

Information Security 3
Sri M J Shankar Raman,
Consultant Department of Computer Science and Engineering,
Indian Institute of Technology Madras
Module 56
Security in Practice (contd.)


So this module we will continue our discussion on what kind of typical security policies and mechanisms are put in place with certain kinds of configurations to deploy a network security in practice. So what are the very common security rights that are typically possible from the external world on any network right, so first activity that is typically done by the hacker or the attacker is that they will try to do a sort of a mapping of the network to find out what are all the potential targets devices that needs to be attack number one.

(Refer Slide Time: 00:56)

Internet security threats

Mapping:

- before attacking: "case the joint" - find out what services are implemented on network
- Use ping to determine what hosts have addresses on network
- Port-scanning: try to establish TCP connection to each port in sequence (see what happens)
- nmap (<http://www.insecure.org/nmap/>) mapper: "network exploration and security auditing"



Once they find out what kinds of targets are running they will try to find out the physical characteristics of the target in terms of what is the hardware, what is the operating system or the firmware which is actually running on it, depending on whether it is a server or a network device right, once I identify what firmware or the OS is running on it, they will basically find out next what is the version of that particular OS or the firmware.

Once they find out what is the OS or the firmware version, they will basically know by experience what kind of possible compromises are available on that particular version and those

kind of compromises they will try to attack one by one and then see whether with that list of compromised loopholes whether they could actually try to penetrate the server and bring it down right, so what they first basically do what is called as a case the joint.

Where where they find out what kind of services are implemented on the network, then a typical command like ping will be made use of to determine what are the host and the kind of addresses the network are that once they do this, once they find out the address on that particular address they will try to find out what kind of ports are opened, so the way they actually try to do is that, they basically try to establish a TCP connection to each port in sequence and then see.

What happens right, so if they get for example a portly set that means there is nothing that running on the service on that particular port possibly and there are also very sophisticated tools like nmap that are available which will basically do this complete scanning activity and then give you the result in a very user interactive form also right, so with all these activities the the external person who is trying to get some details about the the target network will have enough details at hand to start doing is actual attack right.

(Refer Slide Time: 02:42)

Internet security threats

Mapping: countermeasures

- record traffic entering network
- look for suspicious activity (IP addresses, ports being scanned sequentially)

So what kind of counter missions could actually been done to sort of prevent this kind of a mapping, so I record the traffic that is entering the network and if there is any kind of a

suspicious activity be it in terms of the source IP address from which it is originating or if there is a very frequent port scan that is actually happening on any of the IP addresses locally.

So like these if there is any kind of a suspicious activity then an attempt or some sort of a preventive measure should be immediately done to ensure that those specific IP addresses are actually blocked immediately from getting inside our network.

(Refer Slide Time: 03:21)

Internet security threats

Packet sniffing:

- broadcast media
- promiscuous NIC reads all packets passing by
- can read all unencrypted data (e.g. passwords)
- e.g.: C sniffs B's packets

Countermeasures?

The next possibility of a threat is basically packets sniffing, so packet sniffing as we will see subsequently in one of our letter modules, since there are tools that are actually available to tool sniff the packets on an on a media.

And then display the contents of the packet right, so any kind of a packet that is actually getting broadcasted out a person will be able to sniff it out very easily and all he needs is only a promiscuous nick mode which will have the capability to read all the packets that is actually passing on in that broadcast medium right, and unfortunately if the packets is containing some kind of very highly secure data like the passwords that too unfortunately in an unencrypted form.

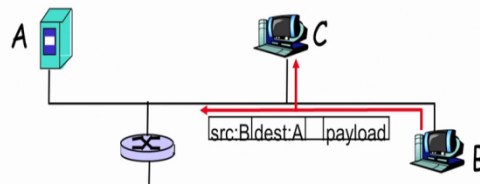
Then all the passwords of the users will be easily get accessible by the attacker, right?

(Refer Slide Time: 04:11)

Internet security threats

Packet sniffing: countermeasures

- all hosts in organization run software that checks periodically if host interface in promiscuous mode.
- one host per segment of broadcast media (switched Ethernet at hub)



So what could be some countermeasures that could typically be done by an organization against packet sniffing is that so so all the host and the organization can run a software that could periodically check if the host interface is the promiscuous mode because only if the the network card is basically in a promiscuous mode the packets could basically be sniffed out.

