[COMPUTER SECURITY SLAYTINDA] In 1983 there was an intrusion on a pentagon’s computer for exmp. , first computer worm was sent later from MIT and created in 1983 created 50000 dollars of damage. And in 19994 , one guy intruded in an American bank and stored 10 millions dollars. In 1999 NASA computer had broken in and one point seventh million of data stolen. So, today nearly half of the companies maybe more than half of the companies complaining damages due to computer security issues, financial damages due to comptr security issues. The Amount of damage caused by these computer security issues is much more than written here, which was taken from the book , several years ago. So, what we have is, we have financial ,personel,privacy,data,computer loses and sometimes computer doesn’t work so that also causes additional loses etc. So, computer security is a big problem for today, the reason that computer security became a problem is interesting. In the older days, internet did exist between 1970s 1980s 1990s and compt security was not that significant many sistems many rautırs(rauters) had very weak password autantication (\*Password authentication is **a process that involves a user inputting a unique ID and key that are then checked against stored credentials**. You've likely been asked to create and/or enter a password to gain access to a personal account, whether that's a social media platform or an online banking tool.\*) sometimes password autantication “ Authentication is **the process of recognizing a user's identity**. ... Different systems may require different types of credentials to ascertain a user's identity. The credential often takes the form of a password, which is a secret and known only to the individual and the system.” did not even exist in 1980 for exmp, when the first computer system started to exist simultaneous jobs, they did not password, bc if you have an access to computer center physically, that means you are eligible person and bc of that they trust you. If you are working in a factory, in tüpraş,petrol refinery, you are an engineer you are responsible from one machines which is processing oil . and security of that machine is depending on you. If you have an access, you can turn it off, if you don’t have an access, you can not turn it off, who is giving the access, if you are working in tüpraş? The security gard. You have an identity card , you show your identity card when you are entering and you go and turn on and turn off just a machine, if you are a bad person, (intelligence agent) who is just trying to destroy the refinery in other country as sabotaj, you either kill the engineer, impersonate the face and so fake the security gard at the door or you enter the system like a pizza delivery guy with the truck , you enter inside of the building and do whatever is necessary to destroy certain things, the aim of destruction is multidimensional, one significant interest is fighting between countries such as the issue iran-united states. Second we call them rogue employee , employee is working in the company but he or she is not happy and want to cheat that company in which they are working.So, internal security issues. Internal stealing can happen. Or, you fire the person,due to several reasons so suddenly he or she turns against the company and tries to steal the information or try to block the operation bc he was also trying to cause damage bc he thinks that it is a right thing to do to make a damage on the company bc he was right that the company was wrong,so , there was a dispute. Another way is to make money, you can gather information from hidden places and sell it for exmp, you can go into tüpraş refinery get some oil to your car and go out, basically it is stealing or you can learn about distributers of oil in the country who is making how much money, you can get that list and therefore sell that list to some additional tair seller or otomobile or transport sellers for them to make additional profit. It can be profit originated.you may just want to try to get profit rather than causing damage. The last one is just playing. Some people just want to block certain operations. For exmp, one of you is trying to block hepsiburada why? Bc you don’t like them. Just playing. And that will sort of register you as a hacker and as a hacker you will be proud so you do it for fun. There are several reasons. That kind of physical security and computer security is actually closely related in the army. There is a password thing which is famous , Kemal sunal, and actually he shout şener şen two or twice times bc şener şen couldn’t remember the second password . Computer and Network security was not at all well known , several years ago.lets say after 2005 computer security became in issue why is that so bc networks were not that complex that is one issue. Networks and software was not too complicated so if the software is not complicated, there will be less bugs. If you have too many things going on when you have too many doors of the refinery that means you need to have too many security guards. When you have too many security guards, too many probability of having a weak security guard but when you have only one entrance with a good security guard and policies, one security guard is watching another security guard, that will be a secure entry system.relatively better system than having multiple doors to the building. As systems we came(?) complex for exmp. There is a trash door trash track comes in famous in American film, pizza track breaks in all the places,they can break in army , CIA , banks , so pizza guy is the most accessibility showing guy in all Hollywood films . So, today when we say security people will stand up and say okay okay it is good very good nice, so we have to put more money in security. When I say do you want security or, usability that is one search area, doo you want more security or functionality, people say security. So there is a default tendency to go to security accept security is a necessity but really it may not bewell understood the word security is also related to physical security, national security,army, that’s why people are very keen to accept it. They accept it as default, bc the word security has the background, so there are interesting topics of threats, countermeasures,risks,stories,events and paranoia also about security and we in this department have siber security graduate program as an additional program to regular computer engineering graduate program, so siber security graduate program is directed to Ibrahim soğukpınar, we havea separate kontenjan for that we accept additional student for that area for graduate masters program so it is interesting and the money you make with security work as a computer security employee is relatively high. Bc as I say public opinion is security is very good so management says it is important thing bc it is important and they pay you high salary. There are mathematics