands having a numerated the requirements let us get into our mission to create a virus just open the notepad application key in the following code and save the file with the name followed by the extension dot bat and with save as type 2 all files in any desired folder your virus is ready before proceeding to the next stage please stop it would be mean of us not to tell you the easiest way to create a virus we would all be very happy for our work to be done with a single click of a button let's show you how to use a tool to accomplish our task the requirements for creating a virus using tool include the much needed IOS and a virus maker tool here Got Fidel Mays batch virus maker opening delme batch virus maker tool navigating to the payload tab and clicking on spam with message box name your virus and click on saveas.bat for saving it in any desired folder having created a virus what would be the point in keeping it to oneself timeline.

Worns

Having infected an individual host the next target of any attacker would be to infect the network which can be achieved with the help of a worm So what do you think a worm is a worm is a network specific self replicating computer program that propagates over the network in order to implement its malicious intent a worm comprises of the following components the first component being scanner it looks for vulnerabilities in the victim system once a vulnerability is found the second component penetration tool is used to exploit this vulnerability this paves the way for the next component installer to bypass all the security mechanisms and inject the malicious code that is payload into the victim system the final component discovery tool is the one that leads to the worm being called a network specific worm as it discovers the systems that are networked with the victim's machine.

Trojan

The third type of malware is the Trojan a Trojan disguises itself as a benign application say for instance an antivirus update or a game or an advertisement by wrapping itself up to the application Trojan is a destructive piece of code with payload concealer and rapper as its components payload it is the actual piece of mail code that does the destructive work concealer it uses concealment techniques in order to hide itself and prevent itself from being identified by any antimalware programs renaming it renames itself as a non malicious application EG Trojan dot bat to run DLL corruption it corrupts the security software in the system which is responsible for the tech.

Backdoor

Get to knowing the final category of malware backdoor what is a backdoor it is a small piece of malicious code that gains access to a system bypassing all authentication mechanisms backdoor comprises of a single component which is a piece of malicious code called the payload when it is sent from one machine to another weather receiver executes the code the sender requires full access of the receiver system as seen backdoor is a method whereby one system gains access to another system which follows

client server architecture a normal communication between a client and a server is termed as an overt channel however when the client which is the attacker sends the malicious payload to the server that is the victim for gaining access to the victims machine the overt channel becomes a covert channel

Anti virus

It would be unfair to sign off without discussing antivirus which takes care of this malicious software which would be absolutely unmanageable to remove manually what is antivirus it protective software designed to defend your computer against malicious software is termed as antivirus it has derived its name due to its first inception where it was purely designed to defend against the category of malware virus how does antivirus work an antivirus protects the system in two modes first is the interactive mode where the AV is kept running in the background all the time when an external drive is inserted it checks the files inside and prevents malicious files from being opened the other mode is the scan mode when this is enabled on a timely basis the critical areas of the system such as the registry startup services and task manager are monitored.

Nation gathering objective to study and gather information about the target which may include any of the following an individual and organization web system or network this is done via direct intrusion or indirect obstruction of information outcome on completion of this chapter one would have a complete blueprint of the security status irrespective of the target being any of the following system web or network haven't got an idea about hacking and cracking let's get into the process of launching an attack oh but whom are you going to attack the first and foremost task here is to fix the target which may be an individual or an organization so let's fix a target say Mr ***** YZ and Co now let's attack launching an attack now leads to gathering information about the target

What is information gathering information gathering is the preparatory phase for an attack that involves a collection of information to reveal holes in a system this process is also called reconnaissance which is the term military uses when asked to gather information in order to study the enemy reconnaissance can be done in two ways passive or active passive reconnaissance is the method of gathering information without directly intruding on the target that is by probing the web active reconnaissance involves direct intrusion on the target to collect information now that the target is fixed let's probe the target for information what is happening the target is able to track the attacker what happened when the pro was initiated whenever a request is sent to a server say for example whatismyip.com it captures the actual IP of the sender what can be done to avoid from being traced.

Masking identity in order to hide the actual IP a person can send the request via another machine making it act as a proxy server in order to mask the identity routing the traffic from the attacker system to the proxy involves tunneling tunneling is the creation of a private channel between two nodes via the public network that is the Internet weather channel can be secured using protocols such as SSH HTTP L2 TP etc masking identity is done when carrying out either active or passive reconnaissance for carrying out passive reconnaissance the following methods can be followed SSH tunneling HTTP tunneling or Tor for carrying out active reconnaissance which involves anonymous application usage against the target the following methods can be used proxy chains or proxy Trojans VPN or virtual private network can be used for masking identity while carrying out both active and passive reconnaissance what is SSH secure shell is a protocol that runs on ports 22 to ensure secure data communication between two systems this secure data communication is achieved by establishing an encrypted channel called an SSH tunnel the process of creating the channel is known as SSH tunneling let's see how an attacker makes use of SSH tunneling to mask his identity consider this an attacker is trying to access a server called what is my IP from his browser when I request is initiated from the browser the traffic is directed to port 80 and uses the gateway IP of the system or the network to reach the destination server what is my IP when the what is my IP server receives the request it's a new marets the source IP as the attacker's IP in order to route the browser's traffic via remote server using SSH tunneling the attacker creates an account on a remote server which renders shell services once an account is created then with two simple steps an SSH tunnel can be established between the attackers browser and the remote server by configuring the browser and a shell client application for example putty step one rerouting browser traffic the normal browser traffic routed via the gateway should be re routed via a proxy server this can be done by configuring the browser by choosing the option use proxy server for your LAN to use socks proxy the lamb is then configured to use loop back IP 127.0 dot 0.1 via port 8080 and alternative port for port 80 as a source port step two bridging client and server creating a bridge between the client port as the source port and the remote server port as the destination port can be done using an SSH client application such as putty the configuration of putty is done by entering the settings pertaining to the remote server that requires the name of the remote server for example shell dot dot net the port on the remote server to which the traffic has to be forwarded that is 22 the connection type pertaining to the port that is SSH and the name for these configurations for example test settings pertaining to the client requires the source port which is configured as 8080 in the browser and the type of connection is set to dynamic which tunnels all traffic to remote destinations via this port having set the source and destination the remote server account can be accessed via putty by providing the correct login credentials upon successful login an SSH tunnel will be established between the attackers browser and the remote server when the attacker initiates a request to what is my IP server the traffic gets routed to the loop back address on port 8080 which is now connected with port 22 on the remote server when the what is my IP server receives the request it enumerates the source IP as the proxies IP instead of the attackers IP this is how an attacker masks identity using SSH tunneling.

