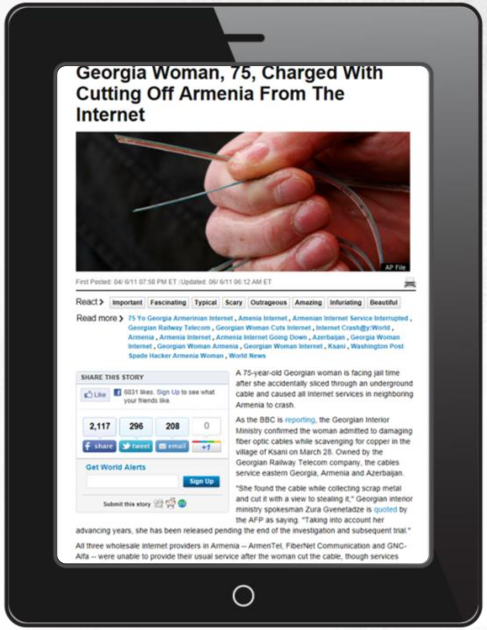
NETWORK PROTOCOLS

PHYSICAL LAYER

Threats: Denial of Service

- **THE MOST BASIC** element of computer networks, the function of the physical layer is to transmit raw data bits
- **BLOCKING DEVICES** and media in this layer is the equivalent of launching an effective denial of service attack in the entire system



Georgia Woman, 75, Charged With Cutting Off Armenia From The Internet

AP File

First Posted: 04/ 6/11 07:58 PM ET | Updated: 06/ 6/11 06:12 AM ET

React › Important | Fascinating | Typical | Scary | Outrageous | Amazing | Infuriating | Beautiful

Read more › 75 Yo Georgia Armerinian Internet, Amenia Internet, Armenian Internet Service Interrupted, Georgian Railway Telecom, Georgian Woman Cuts Internet, Internet Crash@y:World, Armenia, Armenia Internet, Armenia Internet Going Down, Azerbaijan, Georgia Woman Internet, Georgian Woman Armenia, Georgian Woman Internet, Ksani, Washington Post Spade Hacker Armenia Woman, World News

SHARE THIS STORY

Like | 6031 likes. Sign Up to see what your friends like.

2,117 share | 296 tweet | 208 email | 0 +1

Get World Alerts | Sign Up

Submit this story

A 75-year-old Georgian woman is facing jail time after she accidentally sliced through an underground cable and caused all Internet services in neighboring Armenia to crash.

As the BBC is reporting, the Georgian Interior Ministry confirmed the woman admitted to damaging fiber optic cables while scavenging for copper in the village of Ksani on March 28. Owned by the Georgian Railway Telecom company, the cables service eastern Georgia, Armenia and Azerbaijan.

"She found the cable while collecting scrap metal and cut it with a view to stealing it," Georgian interior ministry spokesman Zura Gvenetadze is quoted by the AFP as saying. "Taking into account her advancing years, she has been released pending the end of the investigation and subsequent trial."

All three wholesale internet providers in Armenia -- ArmenTel, FiberNet Communication and GNC-Alfa -- were unable to provide their usual service after the woman cut the cable, though services

PHYSICAL LAYER

Threats: Unauthorised Access

THE SECOND TYPICAL THREAT

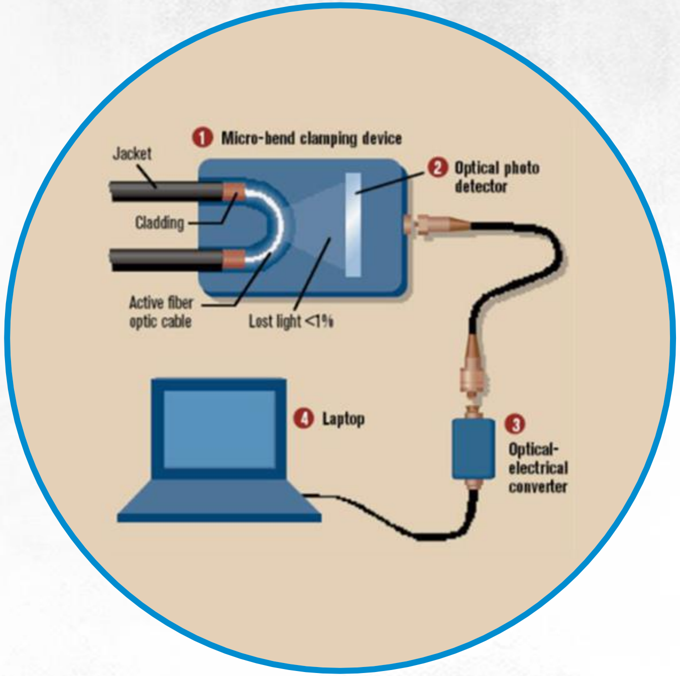
in the physical layer can occur if unauthorised persons obtain access to a medium