going on ,algorithms,designs and software issues mixed in and also experience is very important in security experience is very important in army as well, so for that reason Turkish army is switched from regular soldier to professional soldier in the combat for the training part, you do surve but they don’t take you to dangerous places since you are not experienced bc it is a biggest security related places the army in general security issue. Not enough people even security specialist understand the issues and implications so it is like a Kristof if you keep looking this direction too long you forget the holes in this direction if you are working in the security gate in the tüpraş refinery for years but not going around the plant, you may forget the whole in the whole, you didn’t see it, it requires to have multidimensional understanding of all the problems bc everything is related.when engineers started to see factory from their home to see what factory is doing during the night they want mobile application connecting to tüpraş refinery so they open up we worked in such a project they open up and see how many tons and galons of fuel is processed during 11. Pm in izmir,adana. They want to check but that gives an access to their machines that means anyone who can access this phone can access the factory so security gard at the door becomes irrelevant you don’t have to go into the refinery as a pizza delivery person rather you can hack into engineers’ telefon and go into refinery. A famous Iranian incident some of you remember… Iranian nucleus virus incident.. since Iranian guys new that, they may be attacked through internet, devices were not connected to internet whole information was running in local area network. Uranium arrangement plant. But the virus came through usb flashdrives they root a virus for usb flashdrives. For the world. And that virus is expencting to go into iran and to that kind of machine to get activated otherwise that virus stay silent so for several months the virus traveled the world everybody is infected but no one knew nothing bc it wasn’t causing any harm. Only harm is done when the virus attacks okay im in the plant and im not connected to this kind of machine, then it destroys the enrichment machine.by changing the revolution per minute etc. changing the parameters. In turkey in tubitak, they have 2 lines, external which is connected to internet and internal which is not connected to internet and flashdrives is not allowed. You can apply security policies flashdrives of the drives are not functioning. So that you can not use it. There is a new treat recently due to the issues between china and usa . people believe that hardwire viruses is injected while manufacturing process, when you design a circuit and send it to tayvan for fabrication the chip they insert additional code in the chip so chip comes back you think that it is your chip it is functioning perfectly but somtmes it is functioning differently and you don’t know when . alparslan hoca has verification technics whether there is an additional crcuit put into the chip during manufacturing In china for malicious bad purposes.it is gerçek not iddia. In 1992 , we have several student friends, in graduate program, from army, from denizcililk school, during training in ege see, tatbikak, their radars show map of united states when the American ships were present, theirs radars show the map of usa. So, in 1992. So, probably software has switched to another state, there is a big if at the beginning saying that if usa ships present, switch to map,that is basically, some showing the power, not doing anything, im capable of disabling your radars.and then you see and obey the orders. So, the media pushes the issues with security.credit card robs, corporate loss, identity theft etc.there are many interesting ways to do them, one of them for exmp, social engineering by calling and saying that pkk in your bank account etc. but actually it happens. Soü why this is happening? [WHAT IS SECURITY SLAYTINA GECIYOR] .When you lock the doors you are partly in safe, not completely. (call the police when you feel insecure, really??)The dispute between punishment vs prevention. If there is no punishment , rate of incident inrcreas so having a proper and applicable punishment process reduces the probabilities of “threats” ın usa house burglaries are much lower than UK bc the police and probability of getting caught, that probability is much much higher in united states.if you do something wrong, you get caught. Since you cannot escape, you don’t do it, unless you are crazy.since the programs are complex, whoever controls the program controls the operation so they can buy the person, they can bribe(rüşvet vermek) a person who is developing the code and insert some interesting code to activate it later and coder says I didn’t know it. So that brings an issue about crosschecking the developed code whether the programmer is not in foreign countries agent if you are working for aselsan, everybody should be screen so that the developed code should not be leaked should not be changed for certain reason so networks are general an visible it is like public rood it is not(?) a communist country in the old days when you travel from one city to another city.you need to get permit. So the human traffic requires permit also in ottoman times. But today human traffic in the country is free except borders of the countries. Therefore complete security is very difficult therefore you have to go and check what the people are doing continuously and improve yourself, so both sides improve abilities. For emxp. One of the faculties said some turks on the way of going usa without visa recently how? They go to Mexico and they are crossing the border as if they are mexicon there are certain goals of computer security one is integrity. “ **Integrity** is the ability to ensure that a system and its data has not suffered unauthorized modification. Integrity protection protects not only data, but also operating systems, applications and hardware from being altered by unauthorized individuals.”It guarantees that the data is what we expect. For exmp. You gpa is your gpa. He was also asking me that they are having whether the student has a registered scholarship which is registreted the system. But some people are entering there illegally to the system and changing their status from no scholarship to scholarship so they don’t pay.so, they want a secure system and one security procedure the rector was thinking that a cm-ompany that is totally unknown by people in cyprus so that company wont be accessible. Confidentiality , “The information must just be accessible to authorized people” “**Confidentiality** ensures that data exchanged is not accessible to unauthorized users. The users could be applications, processes, other systems and/or humans. When designing a system, adequate control mechanisms to enforce confidentiality should be in