individual profiling our target may be an individual or an organization which paves the way to collecting their respective profiles fixing an individual as the target the thrust falls immediately in framing the target social profile with a vital thing is to find how people call the individual which may be his or her pet name or nickname next comes finding the way to contact the individual which is primarily via the email ID look at social networking sites and communities such as Facebook Twitter Google Groups Myspace

about dot me netlog BDO orcutt meet up high five and tagged these reveal the name email ID and also the likes and interests of an individual not many are aware of the information that they post on their Facebook wall looks of the target individual can be extracted and by tracking the status messages of the individual which includes the physical location of the places they loiter a physical attack on the target individual can be launched Google Groups provide a shared user interface that allows threaded conversations among like minded people meetup differs from other social networking sites in a way that facilitates offline group meetings which provide a way to interact with people unified with common interests people search websites to help in locating the physical address of the target individual such sites include 411.com anywho Yellow Pages peoplefinders.com personlookup.com dot AU PQ people smart people zabasearch and 192.com 192.com reveals the physical location of the individual along with the phone number of people residing in the UK whereas zabasearch is yet another website that allows a person to acquire the location of an individual in the US believing that the target individual is the only source to gather information is not a good idea finding the house inmates or the targets close associates that is relatives make the job easier familyhyphentree.co.uk it's a website that allows tracking information about the people in the UK and the website search.ancestry.com allows tracking the very same information for people in and around European countries there are times when you might have arrived at a phone number but not the name of the target or vice versa in this case Truecaller a telephone look up and reverse lookup directory can lend a helping hand retro- sleuth.com is yet another website offering the same service.

Does something to earn their living they often appear differently in this career world than they do in their social world this leads to flaming ones career profile people are often called by their nicknames in the social networking world but they may not be known with the same name when it comes to their work arena and this information needs to be gathered LinkedIn play to vital role in managing one's professional identity when surfing for a profile in LinkedIn it may reveal the official email ID for contacting the individual and professional details such as skill sets recently acquired skills organization associations domain names experience professional network connections other business networking sites also aim to provide the same service such as torque biz now viadeo branchout and Zing branch out is a Facebook application that spits out both social and professional information which includes work history and corporate relationships of the target on a dashboard consolidating the information gathered the individual profile of the target is done.

Email address harvesting what is email address harvesting obtaining lists of email addresses using various methods is called email address harvesting why do we do email address harvesting email harvesting allows the ability to track down other email addresses associated with the target and their network of connections for harvesting the email ID's associated with the target use search_email_collector which is a module in the metasploit console once the domain is set and the exploit is triggered it searches for the email ID's associated with this domain in universal search engines such as Google Yahoo and Bing it also looks for the email addresses on the domains official site social networking sites forums blogs and guestbook once an email ID associated with the domain is found it is

extracted to be displayed harvesting of email ID's associated within an organization paves the way for launching the next attack.

Network attacks objective to understand what a network is tell communication happens in a network how network attacks are classified based on the OS I model physical layer attacks datalink layer attacks network layer attacks and transport layer attacks outcome on completion of this chapter the participants will understand how I see systems communicate with each other using a network and how network attacks are performed based on physical layer datalink layer network layer and transport layer.

Network basics what is a network when two or more systems or electronic devices are connected or linked together it forms a network consider this network this network has three lands namely eat zero F1 and DTH two connected to the Internet via a router under modem notice that there are different devices linked together in this network but have you ever wondered how these communicate with each other imagine an apple computer and windows based computer wants to communicate with each other it is like French and German communicating with each other do you think there is a possibility for good communication yes if there exists a common language known to both say for example if both knew English it would facilitate the communication between them in the same way in order to accomplish a smooth communication between systems and networks have different architectures OS I open system interconnection model was introduced LSI defines a layered framework for the travel of data from one system or network to another it has seven layers physical layer datalink layer network layer transport layer session layer presentation layer and application layer each layer in this model performs its respective tasks by communicating with the layers above and below it take for example that two systems say a windows and a Mac communicate via chat application wherein the windows system is the sender and the Mac system is the receiver suppose if the windows machine sends a welcome note such as heimach via this application the data travels via these seven layers and reaches the destination after being operated upon by the underlying protocols but what happens when the data travels through these layers let us take a look at the user interface that allows the windows system to chat with his peer this is where the application layer plays its role controlling the application that allows it to communicate along with the UI's look and feel the application can also be a browser a file sharing program or something else as mentioned this layer has its own protocols such as HTTP HTTPS for web applications FTP for file sharing and SMTP and pop 3 for the sending and receiving of emails respectively in this case the application is the chat client once the data that is iMac is typed in and sent the control gets transferred to the presentation layer the presentation layer checks for the OS compatibility encryption and compression of the data before passing it on to the next layer which is the session layer the session layer is the one that provides the mechanism to manage sessions that is the active time of a user and a particular web application the session ID is assigned for the current session and the data now gets passed onto the transport layer study on the OS I model reveals the top three layers are called the web interface where one can see the data being passed on without adding any specific headers the three layers at the bottom are called the network interface the transport layer is the one that acts as a mediator to shoot the data out as well as receive the data in that's the name says this layer is responsible for the transmission of the data it converts the data into segments of a limited size with a segment number for easy reassembling at the other end along with a header called the transport layer