BECAUSE IN MANY NETWORKS

this means automatic easy access to all, or nearly all data transmitted across this medium, the unauthorised local access attack is a serious threat for the confidentiality and integrity of data

YOU CAN'T CHOOSE A MEDIUM

that will make you more secure in the face of the eavesdropping threat



PHYSICAL LAYER

Threats: Unauthorised Access

Most protocols running in the upper layers in the OSI model cannot validate the identity of the packet source and cannot ensure the security and integrity of the packet

THE ONLY FEASIBLE COUNTERMEASURES IN THIS LAYER ARE:

- Limiting physical access to network devices and media
- Monitoring company premises and their vicinity
- Duplicating the most critical connections

DATA LINK LAYER

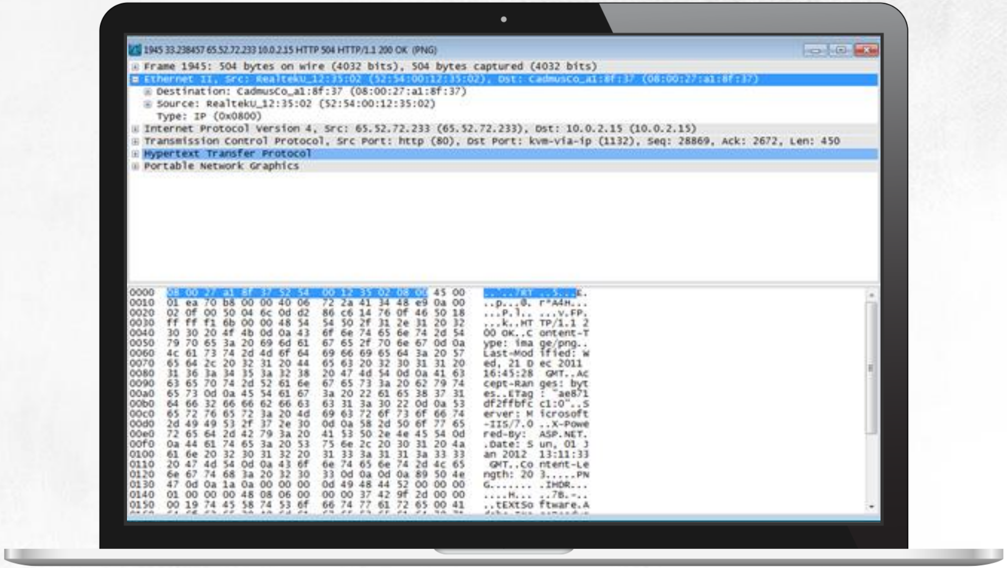
Threats: MAC Spoofing

THE DATA LINK LAYER protocol mostly used is the Ethernet protocol. Ethernet frames carry higher-layer protocol packets

THE MAC addresses of the source and destination hosts are contained in an Ethernet frame header

THE MAC addressing rules:

- If the source and destination hosts are in the same network, the packets are transmitted directly
- If the destination host is not in the same network, the source host forwards packets through a router