place, as well as policies that dictate what authorized users can and cannot do with the data. The more sensitive the data, the higher the level of confidentiality. Therefore, all sensitive data should always be controlled and monitored”the information must just be accessible to the authorized people. For exmp, [ŞUAN GOALS OF COMPUTER SECURITY SLAYTINDA] you had an incident in the past and you don’t want others to know it , that should be confidential. You may have illness for exmp, that you don’t want to reveal, so unauthorized people should not access that information. When you have a computer system should work all the time when we have a network should work continuously, we call it reliability, “computers should work without having unexpected problems” actually, functioning continuously and correctly without unexpected problems and security also with that.Fourth is authentication “guarantees that only authorized persons can access to the resources”.kimlik kontrolü. [MORE SLAYTINA GECIYOR] . one of the interesting facts with computer security is NON-REPUDIATION WHICH MAY BE ASKED IN THE EXAM THEREFORE. “ **Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity**, so neither can later deny having processed the information.”It means if you do something, such as you ate meal in cafeteraia during lunhch later you go to office I didn’t eat lunch but the system shows me you ate so my credit is reduced so give my money back. In this case, the machine should be able to tell “you actually ate meal” so, “I did not do it” issues, kind of should be prevented. You writing smt on social media agains someone and later that day you sue that guy and that guy is saying that I did not do it.So, that should be prevented. Bc if I did not do it succeeds, a lot of bad things might happen. So, if you do something, that should be registered.,either positive or negative again,formal autantication is the access control who can pass who can not pass the last was is related to reliability is AVAILABİLİTY availability means if you have a service like website it should be available all the time “Data availability means that information is accessible to authorized users. It provides an assurance that your system and data can be accessed by authenticated users whenever they’re needed. “ with the security threats the availability can be harmed one idea is DOS attacks “ A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected. “Denial Of Service means that you have a store that you don’t like. Like LCW . so, how do you prevent business in the store? Turn electricity, second steal all items , kill the workers, buy everything so that nobody is coming by, or bring school children to visit the store, so , all the places are fulled with school children , nobody is coming since it is so crowded but children don’t buy anything just coming , so , there are too many customers, no one is buying anything, and the service is busy but nothing is being sold so we call it as Denial of Service which is famous , and it could be distributed these busses coming from different countries, so that they look like they are legitimate. This security guard says okay they are legititimate customers. What can I say? They are customer. But the wrong thing is, they only come for one purpose , they are coming for doing nothing but they are keeping the system busy. So, it is what DOS ATTACKS is. That reduces the availability. What does it mean to be secure? The Wikipedia says “Include protecton of information from theft or corruption or the preservation of availability , as defined in the security policy. There are types of securities.Usually, one thing is theft , corruption or preservation of availability, “ Identity theft is a **crime in which an attacker uses fraud or deception to obtain personal or sensitive information from a victim and misuses it to act in the victim's name**. “ Data corruption refers to any unwanted change to data during its transmission or storage.”. first thing is losing smt, second is changing from non,scholarship to scholarship, third is no functioning. The dangerous one is corruption. Because you change it for exmp, when ırak is invaded the first thing they lost is “tapular” then they lost information who is having which land? The data is lost. That is interesting.so, the types of security is NETWORK SECURITY, SYSTEM AND SOFTWARE SECURITY AND PHYSICAL SECURITY. I have a computer here. Physical security is who has the computer? I have it but you can steal it, if there is no password associated at the opening, you have all data. Even if there is password, you can take the harddrive out. Put the harddrive on your machine and read all the contents. So, this is physical security.So, I have to keep my drive secure, for that purpose there are some programs which encrypts part of the harddrive so that even if it is stolen it cannot be read by another computer like financial informations. NETWORK SECURITY. Im connecting to the some Z23-5G now. Our famous new access point which is fast enough to make a class but one of you may come with an access point with the battery or with your phone with the same name.I can connect it,thinking that that is the point of connection. For example you are seeing freewifi in shopping places. Or sturbucks and you trust and connect fine. You connect it . and you enter garanti bankası to chechk your bank account so far so good. So, which IP is connected to garanti ? what is the IP of garanti bank? How do I know it? What is the DNS server? 888.8 is DNS server. So, when you type this number, the browser asks this IP number about where is the IP number of garanti com and 888 returns an answer indicating that garanti is 193.194.18…. and garanti web comes enter password etc. if you are faking this Z23-56 at the beginning with the freewifi, if you are faking this DNS, your browser will think that it is connecting to 888.8 it is getting information about garanti legitimately as an IP number and try to connect that information and if the person is made an entrance in the entry screen, “sistemde bir aksaklık oluştu” but they got your password therefore most banks know use two factor(?) autantication with the phone so but it actually is not happening this year but last year, the hackers say you have an autantication message to your phone in the fake website and they ask the model of the phone , you select model, they send you a malicious code as well, this malicious code is installed automatically it comes you are thinking that it comes from garanti but what is does it it redirects the sms confirmation strings back to the hacker’s computers, when you are really entering when they are entering your account, without your knowledge,so they install sms redirection software, sms comes in, redirected to hacker’s computer bc you install it as they request on the website, so one important thing is when you are going to a wbsite make sure that website is the website that you go. (47.11’e kadar)