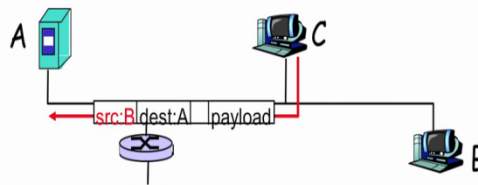
And if it could be if the the network card is prevented from getting into a promiscuous mode, then the the risk associated with the packets getting sniffed gets completely eliminated.

(Refer Slide Time: 04:42)

Internet security threats

IP Spoofing:

- can generate "raw" IP packets directly from application, putting any value into IP source address field
- receiver can't tell if source is spoofed
- e.g.: C pretends to be B



So the next threat that could possibly happen is IP spoofing, so as we were discussing in the previous module IP spoofing is basically a mechanism by which I try to use another IP address rather than my own IP address, I in situations where I know that if I actually use another IP address.

I will basically be able to bypass certain rules that has actually being configured right, so maybe a one particular IP address is actually allowed access through a firewall to the external network and attacker would basically want to change his own IP address, source IP address in his packet to be that of the IP address which is in which the firewall is being configured to allow the packets to get out right, so if that actually happens then that would be a violation of the firewall rule.

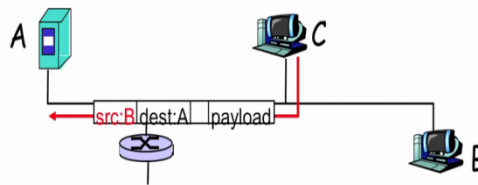
Wherein even though my packets are not allowed to get out of the network, my packets will be able to get out because I have actually changed the IP address, the source IP address in my packet to be the IP address of another mission, which is actually allowed in the firewall to get out right.

(Refer Slide Time: 05:45)

Internet security threats

IP Spoofing: ingress filtering

- routers should not forward outgoing packets with invalid source addresses (e.g., datagram source address not in router's network)



So this is a possible threat that could actually bypass certain firewall rules that has been setup, so for that one of the common missions that is actually avoided, that is actually implemented.

Is what is called as a ingress filtering, where the routers will not basically forward the outgoing packets with an invalid source address right, so now how the router determines that it is an invalid source address, it has its own algorithm to determine whether the source address is invalid or not, one of the checks in that validity of the source address is that, is this source address present on the interface in which this packet is actually come right.

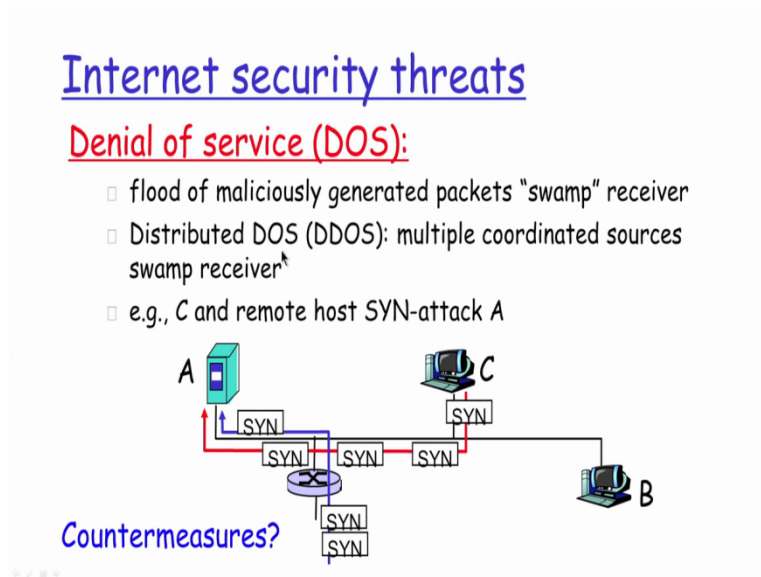
So if that is not the case, then the router will know that there has been actually IP spoofing because of which the router is actually sort of program to drop those packets right, so for example if I if I am basically getting a packet from this particular interface and the source IP address of the packet is basically the address of b right, and let say that my b is somewhere here and there is no connectivity of b with this particular router at all right.

So there is no way by which I will be able to get the the packet that is actually coming in here with the source address as b, now with this kind of an ingress filtering mechanism the router when it receives the packet, will have this as one of the criteria's to check for the validity to

source address and will silently drop the packet in cases where it finds that the packet is being received on an interface and a source IP address of the packet.

Is not matching with the network address of that particular interface, so this is one way by which the IP spoofing threat is actually eliminated by doing certain configurations on my router device, right?

(Refer Slide Time: 07:36)



So we just had a look at what the denial of service attack is in the previous module, so it's basically a flood of maliciously generating packets just with the, purely with the intention of only swamping the receiver and without any real intention of really making use of the establishing a a legitimate connection with the receiver right.