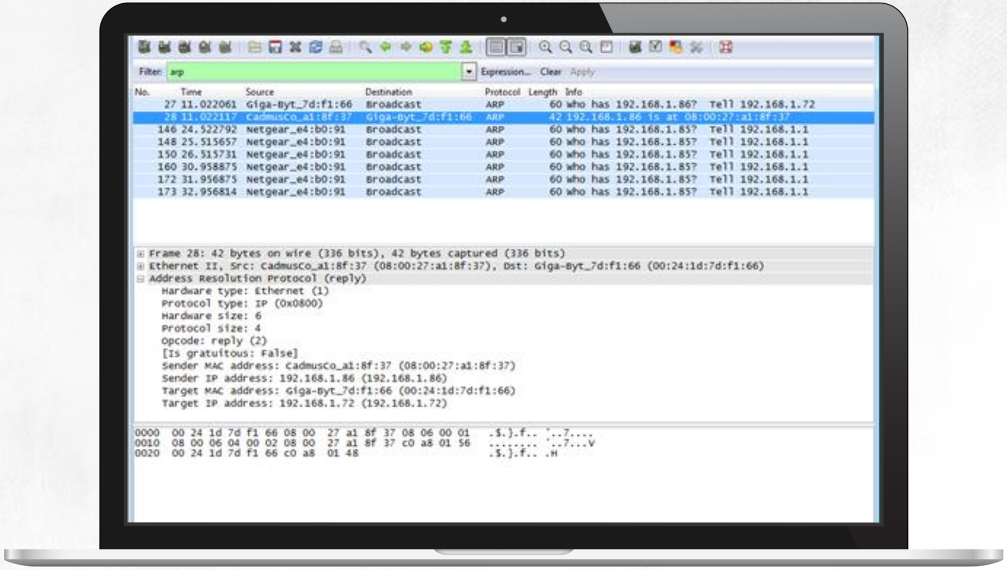
DATA LINK LAYER

Threats: MAC Spoofing

HOW DOES THE SOURCE HOST KNOW THE DESTINATION HOST'S MAC ADDRESS?

The source needs to broadcast requests to all networked computers checking if they have the destination MAC address

Under RFC 826 this request should only be answered by the computer with the searched MAC address



DATA LINK LAYER

Threats: MAC Spoofing

ONCE GETTING A

response, the requester does not validate its authenticity

What's more, the ARP protocol is stateless

ARP specification states MAC addresses can even be broadcast without a need (Gratuitous ARP)

ALL THIS, AND THE FOLLOWING FACTORS:

NICs being able to receive all packets sent through a medium to which they are connected

MAC addresses being changeable

contribute to the greatest data link layer threat: MAC Spoofing and attackers sniffing out data transmitted through a shared medium

DATA LINK LAYER

Threats: MAC Spoofing

The second layer in the OSI model has two types of networking devices operating: hubs and switches

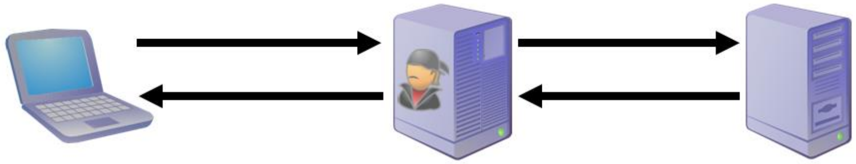
A HUB TRANSMITS RECEIVED packets across all the ports (to all networked hosts)

A SWITCH TRANSMITS PACKETS only to the one port to which the computer that has the target MAC address is connected

Since today all network architectures include switches, simply connecting a computer to a local network may not allow the attacker to sniff out data that is transmitted in the network

DATA LINK LAYER

Threats: ARP Poisoning



DATA LINK LAYER

Threats: ARP Poisoning

Method #1: flooding a switch with fake MAC addresses and associated fake IP addresses

THIS ATTACK:

Is easy to detect

May or may not be effective depending on the switch

DATA LINK LAYER

Threats: ARP Poisoning

METHOD #2: poisoning the ARP cache in the targeted computer

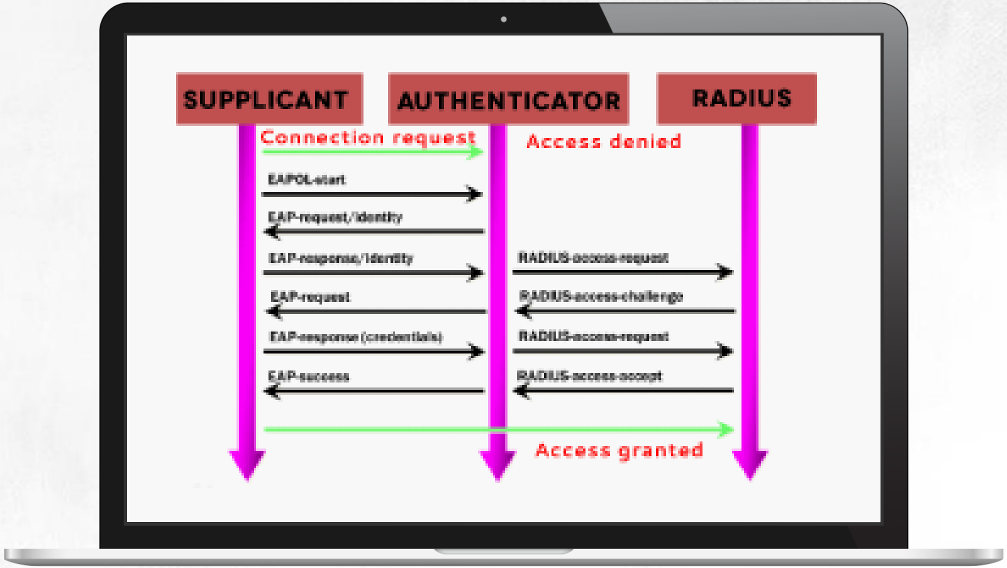
SINCE IT'S ARP that is responsible for translating MAC addresses into their associated IP addresses, by modifying the ARP cache the attacker can cause packets sent to the IP address of server X to be in fact sent to the computer chosen by the attacker