header which is either based on TCP or UDP let us take a glimpse at these protocols TCP transmission control protocol is a connection oriented protocol which when used sends a probe using this TCP header it consists of source port it is through this port the client gets connected to the server usually the source port is an ephemeral port which is nothing but a short lived transport port assigned automatically from a predefined range that is always greater than 1024 the destination port is a well known port on the server whose range falls between zero and 1023 sequence number acknowledgement number data offset window size checksum argh pointer and six other flags to ensure a connection oriented communication it uses a 3 way handshake wherein these Six Flags play a major role the flag is a one bit boolean feel to mark the occurrence of an event let us get to know how these flags are helpful in the communication when host a needs to send data to host B connection initiation is done by setting up the synchronization shortly syn flag in the pro when host B receives this probe it sends a reply probe with reset flag when it is not available for communication otherwise it sends a reply probe with synchronization acknowledgement shortly synak on receiving this host a sends a probe with acknowledgement shortly act to impart that the connection is established and then it starts sending the data this is called a 3 way handshake and this process of connection establishment makes TCP a connection oriented protocol when the data transmission is done the sender can send a probe with finished shortly Finn flag which closes the connection apart from this while in data transmission a push flag can be set along with the data that would instruct the system to send data immediately or in urgent flag can be set which will inform the receiving station that certain data within a segment is urgent and prioritize the delivery of this data next comes the user datagram protocol which when used consists of this header one may notice that the header consists of only the source and destination addresses along with the length of the data its checksum and the data to be sent since it does not wait for any acknowledgement for establishing a connection and for transmission of data it is called a connectionless protocol this protocol is best when used for query response or streaming TCP is a reliable protocol when compared to that of the UDP since it establishes a connection using the three way handshake ensuring a connection oriented data transmission while UDP simply transmits the data terming itself to be a connectionless protocol in terms of speed UDP is faster than that of TCP since this one does not wait until the recipient acknowledges any data transmission once the headers are appended this layer concentrates on handing over the data to the appropriate application process on the host computers wherein the control is transferred to network layer network layer is responsible for the host to host delivery of data segments from the transport layer this layer adds a header called the IP header consisting of the source and destination IP address which is similar to that of putting a letter into an envelope with a from and two address thus converting the segments of data into a packet of data So what is an IP address similar to that of a physical mailing address Internet Protocol addresses a logical address that uniquely identifies each and every system connected on a network at this point it is important to know whether the communication is going to happen between systems inside a network that is baseband communication or we also have the network that is broadband communication the routing of packets from the network layer is taken care by the network layer device called a router a router is a device that connects two different networks it works based on IP addresses and routes the data packets along the network on deciding the next point to which the packets need to be forwarded it acts more or less like a dispatcher to put in simpler terms the router acts like a traffic cop who forwards the traffic to Destin places either from and to the Internet or within the same network thus the data is now transmitted to the next layer the data link layer this layer is further divided into 2 sublayers logical link control or LLC and the media access control on Mac LLC ensures reliable data transmission by

appending sequence number to each transmitted packet before sending and sends back an acknowledgement for each received packet when the Mac layer receives the data from LLC it interacts with the physical layer below this is responsible for creation of frames from the packets it received from the network layer on a pending a frame header and frame trailer switch and hub come into play at this layer unlike the router the switch and hub cannot connect two different networks however a layer three switch can act like a router switch is a device that works based on the Mac address that is the unique number assigned to each and every system in their network interface card this device ensures point to point delivery of data a hub is a device similar to that of the switch or in the difference lies in the delivery of the data a switch is a unique cast device that concentrates on point to point delivery but a hub is a broadcast device and the data reaching the hub is broadcasted to all the other devices connected to it finally the data reaches the physical layer or in the frame is converted either as a digital or analog signal that is bitstream and gets passed on via the wires if the network is a wired network or via air if the network is a wireless one basically this is where the network hardware seemed facilitating the functions of the data link layer and the network layer gets into action as seen already when two or more systems or electronic devices are connected or linked together it forms a network and these connections are made possible via connection cables and Ethernet cable is one of the most popular forms of network cable used on wired networks Ethernet cables connect devices on local area networks such as PC's routers and switches the physical layer thus forms the fundamental for all the communication and it is revealed that 95% of network related communication issues arise at the physical layer once the physical routes to deliver the bitstream either as analog signals in a broadband communication or digital signals in a baseband communication is identified the data is routed to its destination finally the receiver gets the data in bitstream and the corresponding headers for all the layers are verified and the application layer now displays the message to the Max system this is how communication happens between systems on a network having seen how communication happens between systems one might have noticed that certain parts of the network here have not been touched upon at all let us get into knowing these things did you say that the router is allowing traffic that seems to be legitimate while it discards the illegitimate 1 this is because a firewall is configured at this point what is a firewall a firewall is a system that filters the incoming and outgoing traffic to avert unauthorized access to or from a private network all messages entering or leaving the intranet pass through the firewall which examines each message and blocks those that do not meet the specified security criteria as such a firewall can be described as stateful and stateless when a firewall is turned to be stateful it is capable of monitoring the entire content of the data packets that is the traffic stream passing through it and distinguish the legitimate packets that belong to different types of connections when a firewall is turned to be stateless it is capable of capturing only the source and destination IP it does not monitor the entire traffic stream and does filtration based on the source and destination IP's alone did you notice the IP address of the rotor and the systems in the lands are different why is it so just imagine a tech giant like Microsoft which holds N number of systems to run their processes if each and every system is assigned with a unique IP the range of IPS available will surely be exhausted at some point in time to overcome this issue the I CNN or Internet corporation for assigned names and numbers a nonprofit organization takes care of the coordination and maintenance of the databases of their unique identifiers that is IP addresses and came up with the concept of subnetting what is subnetting the process of dividing an IP network into subdivisions is called subnetting computers belonging to a subnetwork have a common group of the most significant bits in their IP addresses the addresses used for subnetting fall under the following series 10 dot X dot X dot X series 172.16 dot 0.0 to 172.31 dot