780

00:47:12,127 --> 00:47:13,663

The famous story is

781

00:47:14,175 --> 00:47:18,015

Actually they are turks several turks open and

782

00:47:18,783 --> 00:47:20,319

American embassy

783

00:47:20,831 --> 00:47:22,111

In an African country

784

00:47:23,647 --> 00:47:25,951

They hired a building

785

00:47:26,719 --> 00:47:28,255

They open the embassy

786

00:47:30,047 --> 00:47:32,095

And they gave visus to people with money

787

00:47:34,143 --> 00:47:35,167

For a long time

788

00:47:37,215 --> 00:47:40,031

So they make they make a lot of money

789

00:47:40,287 --> 00:47:41,055

and Run away

790

00:47:41,823 --> 00:47:43,103

Another story is

791

00:47:48,991 --> 00:47:51,295

in the western turkey

792

00:47:51,551 --> 00:47:55,391

they open the bank bank branch

793

00:47:55,647 --> 00:47:56,671

In a small town

794

00:47:57,183 --> 00:48:02,047

Probably.Ziraatbank They started operating a bank

795

00:48:02,815 --> 00:48:04,351

But the bank was fake

796

00:48:06,399 --> 00:48:11,263

So they were collecting money from giving something or giving some money and collecting money but

797

00:48:11,775 --> 00:48:14,591

relatively

798

00:48:15,871 --> 00:48:20,223

Less money is given then they disappear

799

00:48:22,015 --> 00:48:22,783

Another

800

00:48:23,295 --> 00:48:24,575

Example was

801

00:48:29,183 --> 00:48:29,695

Is it

802

00:48:31,999 --> 00:48:33,791

It is an eminonü

803

00:48:35,071 --> 00:48:36,863

One Police Station

804

00:48:38,655 --> 00:48:39,423

as Operated

805

00:48:40,447 --> 00:48:46,591

Like over 10 years I think 12 years I will find the story for you

806

00:48:48,383 --> 00:48:50,431

People retired from

807

00:48:50,687 --> 00:48:51,967

Police Department

808

00:48:52,223 --> 00:48:58,367

several friends like 3 I think 3 policeman retired and they thought that they couldnt do anything other than being a policeman

809

00:48:59,647 --> 00:49:01,439

810

00:49:01,695 --> 00:49:05,279

so they hired

811

00:49:05,535 --> 00:49:08,863

Building and open the karakol

812

00:49:09,631 --> 00:49:15,775

They got the furniture and they put the some

813

00:49:16,031 --> 00:49:21,919

Blah blah blah karakolu at the top, they operate the karakol several years

814

00:49:22,175 --> 00:49:23,199

Several years

815

00:49:24,223 --> 00:49:25,503

They arrest people

816

00:49:29,087 --> 00:49:33,439

They have to community to text you today works

817

00:49:34,975 --> 00:49:41,119

as they supposed to work and it is revealed when

818

00:49:44,703 --> 00:49:46,239

Call was distributed to the karakol , in the policestation, in the list of the ministry..

819

00:49:46,495 --> 00:49:47,263

Today

820

00:49:47,519 --> 00:49:51,871

Color codes in the police station stand in the list of the

821

00:49:52,383 --> 00:49:58,527

Ministry of Interior Department for call distribution.

822

00:49:58,783 --> 00:49:59,807

that karakol was not listed and they realized that karakol was not real rather than fake. they call police guys and police guys apologized and they disepperaed,didngt get punished , karakol turned into a real one and operated later

826

00:50:19,263 --> 00:50:22,591

Probably the guys apologized and they disappeared

827

00:50:23,359 --> 00:50:27,967

So they didn't get punished and interestingly

828

00:50:28,223 --> 00:50:30,015

Turn to a real one

831

00:50:42,559 --> 00:50:45,887

That is important when you visit hepsiburada.com

832

00:50:46,143 --> 00:50:47,935

if your connection point is

833

00:50:48,191 --> 00:50:49,983

Z23 5G

834

00:50:50,751 --> 00:50:54,847

Make sure that it is they make sure that it's that one not the one in there

835

00:50:55,103 --> 00:50:55,615

Back

836

00:50:57,663 --> 00:50:58,431

it can be

837

00:51:05,087 --> 00:51:07,135

Also that can happen

838

00:51:11,743 --> 00:51:13,279

int the building level

839

00:51:13,535 --> 00:51:16,351

If the attackers attackers

840

00:51:18,655 --> 00:51:20,703

Got our computer center

841

00:51:20,959 --> 00:51:21,983

in the University

842

00:51:22,495 --> 00:51:25,055

All the DNS information is

843

00:51:25,311 --> 00:51:28,639

Getting dns numbers from that

844

00:51:28,895 --> 00:51:29,919

computer Center dns server (garanti bankası resim seçer gösterir çünkü fake garanti bankası sayfası asıl garanti bankasının seçtiği resmi göremez ve bu resim kullanıcıyla asıl garanti bankası sayfası arasındadır.

“Software cannot protect software (Maybe hardware can)”

“Networks can be protected better than softwares”

845

00:51:30,431 --> 00:51:36,575

routing is done there so if they can access.

846

00:51:36,831 --> 00:51:39,391

rauting table and dns information

847

00:51:39,647 --> 00:51:41,183

they can raute you

848

00:51:41,439 --> 00:51:42,463

to a different server

849

00:51:43,231 --> 00:51:45,279

And you still think that

850

00:51:45,535 --> 00:51:48,351

You're going to you are typing the correct

851

00:51:48,607 --> 00:51:49,631

Thing but

852

00:51:49,887 --> 00:51:55,263

Actually could be a different site that's why banks are showing some pictures

853

00:51:55,519 --> 00:51:57,567

when you log on there is a picture

854

00:51:57,823 --> 00:52:00,383

That you should remember from the previous time

855

00:52:00,639 --> 00:52:01,407

Because

856

00:52:01,663 --> 00:52:07,807

like kemal sunal and şener şen that should be agreed on in the previous meeting

857

00:52:08,063 --> 00:52:14,207

When you have a picture of a car as a security

858

00:52:14,463 --> 00:52:18,047

measure that picture of the car must be shown by garantibankası

859

00:52:19,583 --> 00:52:21,631

To you so that

860

00:52:22,911 --> 00:52:28,031

You can be sure that that garantibankası is the same garantibankası you talk last time

861

00:52:29,567 --> 00:52:35,711

not a new garantibankası, bc if garantinankası is the new garantibank,which is fake, they cannot remember the car picture that you choose.