IF THAT SERVER'S ARP cache becomes poisoned as well, and the attacker's computer will forward received data to its original destinations, the communications between client and server will not be interrupted: however, the attacker has full access to all the data transmitted

DATA LINK LAYER

Protection: 802.1x standard

THE 802.1X STANDARD
provides definitions for medium access control techniques both in wired and wireless networks



DATA LINK LAYER

Protection: 802.1x standard

A CLIENT

(supplicant) must have an authentication code, which could be a certificate issued for the computer (EAP-TLS) or a password (EAP-PSK)

GLOBAL TRENDS

A RADIUS

server verifies computers' identity and allows the switch to open a given port or blocks this

AN AUTHENTICATOR

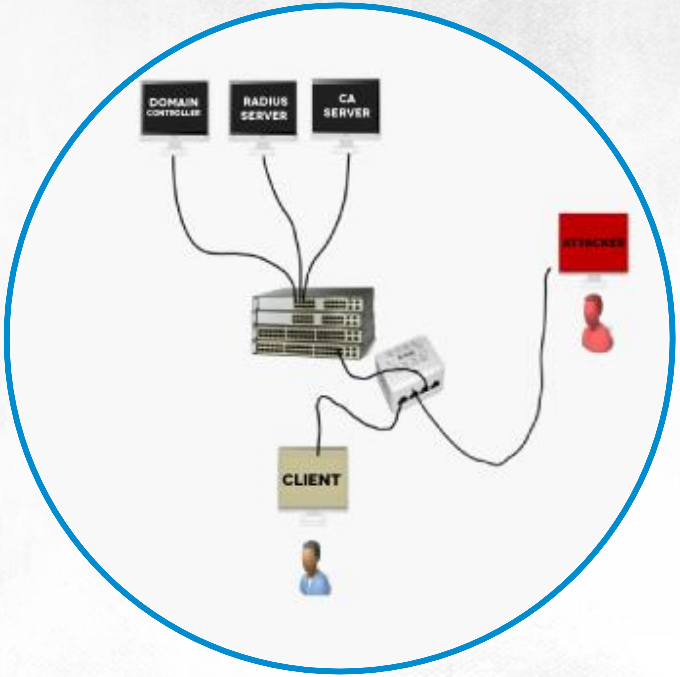
(a switch in wireless networks) is supposed to be a RADIUS server's proxy. It only opens a port if a computer trying to connect can prove its identity

DATA LINK LAYER

Protection: 802.1x standard

THIS SOLUTION IS FUNDAMENTALLY flawed: once a computer is granted access, all other computers connected to the port will be able to listen on the data transmitted over this port

WHAT'S MORE, ALL PACKETS SENT through this port will be accepted provided the MAC address of the source matches the MAC address of the authenticated computer



DATA LINK LAYER

Protection: 802.1x standard

THIS MEANS THAT TO GAIN FULL ACCESS TO THE COMPUTER, IT'S ENOUGH TO:

ONE

Disconnect an authenticated computer from the switch

TWO

Connect a hub to the port

THREE

Re-connect the computer to the switch using the hub

FOUR

Connect your computer to the hub

FIVE

Listen on for the MAC address of the authenticated host

SIX

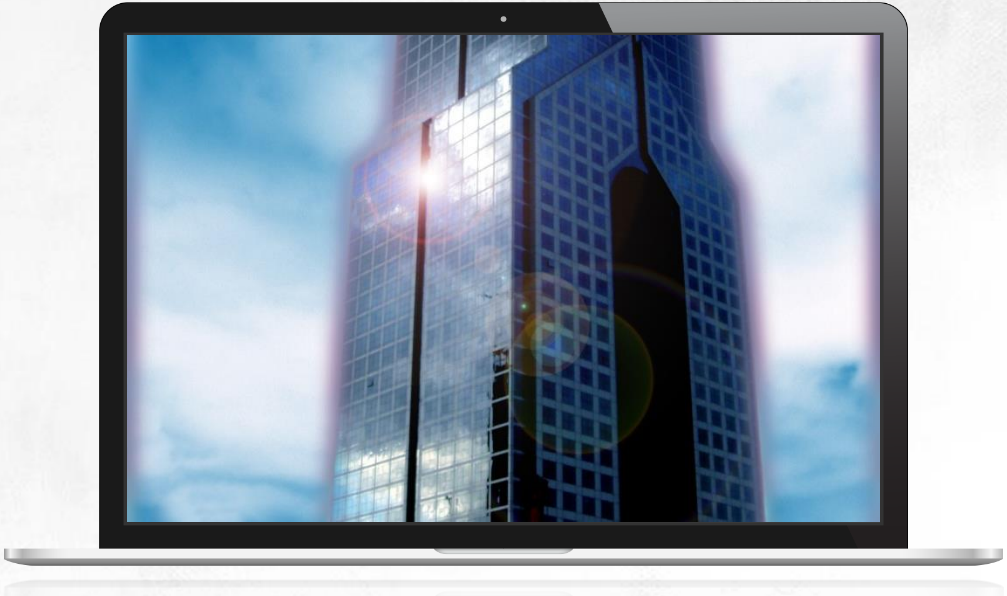
Change your computer's MAC address to the address of the trusted computer

DATA LINK LAYER

Protection: 802.1x standard

THE BEST PROTECTION
in this layer is still turning off all unneeded port switches

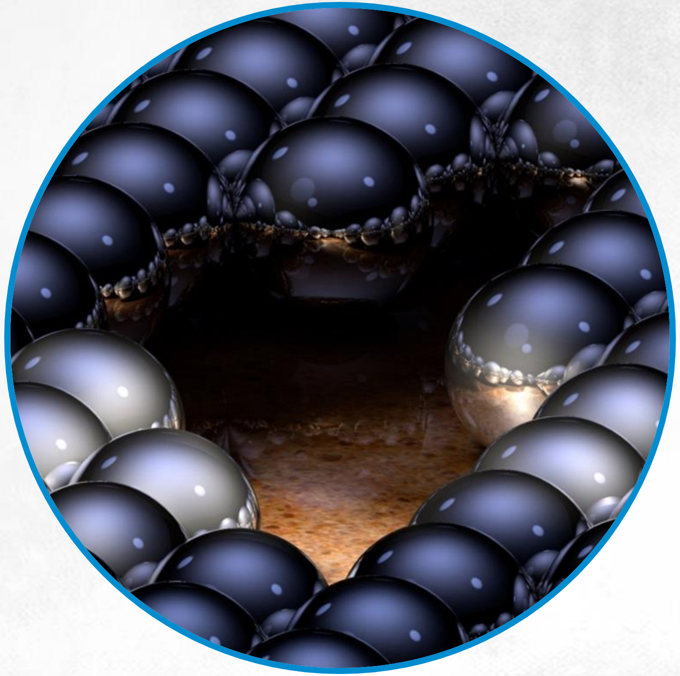
DIVIDING A NETWORK
into VLANs will only help to reduce attack territory