255.255 and 192.168 dot X dot X series when these multiple subnets with a common prefix are combined to form a large network it is called supernetting the IP address assigned at the router point is the public IP and this entire network connected to this router is identified with this IP by the other systems on the Internet the IP address of each and every system inside the network is its private IP this IP is not known outside the network so how is it ensure that the data packets to and from the public network are delivered properly from and to the system in the private network here comes the role of the router the router is configured to support a concept called nating Nat network address translation the process of translating a private IP into a public IP is called nating when there is no large network and you just want to connect a router to two different systems in your home network the concept of putting comes into picture port address translation is the process of assigning port numbers to the internal IP address of the machines connecting to the Internet this now facilitates the data transmission although all these implementations seem to be effective the study on the growth of Internet devices in recent times shows that the time where one Internet device was used by at least four to five members has gone and each and every individual now owns at least two to five Internet devices which eat up the available public IPS this clearly shows that the number of machines connected to the Internet exceeds the number of people alive on the earth that's where the introduction of IPV six came into play which is at 128 bits in length and ranging between the following address space this is how a network is and how the systems here communicate.

Introduction having seen how a network is and how communication happens inside a network let us dive deep into how network based attacks are performed at each and every layer of the OS I model physical layer attacks the mere concept of a physical attack implies that you have direct physical access to the systems on the network physical layer attacks include the following eavesdropping inserting a hub vandalizing datalink layer attacks this is the second layer of the OS I model which works based on the Mac address of the devices connected in a network datalink layer attacks include the following Max foofy Mac flooding arpu poisoning DNS spoofing DNS poisoning DHCP starvation rogue DHCP attack network layer attacks the network layer works based on the IP address of the systems connected in a network some of the attack vectors that disrupt the communication at this layer of the OS I model include IP spoofing sniffing MITM ICMP flooding Smurf ping of death transport layer attacks the transport layer is the one responsible for the transmission of data across the systems in a network the attack vectors that disrupt this transmission include TCP flooding and UDP flooding.

Free services offering web applications use this Mac address of the engines to terminate the free service after a specified time at such times one would like to trick the web application into believing the system to be another one by masking the Mac address called Mac spoofing this can be done manually by opening my computer manage device manager network adapters and selecting its properties traversing over to advanced tab one may spoof the Mac address to any 12 digit hex value in the network address text box let us now check whether this got updated by scanning the systems in the network using Cain and Abel here it is your spoofed Mac is seen here

Datalink layer Mac spoofing media access control or Mac as it is called is the unique physical address on a systems Nic masking this Mac address is called Mac spoofing task spoof your Mac address step one open device manager network adapters Step 2 right click on the systems network adapter and select properties Step 3 traverse to advanced tab and select locally administered address and key in any 12 digit hex value in the network address text box results open command prompt with administrative privilege and type in IP config slash all you may find the spoofed Mac address of your system.

Cafe latte this attack allows obtaining a web key from a client system by capturing and AARP packet manipulating it and sending it back to the client which subsequently generates packets that are captured and cracked to determine the web key using aircrack Ng having landed upon this whip enabled network in preparatory phase a cafe latte attack can be done in three steps one launch of the attack two capture packets 3 crack key one launch of the attack having done with the prerequisites for launching the attack let's get into launching 1 but come on when given makes the attacker wait for Abreu to say arp from any of the associated clients of the AP and grabs it to form AARP requests of its own and sets up a fake AP is a packet that is broadcasted by blind by setting the source and destination IP to itself and the test port to this address which is nothing but the broadcast port for resolving IP conflicts updating AARP tables etc this grad AARP packet is captured to make one that will look like a legit one and this is broadcasted to the network claiming the attacker to be the AP by changing its SSID to that of the legit AP this will not dissociate the client from the legit AP and start associating the client to the fake one thus making the clients in back replies that would be encrypted with the legit key two capture packets it's time now to capture the packets from the clients associated with fake AP to crack the password starting airodump Ng G using this command on double and zero now will capture the packets and save it to the file named cafe LP requests from the fake AP now generates many genuine LP replies from the clients that are captured in the file named cafe 3 crack key now that the large number of packets transmitted between the AP and the client are captured in a file opening the same file with aircrack Ng allows cracking the whip password aircrack Ng uses FM S&P TW attacks that are nothing but a form of cryptanalysis for attacking RC4 stream ciphers and do not eat many ivs that is packets to crack the key the cafe latte attack allows cracking of wireless packets in an average time of 6 minutes being the best case while two hours to crack being the worst case.