862

00:52:35,967 --> 00:52:37,247

Which is fake

863

00:52:37,503 --> 00:52:38,271

10

864

00:52:38,527 --> 00:52:40,575

They cannot remember the last

865

00:52:40,831 --> 00:52:43,647

Car pictures that you have chosen

866

00:52:43,903 --> 00:52:50,047

that is for machine operated scripts

867

00:52:50,303 --> 00:52:54,143

Scripture that is to eliminate machine Scripts

868

00:52:55,167 --> 00:52:58,751

Attackers sometimes use automated Scripts

869

00:53:00,543 --> 00:53:01,055

to test several things

870

00:53:01,311 --> 00:53:02,591

or

871

00:53:03,103 --> 00:53:04,639

There are some

872

00:53:05,151 --> 00:53:06,175

Websites

873

00:53:06,943 --> 00:53:09,247

that can make money

874

00:53:09,503 --> 00:53:15,647

Legitimately no problem giving a service but as if they are giving the service by themselves

875

00:53:17,695 --> 00:53:19,999

such as certain a government tasks checkhing your sabıka kaydı, when you are checking your sabıka kaydı, you go to A government type your ssc number and get your belge but some guy make a website

876

00:53:20,255 --> 00:53:23,327

877

00:53:23,839 --> 00:53:24,863

882

00:53:38,175 --> 00:53:43,039

but some guy may make a website

883

00:53:43,807 --> 00:53:49,439

to Make little bit easier with additional information like weather,news etc etc

884

00:53:49,695 --> 00:53:50,463

Get your

885

00:53:51,999 --> 00:53:54,815

sabıkakaydı if you type your

886

00:53:56,863 --> 00:53:58,655

Social security number and password

887

00:53:59,167 --> 00:54:00,447

when you press enter

888

00:54:00,959 --> 00:54:04,287

The website calls automatically the A government site

889

00:54:04,543 --> 00:54:08,383

And returns the information so it is working as a proxy

890

00:54:08,895 --> 00:54:11,199

A government doesn't want that

891

00:54:11,455 --> 00:54:13,247

Because they are giving the service

892

00:54:14,015 --> 00:54:17,343

They don't want additional third parties are (arzuhalci websites?) in front of theirs.

893

00:54:17,599 --> 00:54:22,719

if you are going to work with them

894

00:54:23,487 --> 00:54:25,279

You have to work with them in person

895

00:54:25,791 --> 00:54:27,583

not through automated players

896

00:54:27,839 --> 00:54:29,375

therefore they put

897

00:54:29,631 --> 00:54:30,143

Capche(sitelerde robot musunuz? Diye gösterilen şey)

898

00:54:33,471 --> 00:54:34,495

Algorithms

899

00:54:35,007 --> 00:54:37,567

To detect that there is a really person

900

00:54:38,335 --> 00:54:39,359

In front of it

901

00:54:40,383 --> 00:54:45,247

student registretion system asked you to add two numbers right

902

00:54:46,271 --> 00:54:46,783

So

903

00:54:48,575 --> 00:54:50,367

that is Done by a person so

904

00:54:50,623 --> 00:54:52,415

Student registration system

905

00:54:53,695 --> 00:54:57,791

then understands that there's a person in front not another machine

996

01:18:20,927 --> 01:18:23,231

so, What are the

997

01:18:23,487 --> 01:18:27,327

certain attacks this class I am going to

998

01:18:27,583 --> 01:18:30,143

go over certain type of attacks what is it

999

01:18:31,679 --> 01:18:36,543

I just got over it in the previous hour

1000

01:18:37,055 --> 01:18:38,591

"Network attacks" ilk 3 kırmızı yazı çeşitleridir.

such as Creating a fake network, fake wireless network, fake wired network or listening to network

1001

01:18:40,383 --> 01:18:42,175

Packet sniffing = “A packet sniffer — also known as a packet analyzer, protocol analyzer or network analyzer — is a piece of hardware or software used to monitor network traffic. “man- in -the- middle proxiying all the data so that you learn everytihing what is going on

1007

01:19:01,887 --> 01:19:03,167

1008

01:19:03,679 --> 01:19:06,239

Impersonating a certain websites which is DNS hacking

I just described garanticom TR is it garanticomtr really????

That is what DNS hacking is

1011

01:19:14,431 --> 01:19:15,711

Second

1012

01:19:15,967 --> 01:19:18,271

"Web attacks" ilk 3 kırmızı yazı çeşitleridir. like "phishing"

“**Phishing** is a type of [social engineering](https://en.wikipedia.org/wiki/Social_engineering_(security)) where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message designed to trick a human victim into revealing [sensitive information](https://en.wikipedia.org/wiki/Sensitive_information) to the attacker or to deploy malicious software on the victim's infrastructure like [ransomware](https://en.wikipedia.org/wiki/Ransomware). “

1013

01:19:18,527 --> 01:19:19,807

Impersonating

1014

01:19:20,063 --> 01:19:21,343

"SQL injection" = database corruption.