EXERCISE

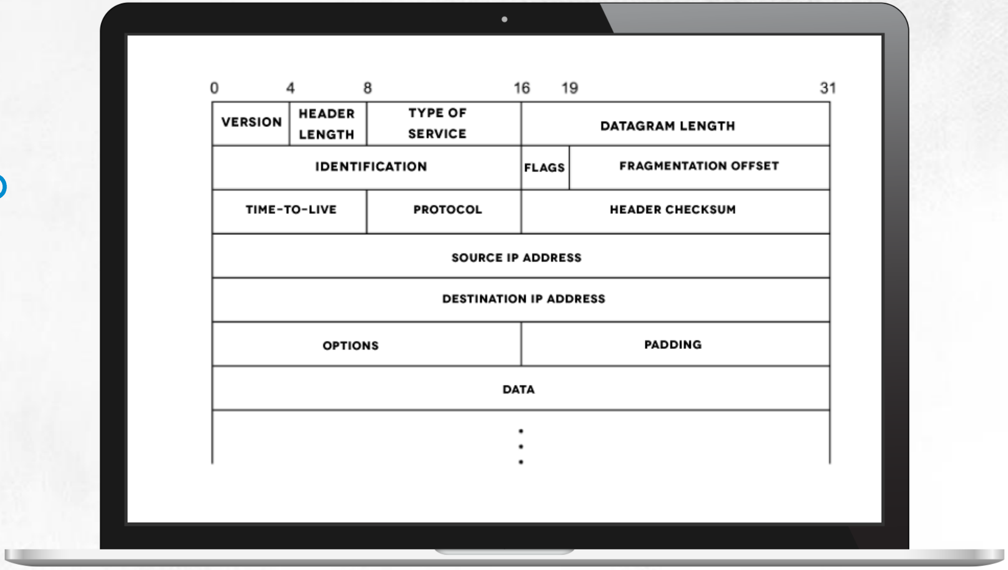
Data Link Layer Attack

- **A MITM ATTACK**
  using Cain & Abel



NETWORK LAYER

IPv4



THE PROTOCOLS OF THE THIRD OSI model layer are responsible for addressing data packets and diagnosing network problems

NETWORK LAYER

IPv4

GLOBAL TRENDS

EACH HOST

in a network has a unique address

THIS ADDRESS

is a 32-bit number divided into four 8-bit numbers

APART FROM

its IP address, each host must have a subnet mask associated with the IP

A SUBNET

mask may be expressed in octets of information (like IP addresses) or in the number of bits the mask has

THE PART

in a mask where a bit has the value of 1 identifies the network address, while the part in a mask where a bit has the value of 0 identifies the host number

THE NETWORK

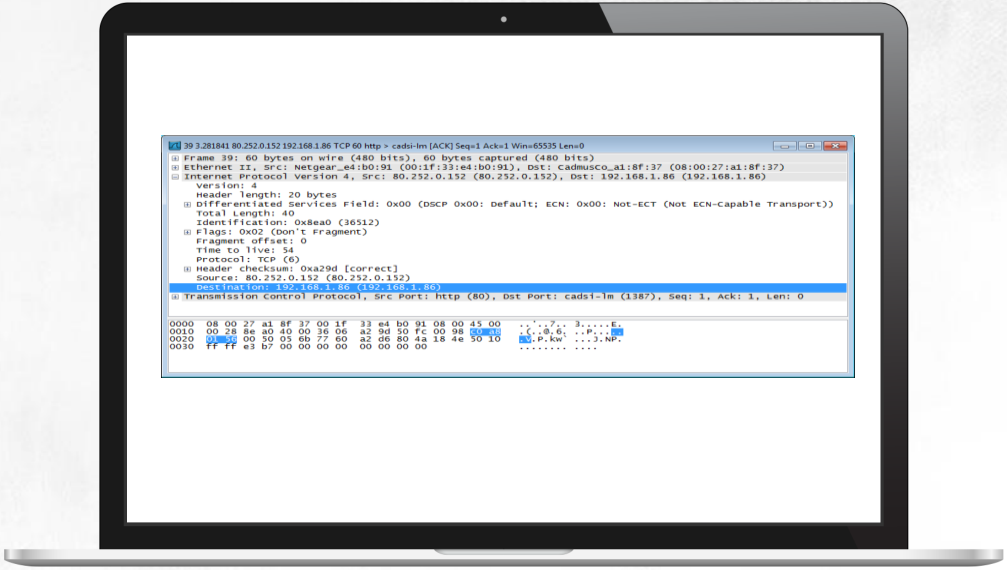
address is given in full before the host address