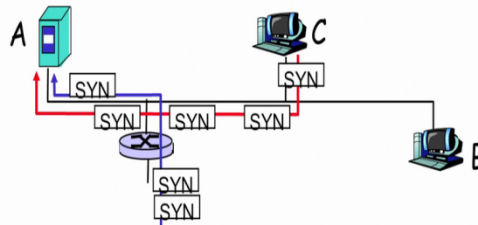
So a modified version in the denial of service is what is called as a distributed dos, where instead of a single attacking mission, there is a very very well coordinated multiple sources which actually swamp a single receiver in the same time right, so thereby the server which is being getting attacked can possibly died on in a much quicker time as compare to getting attacked only from a a single external server right.

(Refer Slide Time: 08:30)

Internet security threats

Denial of service (DOS): countermeasures

- filter out flooded packets (e.g., SYN) before reaching host: throw out good with bad
- traceback to source of floods (most likely an innocent, compromised machine)



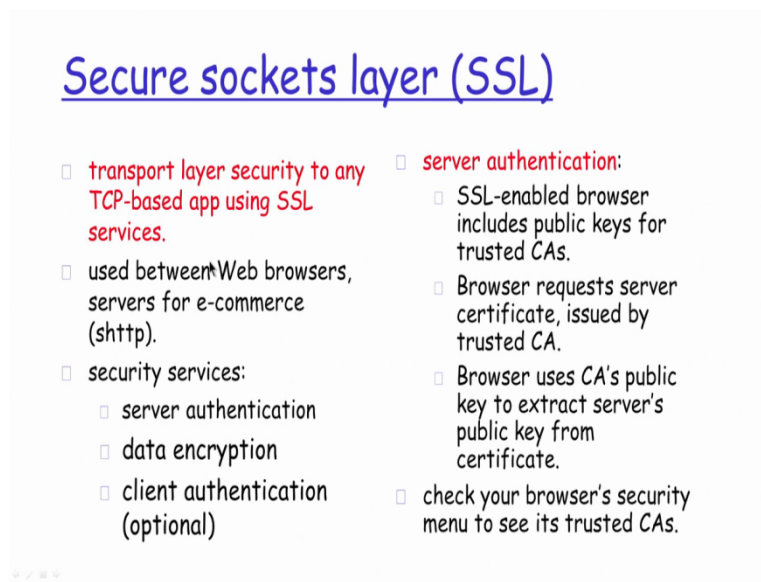
So that is basically what is referred to as a distributed dos also, so what kind of counter missions do I really have so the the firewalls today basically have a mechanism to filter out any kind of flooded packets that are actually coming in beyond a particular threshold level right, so all these configuration is configurable at the firewall device where I will say that within a particular duration of time if I basically get the same type of packets right.

I will basically block that particular IP address for a certain period of time right, so the certain period of time is typically random period of time because of which that particular server that is there behind my firewall is protected from getting attacked and wasting all his memory resources or whatever it is on the on the attacker that is getting trigger from outside the network right, so in addition to having this filtering of mechanism, typically I also have a way by which I could do a trace back

To the source of floods right, which which is the mission that is actually triggering this attack by trying to generate this kind of heavy traffic with this whole intention of trying to bring down my server right, so it's also a possibility that even though I sort of trace back to that source mission that mission itself is something which is very innocent and which is not triggering this but because of some level of loop wholes that was existing there right.

That mission itself would have been compromised first and because of that fact, that mission would have been used as a source for generating these attacks by the attacker right.

(Refer Slide Time: 10:04)



Secure sockets layer (SSL)

- transport layer security to any TCP-based app using SSL services.
- used between Web browsers, servers for e-commerce (https).
- security services:
 - server authentication
 - data encryption
 - client authentication (optional)
- server authentication:
 - SSL-enabled browser includes public keys for trusted CAs.
 - Browser requests server certificate, issued by trusted CA.
 - Browser uses CA's public key to extract server's public key from certificate.
- check your browser's security menu to see its trusted CAs.

So then he come into a secure sockets layer so any kind of a network browser to a network web server that we are trying to use right now right, so if you for example try to access any kind of online bank account or a e-commerce portal site or whatever it is.

You will always find that you have to make use of only what is called as an https right and not http, now what is this https this is basically a secure form of http protocol where before your data actually goes out so for example let say that you are giving your bank account details or you are giving your credit card details or whatever it is or for obvious reasons you don't wanted to be getting transmitted in a plain text form but you want it to be actually getting transmitted.