The next incription mechanism incorporated by this hotspot is WPA what is WPA and how is it different from web WPA WEP uses a 40 bit or 104 bit encryption key which do not change and needs to be manually entered at the access points and clients to overcome this weakness WPA came into existence web generates a per packet key by concatenating the Ivy directly with the passphrase or master key which exposes the master keys to carry out attacks such as FMS and PTW attacks WPA stands for Wi-Fi protected access which works based on two mechanisms namely PSK and TKIP the PSK is a client authentication method wherein the network admin assigns a pass phrase containing up to 133 characters this pass rate is X or add with keystream which is a combination of a random 32 bit key with Ivy which is nothing but the trick sum of 32 bit in length to generate unique encryption keys these encryption keys are constantly changed on a timely basis which is then shared between the clients associated with the network whenever you client gets connected to the network authentication request is sent to the access point which in return sends a response asking for the password a connection is

established once the password is verified PSK pre shared key is simple and was designed for small offices and home networks that do not require an authentication server however the encryption keys tend to become old as time changes since these keys are not generated dynamically upon login and are subjected to brute force and dictionary attacks this paves the way to opt in for the second authentication mechanism TKIP temporal key integrity protocol enhances WPA by increasing the length of Ivy by adding an extra 32 bits to the original 24 bit accounting to 56 bits to generate a unique encryption key for client to generate a unique encryption key for each client however only 48 bits are used in practice because one byte must be thrown away to avoid weak keys supposing for the communication between two clients connected in a network TKIP takes an extra precaution by ensuring that the data packet has not been altered or modified in any way by the attacker if the data packet seems to be altered it is dropped off this is achieved by the 64 bit message integrity check commonly known as the Michael algorithm TKIP employs a per packet key mechanisms dynamically generate a new 128 bit key for each incoming packet this avoids the same key staying in use as they do with WEP TKIP also provides a re keying mechanism in which it changes the encryption key of an ongoing communication in order to limit the amount of data encrypt it with the same key.

System based cracking objective the objective of this chapter is to make the audience understand how a computer works the methods used to crack system security that target the operating systems memory management process management and file management outcome on completion of this chapter you will know the intricacies involved in the operation of a computer the attack methods via which a system security can be cracked.

Introduction and information system is taken care of by the security management in such a way that it is in no way breached thereby ensuring confidentiality integrity and availability why is security so important in the first place each and every piece of data is information and irrespective of its size and nature it can pose a threat when in the wrong hands when the security of an information system gets breached thus allowing unintended users access to sensitive data it is known as a system hack or crack attacks pertaining to such a security breach can be classified under various categories such as password cracking attacks cryptographic attacks steganography attacks process management hacks or game hacks reverse engineering attacks privilege escalation attacks

System basics inventions are inspired by the world around us when the Wright brothers saw birds flying they were inspired to invent the airplane likewise the computer was invented after being inspired by the human race what is a computer computer stands for common operating machine purposely used for technological and educational research we all have this question on our minds how does the computer work.

Let us first power on the system to find out how it works when powered on the power supply passes through the power supply unit and reaches a place called the BIOS written on the memory of the motherboard but what is a power supply unit similar to that at the digestive system that converts the food taken in by the human body to provide energy the power supply unit converts the alternate

current or AC to direct current DC for the supply of electricity to the internal components of the system the power now reaches the motherboard similar to the human nervous system which connects each and every organ in the body the motherboard is a typical board with a printed circuit in the computer holding the CPU processor and memory and connects with other peripherals like hard drives video cards and soundcards the motherboard receives the power and initiates the BIOS which is nothing but a non erasable memory storage chip also called the CMO S chip which stores the BIOS settings what is the biots the first software run by a PC when the system is powered on is the BIOS or basic input output system it consists of the instructions to run the power on self test or post which checks whether all the peripherals connected to the system are able to receive power when the power supply is correct it gives out a single beep Elsa series of beeps or sound indicating a fault now the BIOS initializes the hardware components such as the processor graphics card video card sound card fans etc connected with the system this initialization is called hardware BIOS hardware BIOS initializes the processor and the memory first.

What is a processor similar to that of the human brain that commands the entire functioning of voluntary and involuntary actions the processor also called the CPU or central processing units of the system is the hardware that performs all the instructions given to a computer it consists of two main parts one arithmetic and logic unit turn control unit and two cache memory and this together forms the processor core the arithmetic and logic unit are directed by the control unit and with the help of the cache memory executes instructions on the system the instructions are executed with the help of cache memory which holds memory units called registers on processor chips for storing and processing the data using logic gates a processor is a combination of one or more cores with supporting hardware and software resources when there is only one core it is called a single core processor and a combination of two single core processors becomes a dual core processor and when two dual core processors are combined it forms a quad core processor a processor can execute end number of instructions per second the speed of a processor is defined by the number of instructions it is capable of executing per clock cycle the architecture and clock cycle of each processor differs from one make to another if the processor is labeled as 2.6 GHz speed it is capable of executing 2.6 billion instructions per second execution of instructions is carried out using the system buses where in system buses are the carriers of the electrical signals representing the machine level language bitstream zeros and ones this is where the 32 bit and 64 bit processor comes into play this can be explained well with an example of a highway road that consists of several lanes a 32 bit processor is capable of handling data in and out via four lanes each of which is 1 byte wide thus supporting only a memory of up to 4GB while the 64 bit processor is capable of handling data in and out via eight lanes that eventually supports memory above 4GB this enhances the speed of the system.

Word cracking the act of using various means to land upon or recover a password is called password cracking password cracking can be carried out either online or offline online password cracking is carried out when the attacker does not have access to the password hashes while in offline password cracking the attacker would already have obtained the password hashes both of them may be conducted actively or passively active password cracking intruding onto the victim machine directly to crack the password is called active password cracking keylogging password guessing man in the middle passive password

cracking cracking passwords without directly intruding on the victim machine is called passive password cracking there is no direct communication between the attacker and the victim password sniffing.