NETWORK LAYER

IPv4

IP PACKETS

are called datagrams



NETWORK LAYER

Threats: IP Spoofing and Routing Tables Modification

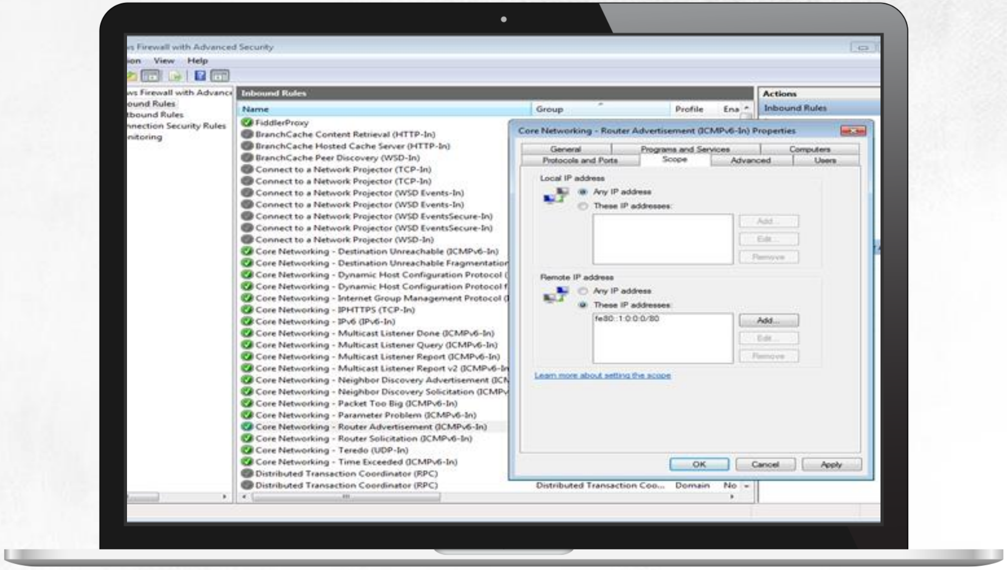
SINCE DATAGRAM HEADERS

(like the data they hold) lack both encryption or signatures, the attacker may use a simple method to obtain this information and modify it

THE BIGGEST THREAT

in the third OSI model layer is IP Spoofing, the ability of attackers to change the source IP address

This is used mainly to obscure the attacker's real IP address



NETWORK LAYER

Threats: IP Spoofing and Routing Tables Modification

THE IP PROTOCOL

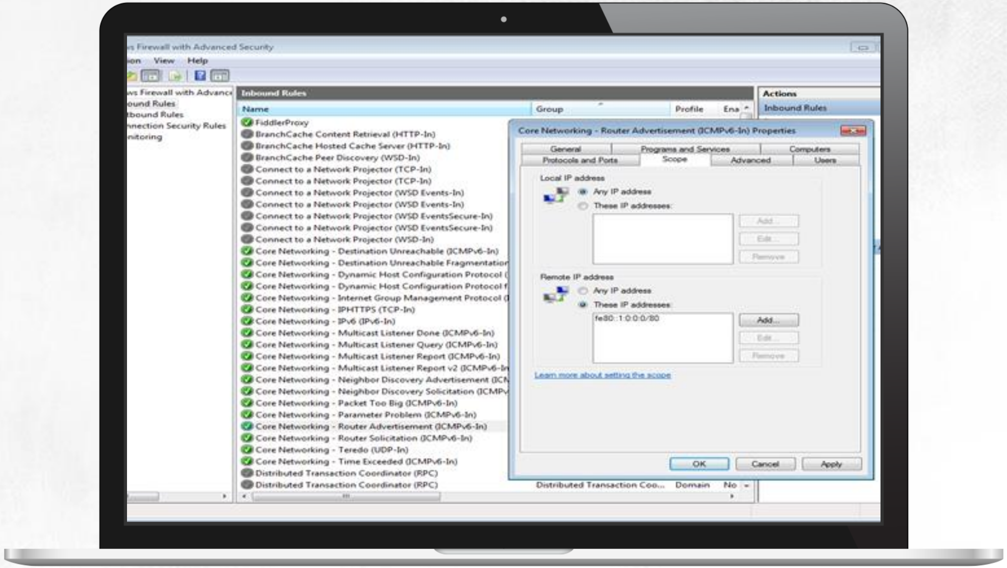
enables routing, or sending datagrams across networks

THE IPV6 SPECIFICATION

stipulates that every computer should be set to listen on for broadcasts about new routing paths and change its routing table accordingly