1015

01:19:21,599 --> 01:19:22,623

1016

01:19:23,135 --> 01:19:23,903

1017

01:19:24,927 --> 01:19:26,719

"Cross-site scripting"

1018

01:19:29,279 --> 01:19:30,047

there is a

1019

01:19:33,887 --> 01:19:36,703

Advertisement in one page web page

1020

01:19:36,959 --> 01:19:40,799

Which contains certain code that could runs on another page

1021

01:19:41,311 --> 01:19:47,455

a malicious page try to get information from the user content on

1022

01:19:47,711 --> 01:19:53,855

On the page that it is reciding on , that is working , so this page sends information to another side. through the script. that is what "cross side attack" is. “Cross-site scripting attacks, also called XSS attacks, are a type of injection attack that injects malicious code into otherwise safe websites. An attacker will use a flaw in a target web application to send some kind of malicious code, most commonly client-side JavaScript, to an end user. Rather than targeting the application’s host itself, XSS attacks generally target the application’s users directly. Organizations and companies running web applications can leave the door open for XSS attacks if they display content from users or untrusted sources without proper escaping or validation.”

1023

01:19:54,111 --> 01:20:00,255

1024

01:20:00,511 --> 01:20:04,863

Or operating system application Level attack or software attacks, ilk 5 kırmızı yazı çeşitleridir. those

are virus,trojan,worms,rootkits,buffer overflow.

1025

01:20:05,119 --> 01:20:08,447

Next one is "social engineering".

1026

01:20:08,703 --> 01:20:12,799

1027

01:20:13,055 --> 01:20:15,104

1028

01:20:15,360 --> 01:20:16,384

1029

01:20:16,896 --> 01:20:18,944

1030

01:20:20,480 --> 01:20:25,856

Like pkk ,fetö Etc so you believe that

1031

01:20:26,112 --> 01:20:28,416

There's a problem and then you are

1032

01:20:28,928 --> 01:20:30,976

Trusting

1033

01:20:31,232 --> 01:20:32,256

one fact is

1034

01:20:33,280 --> 01:20:34,816

It starts with

1035

01:20:35,072 --> 01:20:36,608

Information leak

1036

01:20:38,144 --> 01:20:39,168

they get

1037

01:20:39,936 --> 01:20:40,960

a worker in the bank

1038

01:20:44,032 --> 01:20:45,056

1039

01:20:47,616 --> 01:20:48,384

To tell

1040

01:20:49,920 --> 01:20:52,480

Who get how much money yesterday

1041

01:20:55,040 --> 01:20:56,320

It is usually a

1042

01:20:56,576 --> 01:20:57,856

Unfortunate woman who has a

1043

01:20:59,648 --> 01:21:05,792

Relationship kind of man and at the end of the relationship she's threatened

1044

01:21:06,048 --> 01:21:07,328

And then

1045

01:21:07,840 --> 01:21:10,656

The guy asked certain customer information

1046

01:21:12,704 --> 01:21:14,752

such as who get how much money

1047

01:21:15,008 --> 01:21:16,032

Tell me about

1048

01:21:16,544 --> 01:21:22,688

Five customers who gets over 50,000 Turkish liras yesterday

1049

01:21:22,944 --> 01:21:24,480

And the poor woman

1050

01:21:24,736 --> 01:21:25,504

worker

1051

01:21:25,760 --> 01:21:29,600

Gives those names and information thinking that

1052

01:21:29,856 --> 01:21:31,648

Nothing's going to happen because

1053

01:21:33,952 --> 01:21:35,232

She's not involved

1054

01:21:35,488 --> 01:21:37,792

right

1055

01:21:39,328 --> 01:21:40,864

then the guy calls the person

1056

01:21:42,144 --> 01:21:44,448

The person indicating that

1057

01:21:45,216 --> 01:21:46,496

Pkk is

1058

01:21:47,264 --> 01:21:48,288

Ruining your

1059

01:21:48,800 --> 01:21:49,824

Bank account

1060

01:21:50,336 --> 01:21:51,872

As if you have received

1061

01:21:52,384 --> 01:21:55,968

51036 try yesterday from this person

1062

01:21:57,504 --> 01:22:03,648

You automatically start to believe that because no one else who can learn how much money you get

1063

01:22:03,904 --> 01:22:06,464

Okay so

1064

01:22:06,976 --> 01:22:13,120

That kind of belief is usually that kind of trust is usually started with some kind of private

1065

01:22:13,376 --> 01:22:16,192

Information that private information is given to you

1066

01:22:16,448 --> 01:22:17,984

And then you start believing

1067

01:22:19,520 --> 01:22:25,664

So that is what is called social engineering so after that they tell you to go to the

1068

01:22:25,920 --> 01:22:30,784

Trash bins and put the money in the back in track in the trash and you do it

1069

01:22:31,296 --> 01:22:37,440

Because you trust

1070

01:22:40,000 --> 01:22:41,024

Sometimes

1071

01:22:41,280 --> 01:22:43,584

Actually the word

1072

01:22:44,864 --> 01:22:45,632

Hacking

1073

01:22:46,144 --> 01:22:47,168

Is

1074

01:22:48,704 --> 01:22:52,032

Sometimes misused hacker is

1075

01:22:53,824 --> 01:22:57,152

Sometimes a good thing sometimes a bad thing hacker means

1076

01:22:58,944 --> 01:23:01,248

a very intimate

1077

01:23:01,760 --> 01:23:05,600

A person who has a very intimate knowledge about something

1078

01:23:06,368 --> 01:23:09,952

Very intimate and deep knowledge about some certainty and

1079

01:23:10,208 --> 01:23:12,768

He or she can use

1080

01:23:13,024 --> 01:23:15,072

The device or the software

1081

01:23:15,584 --> 01:23:16,608

In the way

1082

01:23:17,376 --> 01:23:19,424

That it is not intended.