Even though encryption methods provide a secure data communication it does not prevent someone from knowing that something is being transmitted when intercepted and examined by a third party So what can be done to hide the actual data within something else in such a way that even when intercepted the third party will only be able to see the outer cover and not the actual info hidden within to achieve this steganography comes into play the word steganography is derived from a Greek name steganos meaning hidden or concealed and graphite meaning drawing or writing stagger fee also known as concealed writing is the practice of hiding a message within another message or a file within another file when this is used in communication it reveals nothing one interception no one apart from the sender and the receiver can identify the existence of the message before moving further let us get a glimpse of how steganography evolved from the past demaratus the king of Sparta sent a secret message on a tablet covered with wax when it was received at the other end the wax was scraped off to recover the message during World War Two stuck in ography played a vital role in the form of invisible inks which remained invisible when used for writing the actual message can be made visible if the document is heated gently next came the null cipher a cipher as already seen is a method of encrypting text null cipher refers to a method of encryption where the plaintext is mixed with the actual message for example in this sentence please do not throw sausage pizza away when the first letters alone are taken into consideration he gives the first letters of the seven layers of the OS I model this is known as null cipher next was hiding information in images microdots were used to conceal a message a microdot as a text or an image which is reduced in size to hide its contents which are then read using magnifiers apart from these with the help of spread spectrum the data is divided into small pieces and it is spread over the frequency channel of an audio file having gotten an insight about the history of steganography is time to get started types of steganography outside quite a large list of variants let us stick to these six types of steganography image steganography audio steganography whitespace steganography email steganography text eggnog refi and document steganography.

The gaming industry has a huge audience one important way the gaming industry earns income is by letting users play the game for free until they are addicted to playing the game and then lock the higher levels of the game at a certain point at which time the users are either asked to score a certain number of points or to buy out cards lives digital cash or to wait for a certain period of time to pass before continuing the game at such a point game hacks create a way to unlock the levels and score higher points but how do you hack the game scores whenever you play a game the game creates a process in your system memory and the scores you gain reside there game hacks are aimed at modifying these scores as stored in the memory addresses let us see how this can be done take for example this game score more this game can be played both offline as well as online.

To understand how web works what is cruise missile architecture how client based attacks are performed how server based attacks are performed how application based attacks are performed outcome on completion of this chapter the participants will understand how web works and what cruise missile architecture is how client server and application based attack vectors are performed,

Www.worldwideweb commonly known as the web is a collection of electronic hypertext documents stored in a computer linked together like a spider's web which can be accessed via Internet let's take a live example to get an idea of how the web works the web browser is a software program to access information from the web for example Firefox Internet Explorer safari Chrome etc in a day 3.3 billion searches happen on Google let's see exactly what happens when you type www.google.com and click enter on your web browser the browser passes this URL into three parts protocol name server name and the path to the page in the server blank space usually denotes the index as the path by default when a page request is made it fetches the index dot HTML page whereas a specific path say about dot HTML is mentioned it fetches about dot HTML from the corresponding server when this past URL comes out of the browser it becomes an HTTP request consisting of the following paths let's discuss these parts briefly request line consists of three components such as method the path to the page on the server and HTTP version the method is used to forward the request to the server the predominant methods used are get and post a normal get request looks like this wherein the parameters such as username and password are passed on the URL a typical post request appears to be like this in which all parameters are passed in the message body itself by default the first request method will be get however the consecutive request method depends on the application which may either be get or post general headers consists of the timestamp of the request the connection type between the client and the server that may be persistent or closed request headers consists of the domain name of the server acceptable type of the page either text image or application on HTML the type of browser that initiated that request entity headers are optional and are followed by a carriage return or line feed to represent the demarcation between the headers and the message body message body contains the actual content this HTTP request is then passed on to the router from where it is routed to a proxy server if set the proxy server acts as a mediator between the client and the server to serve the following purposes audit for maintenance of network logs Internet usage to report effective utilization of bandwidth and caching for speedy retrieval of the web pages generally the request is forwarded to the firewall but in some cases the proxy is placed after the firewall that is outside the network in order to conceal the identity of the network now the request is passed onto the firewall that is conventionally designed to control ports and is allowed to gain access between the clients and the server one might often get confused with terminology such as proxy firewall and proxy firewall let's see the difference between a proxy and a firewall when a proxy receives a request it checks the access list for the application layer protocols based on this the proxy forwards or blocks the request when a firewall receives a request it checks the access list for the ports however an application level firewall also checks for programs in the access list the request gets forwarded or dropped based on this list when the request goes out of your network the HTTP request header has the information of the domain name of the server which it has to reach but remains unaware of its IP location for the very reason the request goes to the domain name server the DNS translates the domain name to its corresponding IP address once it gets the server IP the request is forwarded to the corresponding server So what is a server as the name implies it is a computer that serves the requests from the clients what is a web server when the server service such as Apache tomcat IIS or Zeus is installed on a computer it becomes a web server capable of handling requests for the static pages installing services such as Oracle weblogic or glassfish over a web server will transform it into a web