THIS CAN ALLOW THE ATTACKER

to block all computers in a local network by broadcasting false paths



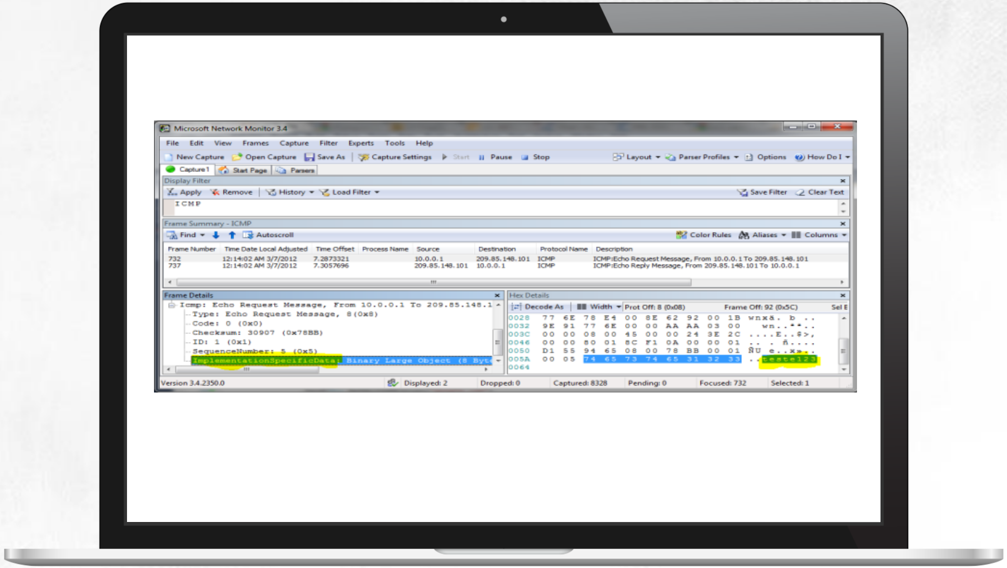
NETWORK LAYER

TCP Tunnelling over ICMP

A THIRD MALICIOUS threat in the third layer of the OSI model involves the non-convention use of ICMP

THE PROTOCOL WAS never meant to be used for packet transmission, and because of this, it is not blocked in most systems

ICMP MAY BE TURNED however into a vehicle for transmitting data, including TCP tunnelling



NETWORK LAYER

TCP Tunnelling over ICMP

To protect the system from threats specific to layer three, consider:

DIVIDING

networks into firewall-protected subnets

MONITORING

all network layer protocol packets, including broadcast packets and ICMP packets

FILTERING

packets that modify routing tables

BLOCKING

automatic routing modifications:
netsh interface ipv6 set interface "Local Area Connection" routerdiscovery=disabled

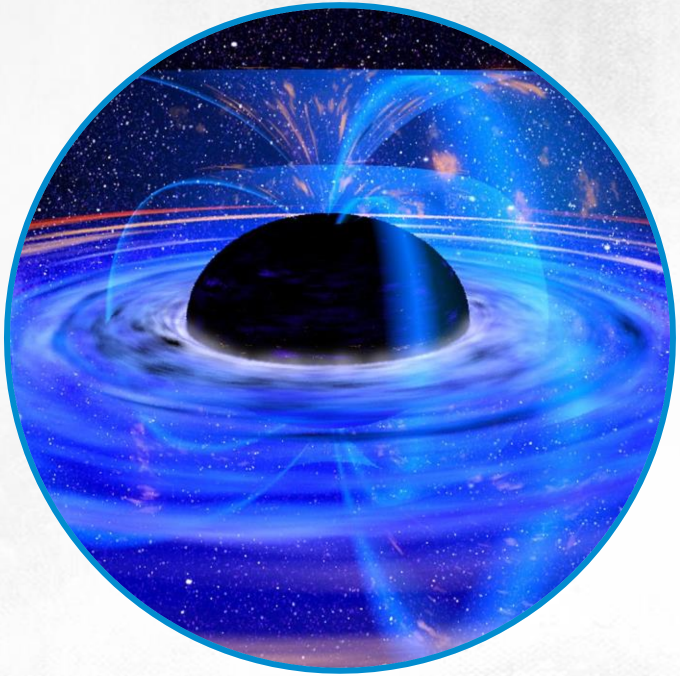
ENCRYPTING

and signing datagrams using IP Sec

EXERCISE

Network Layer Attack

- **IP SPOOFING**
  using nmap
- **DOS ATTACKS**
  using routing broadcasts



THANKS