1083

01:23:21,216 --> 01:23:22,752

Normally

1084

01:23:23,008 --> 01:23:27,872

I am using this phone to make my calls

1085

01:23:28,384 --> 01:23:30,688

Or send my emails Etc

1086

01:23:31,456 --> 01:23:32,736

But as a hacker

1087

01:23:33,504 --> 01:23:35,296

I can use this as a hand heater

1088

01:23:40,928 --> 01:23:44,512

1089

01:23:45,024 --> 01:23:45,792

1090

01:23:46,560 --> 01:23:47,072

So

1091

01:23:47,328 --> 01:23:49,632

That kind of activity is actually

1092

01:23:50,144 --> 01:23:52,960

Labeled as hacking using something

1093

01:23:53,728 --> 01:23:55,520

with a very deep knowledge

1094

01:23:56,032 --> 01:23:58,592

with a function

1095

01:23:59,104 --> 01:24:01,152

That is except basic functions

1096

01:24:02,688 --> 01:24:05,248

Such as calling numbers

1097

01:24:06,016 --> 01:24:07,296

Which is not possible

1098

01:24:08,320 --> 01:24:10,112

Normally

1099

01:24:10,624 --> 01:24:11,904

or

1100

01:24:12,160 --> 01:24:14,464

Going into certain

1101

01:24:14,720 --> 01:24:20,864

Web pages which is normally not available etc

1102

01:24:21,120 --> 01:24:24,192

so , those kind of activity is called as hacking.

1103

01:24:25,216 --> 01:24:29,312

Another example is,

1104

01:24:29,568 --> 01:24:33,152

modifying your bicycle so that it goes backwards

1105

01:24:33,920 --> 01:24:39,040

You can ride your bicycle backwards for example. it means you hacked your bicycle

1106

01:24:39,808 --> 01:24:43,904

so, it doesn't mean that it is bad all the time

1107

01:24:44,160 --> 01:24:44,672

But

1108

01:24:44,928 --> 01:24:46,464

It requires knowledge

1109

01:24:51,584 --> 01:24:52,096

So

1110

01:24:52,608 --> 01:24:57,984

as a hacker you can be "researcher penetration tester so security tester

1111

01:24:58,240 --> 01:25:01,312

Or Security Consultants", as you retire.

1112

01:25:02,592 --> 01:25:03,616

“Network Attacks” The Attacks. Listening Attacks.

1113

01:25:04,640 --> 01:25:09,248

1114

01:25:11,296 --> 01:25:12,576

Packet Sniffing 2 çeşidi var, aşağıda kırmızıyla işaretli.= So listening a text May result in passport sniffing,cookie stealing,session hijacking,information stealing .You authenticate to A bank They can steal your session So they continue After you As if you didn't log out That is one important thing so they still your session remaining Activite. “ **Sniffing attack** in context of [network security](https://en.wikipedia.org/wiki/Network_security), corresponds to [theft](https://en.wikipedia.org/wiki/Data_theft) or interception of data by capturing the [network traffic](https://en.wikipedia.org/wiki/Network_traffic) using a [packet sniffer](https://en.wikipedia.org/wiki/Packet_sniffer) (an application aimed at capturing [network packets](https://en.wikipedia.org/wiki/Network_packet)).  “

1115

01:25:12,832 --> 01:25:16,416

1116

01:25:16,

1125

01:25:41,504 --> 01:25:47,648

"Man-in-the-middle" means insert a router in the path between client and server, and change the packets as they pass through

1126

01:25:47,904 --> 01:25:49,696

"DNS hijacking" = insert malicious routes into DNS tables to send traffic for genuine sites to malicious sites. Need to know: Networking protocols ,routing,TCP-IP. (önemli . ) “Domain Name Server (DNS) hijacking, also named DNS redirection, is a type of DNS attack in which DNS queries are incorrectly resolved in order to unexpectedly redirect users to malicious sites. To perform the attack, perpetrators either install [malware on user computers](https://www.imperva.com/learn/application-security/malware-detection-and-removal/), take over routers, or intercept or hack DNS communication.

DNS hijacking can be used for [pharming](https://www.imperva.com/Resources/Glossary/pharming) (in this context, attackers typically display unwanted ads to generate revenue) or for [phishing](https://www.imperva.com/learn/application-security/phishing-attack-scam/) (displaying fake versions of sites users access and stealing data or credentials).” “ Some governments use DNS hijacking for censorship, redirecting users to government-authorized sites.”

1127

01:25:51,744 --> 01:25:53,024

1128

01:25:53,536 --> 01:25:59,680

1129

01:25:59,936 --> 01:26:04,288

1130

01:26:04,800 --> 01:26:08,384

knowledge is required to prevent this kind of attacks

1131

01:26:10,176 --> 01:26:14,272

that is important attack ("DNS hijacking" yanına yıldız koydu.)

1132

01:26:15,296 --> 01:26:19,648

"Web Attacks" 3 çeşittir aşağıda kırmızıyla belirttim

1133

01:26:20,160 --> 01:26:21,440

"Phishing attacks"

1134

01:26:22,464 --> 01:26:24,000

Phishing attacks

1135

01:26:24,768 --> 01:26:26,816

Website pretends that it is a "mibank.com" instead of "mybank.com" so they dont play with dns tables it is just garantibankasıcom.com.tr ( they take the domain garantibankasıcom.com) so on the webğpage it is a different web address, we call it as "phishing" .