application server this is capable of handling requests to process them based on the business logic and to respond accordingly the business logic may be implemented using a web application or a web service what is a web application it is a program written using packages such as Java PHP Python Ruby etc to accomplish a task example Google Maps it is a web service when a web application uses open standards such as XML soap and HTTP to provide interoperability between applications running on different platforms they are termed as web services consider an example www.virustotal.com this website fetches services from various antivirus web applications such as Bitdefender Avira avast etc in order to give a consolidated report what is a database server software such as MySQL postgre SQL etc provides database services to other programs like web applications and web services called the database server in this case I request www.google.com is for a static web page from google.com the request for this static web page is handled by a web server suppose if the request is for a location on Google Maps it will be processed by the web application server to fetch the corresponding result from the database which is managed by the database server when the request is for fetching a file from a server it is handled by a file server well it is a file server a computer installed with software such as FileZilla logicaldoc Cerberus FTP etc which is purposely designed for storing sharing and publishing files is called a file server this again uses the DB server to access the requested file from the DB and returns it back to the web server to produce the HTTP response when the request is for sending or receiving a mail it is handled by a mail server what is a mail server a computer install with software such as mercury mail transport system H mail server ETC for handling mail requests and responses is called a mail server when the request is to send emails the mail server uses SMTP on port 25 and when the request is to receive it uses POP three on port 110 when the requests are processed by the corresponding servers it generates corresponding responses where the actual HTTP response looks like this and consists of the following parts status line the request line of the HTTP request is replaced by this status line in the response it consists of the HTTP version status code is used for defining the state of the web application or the web page that has been requested for this is clustered into five different groups if the status code falls between 100 to 199 it is meant for experimental purpose 200 to 299 show successful page access 300 to 399 denotes redirection of the request 400 to 499 denote client errors and 500 to 599 denotes server errors recent phrase a brief description of the status code for example status code 404 denotes client error and the corresponding reason phrases page not found general headers consists of the timestamp of the response and the connection type between the client and the server that may be persistent or closed response headers consists of the name and version of the server that hosts the domain accept ranges mebibytes or none when it is none the client needs to wait until all the elements of the web page are rendered when it is bytes the server allows partial loading of the elements of the web page entity headers consists of the content type that gives information about the type of content in the body of the message content length denotes the length of the message last modified denotes the timestamp of the last update of the message message body the actual response for the request the response is then processed by the web browser to display the requested content next time when a user requests google.com instead of fetching the response from the server the browser process the request using previously stored responses from web cache I request that passes through a router proxy firewall web server web application server and database server to fetch response looks like a cruise missile thus making us christen this structure of working as the cruise missile architecture

He stacks fishing and attempt to steal sensitive data via electronic communications by being disguised as a trustworthy Internet resource is called as fishing fishing can be done by either of the following methods redirection using localhost redirection using server base 64 encoding host file manipulation and full screen API the first method is redirection using localhost before stepping further one must know what localhost is localhost refers to the default name of the computer that is 127.0 dot 0.1 which is also called the localhost or loop back address each system has a distinct system name say system one and a unique IP address say for instance 192.168 dot 1.9 to make a system act as a server one needs to install examp examp is a cross platform server stack consisting of a mail server file server web server and a database server once installed the excempt control panel can be opened this now allows starting the Apache server which will make your system act as a web server I seen earlier a web server is the one responsible for handling requests and responses let us see what happens when we type www.gmail.com into the browser the request is handled by the DNS server which translates the hostnames to the IP address and redirects the request to the corresponding server the server holds many files from which the default index dot HTML file is fetched as the response similarly when we type in localhost in the browser the request is handled by a server running on the same system called the localhost this displays the X amp page as a response fetching its contents from the HT docs folder in the examp server when the content of this page is replaced with that of the Gmail phishing page the response thrown for the request of the localhost would be the Gmail phishing page so how do you create this phishing page content this can be done in just two steps crafting the fake page go to the browser and type in gmail.com save the page in the HT docs folder after deleting the existing content with the name index to HTML making it work open notepad paste this piece of code save it as mail dot PHP in the HT docs folder thus your phishing page content is ready when you type localhost in the browser it will now fetch a Gmail phishing page when a username and password is typed in a request gets generated that points to the Gmail server for authentication oh what is happening rewinding back when the Gmail phishing page that is index dot HTML file was saved as such the action attribute of the form holds the link that points to the Gmail server for authentication So what can be done to redirect this request replacing this link with that of mail dot PHP and saving it or redirect the request to the localhost server for authentication which will be handled by mail dot PHP what happens when the request reaches mail dot PHP this piece of code redirects the victim to the original Gmail page while the request parameters such as username and password are captured this piece of code creates a new file named log text in the HT docs folder unlocks the user input such as username and password thus you have completed a phishing attack now when other systems within the network access the localhost it opens the Gmail phishing page when a user keys in the login credentials it gets logged and appended onto the log dot TXT file similarly when the other systems say system two and system three keys in their logging credentials the data gets logged and appended to the log dot TXT file redirection using server this system which is acting as a server in the land can be connected to the Internet directly without address translation now share your IP address with the victim when the victim accesses your IP it leads them to the phishing page hosted on your system.

Acquiring sensitive data through any electronic communications by pretending as a credible source is called phishing phishing can be done by any of the following methods redirection using localhost redirection using server base 64 encoding host file manipulation and full screen API redirection using localhost in this method the phishing pages hosted on the localhost to Fisher user note open eight docs

folder on the examp server and cut all its contents and paste it in a new folder on the desktop named ask Sam backup task creating a phishing page for Facebook number one open browser and type in facebook.com number two save the page as index dot HTML in the HT docs folder of the examp server number three put this piece of code in a notepad and save it as mail dot PHP in the HT docs folder of the examp server number four now open the index dot HTML file with notepad and search for the action attribute and change the URL to mail dot PHP and save the file number 5 by opening command prompt and typing in ifconfig get your internal IP and try accessing this IP from another system in your internal network if another system is not accessible open your browser and type in localhost #6 there's no opens the Facebook phishing page type in the username and password and click on login result open log dot TXT file to view the username and password of the Facebook user redirection using server in this method the system in which the phishing page is hosted is connected to the Internet directly note when connecting to the Internet directly see to it that address translation is disabled in the router the best way to make your system the hosting site would be to connect via dongle task creating a phishing page for Facebook number one open the browser and type in facebook.com number two save the page as index dot HTML in the htdocs folder of the X amp server after deleting the existing content in that folder number three put this piece of code in a notepad and save it as mail PHP in the HT docs folder of the examp server number four now open the index dot HTML file with notepad and search for the action attribute and change the URL over there to mail dot PHP save this file number five note your IP by visiting whatismyip.com and send this IP as a link to the victim #6 type in the username password and click on login result open the log dot TXT file to view the username and password of the Facebook user