Only in an encrypted form, now who is going to do this encryption it's basically the secure sockets layer that is actually available for the TCP to be making use of for having all the data that is actually getting sent out with the browser to the server and back right, back the response back to the server to the browser, all of them getting encrypted and then getting sent out right, so what kind of services that are possible through this secure sockets layer.

The secure sockets layer is actually a huge topic by itself but the kind of very common security service that are typically used is one is the server authentication, so where the server is really authenticated to ensure that it is actually the server with whom this particular browser wants to really get in touch with, number one, number two doing a data encryption and the data decryption part of it and then number three an optional client authentication right.

So there are certain situations in which the server alone is not authenticated but the server would also want to know whether the client is really the client which is actually claiming itself to be right, so the SSL mechanism also has in built techniques in place which will be able to do the client authentication part of it also if require right, so how is the server authentication done, so SSL enable browser includes a public key from the trusted certificate authorities.

The ca's means as a certificate authority which are, who are the people who are actually authorized to basically give what is the the digital certificates through the individual entities, so the browser will basically request the server certificate initially and it will allow only if that particular server certificate has been signed and issued by a a trusted certificate authority right, so that is not the case the browser will basically typically give a warning to the user.

Saying that it seems to be an invalid certificate and whether user would really like to continue taking a risk and only if the user says that yes they would like to continue the session will continue to have proceed further for the actual data transfer and the user says that they don't want to take a risk, the session will be getting dominated then and there right, so then the browser will basically use the public key of the certificate authority to extract the server's public key.

From the certificate, so the digital certificate that we actually saw in the previous module is one mechanism by which I will be able to distribute the public key of the server to the client browser right, so with this the browser will be able to get the public key of the server which has to be used for encrypting the data before sending out from the browser to the server right, so once this encrypted data with the public key sent out by the browser, it reaches a server.

The server will use the private key that it is knows internally, so that it is its own private key, decrypt the data and then get back the original data right.

(Refer Slide Time: 13:51)

SSL (continued)

Encrypted SSL session:

- Browser generates *symmetric session key*, encrypts it with server's public key, sends encrypted key to server.
- Using private key, server decrypts session key.
- Browser, server know session key
 - All data sent into TCP socket (by client or server) encrypted with session key.

- SSL: basis of IETF Transport Layer Security (TLS).
- SSL can be used for non-Web applications, e.g., IMAP.
- Client authentication can be done with client certificates.

So that's basically how typically the secure sockets layer is helping me to do the encryption part of it as well as authentication part of it by having the the the server authentication done by the digital certificate which contains a public key of that server right, so there will be an encrypted SSL session as I was telling you encrypted.

With the public key that has been actually communicated to the browser through the digital certificate and the server will be using the private key to decrypt the data and then getting back the original content right,

(Refer Slide Time: 14:22)

IPsec: Network Layer Security

- **Network-layer secrecy:**
 - sending host encrypts the data in IP datagram
 - TCP and UDP segments; ICMP and SNMP messages.
- **Network-layer authentication**
 - destination host can authenticate source IP address
- **Two principle protocols:**
 - authentication header (AH) protocol
 - encapsulation security payload (ESP) protocol
- **For both AH and ESP, source, destination handshake:**
 - create network-layer logical channel called a security association (SA)
- **Each SA unidirectional.**
- **Uniquely determined by:**
 - security protocol (AH or ESP)
 - source IP address
 - 32-bit connection ID

So in addition to SSL at the network layer you also have something called as an IP sec, so IP sec basically IP security mechanism that is actually implemented that the network layer in my 5 layer stack right.

So I also have a way by which I could have the data completely encrypted inside my IP datagram and I will also be able to do the network layer authentication where the destination host can authenticate the source IP address of a particular packet, so a packet is actually mentioning that this is the source IP address of a packet, so that could actually be authenticated by the destination host, thereby really verifying that it has actually come.

Only from that particular IP address right, so there is something called as a authentication network protocol and encapsulation security payload protocol which helps me to basically have all the network security services that I will typically require right from authentication to providing me confidentiality to providing me the message data integrity part of it, all available as part of these two protocols right, so how this actually works is there is something.

Called as a security association that is actually created between the two ends for both authentication header protocol as well as encapsulation security protocol and the security association that is created between the source and the destination helps me with providing with

all these kind of security services right, so the IP sec is basically a security mechanism is a very very comprehensive security mechanism that is actually available to me as part of the network layer and that provide me all the services that I typically require from a a typical network security protocol.

Thank you.