SQL injection basics have you ever wondered what exactly happens when you type your username and password on a web page and click login the user input username and password is sent as an HTTP request to the web server which hands over this request to the web application server that generates an SQL query to check the equality of the user by fetching the data from the database but the question is what is SQL and database SQL structured query language is the query that functions to fetch and access the data from the database a database is a collection of data arranged intelligently in terms of tables with the rows and columns similar to an excel sheet rose are also called tuples or records and columns are called fields or attributes the combination of rows and columns is known as tables the database server holds an information database called information_schema to store details such as the databases tables columns views and procedures on the server for example if there are two user databases namely infosec and test the information schema consists of read only tables pertaining to infosec and test to hold the details of their structure that is the tables and their columns in the database information underscores schema tables holds the details of all the tables in a database information_schema dot columns holds the details pertaining to all the columns of tables in the database the details of specific tables and databases can be accessed using table_name and tables_schema respectively generally these values in the tables are stored as hexadecimal values let us take a look at the query that gets formed when the web application receives a request based on the user input the query gets modified as follows upon receiving the request the database server checks for the combination of the username and password in the table users that resides inside the database infosec when the data is incorrect it throws login failed as a response when the data is correct the requested data that is the account details of the user is fetched as the response this page in the web application allows the user to perform operations on the table by clicking on the search button that user details can be viewed when an input say 31413

and Chennai is given it generates a request that gets forwarded to a web application server to generate the following query this now fetches the list of usernames from the table users whose contact number is 31413 and city is Chennai in a select statement the relevant data is fetched using either and or logical operators and operator fetches a record only when both the conditions in an SQL query are true for example when an end operator is used in this select statement it fetches records of users who have both given contact number and the city as thus of the user input on the other hand or operator fetches a record if either the first condition or the second condition is true in the same example wenonah operator is used in this select statement it fetches records of users who have either given the contact number or the city as that of the user input this is how a select statement works the result is now forwarded to the web app server which sends it to the web server that delivers it to the client the next button on the web application allows the user to delete a given record take for example when the user clicks on delete and clicks on confirm it forms the query as shown this deletes the entire record of the user whose ID in the database is 1 the next is the drop query this action is allowed only for users with high privileges and the query formed is of this form which deletes the entire structure of the table users along with the records in the table drop query and delete query does the same job of deletion the only difference between them is that drop query delete's the entire table while delete query deletes only the records in a table this is how a delete and drop query work the result of this query is now forwarded to the web app server which sends it to the web server that delivers it's the client view account details button allows the user to view all their account details when do user clicks on this button a query of this form is generated the entire account details of a user can include details such as firstname last name contact details account category etc which are maintained on different tables here the details such as contact and city are located under table users and details such as accounts and account category are located under the table user_info in such a scenario the union command allows obtaining a resultset from different tables by combining 2 select statements with a condition that the number of columns selected in both the statements is the same this is how a union command works this command now retrieves the contact and city from the table users pertaining to user ID 1 along with the account and category from the table user_info whose ID is also one the result is now forwarded to the web app server which sends it to the web server that delivers the results of the client this is how the web application process is the human understandable user input to generate machine understandable SQL query for responding to user requests SQL injection instead of a human understandable input when an SQL query is injected to exploit the web application either to breach the authentication system or to fetch unauthorized information from the database it is called SQL injection.

Objective to understand how web works what is cruise missile architecture how client based attacks are performed how server based attacks are performed how application based attacks are performed outcome on completion of this chapter the participants will understand how web works and what cruise missile architecture is how client server and application based attack vectors are performed full screen API API application program interface is basically a set of GUI components YouTube full screen option uses an API that fills the entire screen called the full screen API let's see how a full screen API can be used to launch a phishing attack creating the fake page visit this URL and download this file once downloaded unzip the file and copy its contents the HT docs folder after emptying the folder now open a browser and type in localhost which loads this page containing a link to Bank of America when this link is clicked the status bar indicates that the request is being redirected to a legitimate Bank of America

website now click on the browser UI what happened you were getting this message box stating that you have been phished you have actually entered into a full screen mode where in the Bank of America web page along with the UI components are mere screenshots that's interesting isn't it so how does this work open the htdocs folder and right click on the index dot HTML page and open it with a text editor say wordpad notice this just loads a screenshot of the Bank of America page and calls some scripts from there what actually happens here is when the link is clicked upon it just does two things one browser fingerprinting and two iOS fingerprinting based on the browser and OS it decides on the UI components to be used for example when the browser is Firefox in a Linux machine it uses the corresponding UI components from this images folder or when the browser is Chrome in windows it uses the corresponding UI components from the images folder now a custom crafted page holding the content of the Bank of America website gets loaded in full screen mode based on the browser and the OS however this page is just an image but how to Fisher user with an image within this image form elements such as username password etc can be embedded when a user case in the login credentials it gets fished this is how a full screen API attack is used to perform phishing full screen API based phishing attack embedding form inputs over an image using full screen API to fish the user is called full screen API based phishing attack task launch a full screen API based phishing attack number one visit this URL and download this file number two delete the content inside the HD docs folder and copy the content inside the downloaded zip folder and save it inside htdocs folder number three now open a browser and type in localhost which opens up this page containing a link to Bank of America when this link is clicked your victim is finished results the browser gets into full screen mode and the Bank of America website loads when clicked on any place on the Bank of America phishing page it throws a message stating that you have been phished