1150

01:27:05,984 --> 01:27:08,288

Some users are

1151

01:27:09,312 --> 01:27:12,384

Accepting this and they also sent mail

1152

01:27:13,152 --> 01:27:15,968

To many people to thousands of people

1153

01:27:16,224 --> 01:27:19,040

indicating that you get some

1154

01:27:19,296 --> 01:27:21,856

Money from the bank or you need to

1155

01:27:22,880 --> 01:27:24,928

reenter your password again

1156

01:27:25,440 --> 01:27:27,232

To the bank to validate

1157

01:27:27,488 --> 01:27:29,792

Or you have some you have some

1158

01:27:30,304 --> 01:27:32,608

Payments remaining

1159

01:27:32,864 --> 01:27:33,632

To pay

1160

01:27:34,144 --> 01:27:36,448

You believe the mail and then

1161

01:27:37,216 --> 01:27:37,984

you go there

1162

01:27:40,288 --> 01:27:46,176

Now an evil person has your information to get your money or get your information

1163

01:27:46,432 --> 01:27:46,944

Or

1165

01:27:53,088 --> 01:27:56,928

it may be Twitter Facebook or maybe social media accounts as well

1166

01:27:57,952 --> 01:28:01,280

They want to do something bad they want to harass a person

1167

01:28:01,536 --> 01:28:02,816

And they can use your

1168

01:28:03,328 --> 01:28:04,096

Account

1169

01:28:05,888 --> 01:28:09,216

Or you may sell your accounts for $250

1170

01:28:10,496 --> 01:28:16,640

And report it as stolen after 2 hours in 2 hours they can arrest the person that's another

1171

01:28:16,896 --> 01:28:19,200

Possibility

1172

01:28:22,784 --> 01:28:27,904

So real people may sell their accounts or phone numbers

1173

01:28:28,416 --> 01:28:34,560

and report it as stolen after few hours with consent.

1174

01:28:34,816 --> 01:28:40,192

"SQL injection"

1175

01:28:41,728 --> 01:28:43,776

it Has been very famous

1176

01:28:45,568 --> 01:28:48,128

web pages are

1177

01:28:50,432 --> 01:28:51,712

Containing active

1178

01:28:52,992 --> 01:28:56,320

Code that changes the database

1179

01:28:57,600 --> 01:29:00,416

If the penetrator if the

1180

01:29:00,928 --> 01:29:01,696

Person

1181

01:29:01,952 --> 01:29:07,328

Can find a way to send a string so that string becomes a command

1182

01:29:07,840 --> 01:29:10,144

of the database system

1183

01:29:10,400 --> 01:29:12,448

That comment can work like

1185

01:29:20,640 --> 01:29:22,688

Something bad

1186

01:29:23,456 --> 01:29:28,576

In the database system I'm going to show an example that was a famous picture on that

1190

01:30:07,744 --> 01:30:09,536

Okay this is one

1191

01:30:10,560 --> 01:30:13,120

This is one example

1192

01:30:15,168 --> 01:30:17,984

The guy is trying to hack

1194

01:30:24,128 --> 01:30:26,432

License plate recognition system

1195

01:30:26,944 --> 01:30:28,224

By feeding a data that may work as a comment

1198

01:30:33,600 --> 01:30:34,368

In the system

1199

01:30:36,416 --> 01:30:38,720

This has been a big vulnerability

1200

01:30:39,488 --> 01:30:40,512

In the past.

1201

01:30:41,024 --> 01:30:42,816

Today it is also

1202

01:30:44,352 --> 01:30:46,912

Possible to have this kind of vulnerabilities

1203

01:30:47,168 --> 01:30:50,496

So make sure that always make sure that

1204

01:30:50,752 --> 01:30:53,056

The data that you are entering to system

1205

01:30:53,312 --> 01:30:56,128

Does not contain and cannot contain commands

1206

01:30:57,664 --> 01:30:58,432

Because

1207

01:30:58,688 --> 01:30:59,968

Somebody else

1208

01:31:00,224 --> 01:31:00,992

may give a comment instead of licence plate as the input

1212

01:31:15,072 --> 01:31:16,864

this was a problem in databases. Another database comment may cause problem in the licence plate recognition system

1221

01:32:33,408 --> 01:32:33,920

so, this is what "SQL Injection" was.

1222

01:32:36,480 --> 01:32:37,248

"Cross Site Scripting” usually happens with the

1225

01:33:08,224 --> 01:33:13,344

happens with the advertisement

1226

01:33:13,600 --> 01:33:19,744

A malicious advertisement so that must be checked by the advertising company significantly

1227

01:33:20,000 --> 01:33:21,280

also When you are using libraries

1228

01:33:22,304 --> 01:33:27,680

We are using a lot of codes for a lot of different places.So, those code may contain certain unnecessary part that is gathering information or inserting advertisement you should be very careful on that.

1232

01:33:41,760 --> 01:33:46,368

"The Virus" . Virus is a code.

1233

01:33:49,696 --> 01:33:50,464

in the

1234

01:33:51,232 --> 01:33:51,744

Program

1235

01:33:56,352 --> 01:33:58,144

If your program is

1236

01:34:05,056 --> 01:34:07,616

4200 KB

1237

01:34:11,456 --> 01:34:13,248

And your viruses

1238

01:34:18,368 --> 01:34:19,904

300 KB

1239

01:34:21,184 --> 01:34:23,232

What is the size of the

1240

01:34:23,744 --> 01:34:24,256

code

1241

01:34:25,024 --> 01:34:25,792

If your

1242

01:34:27,840 --> 01:34:29,120

code is infected

1243

01:34:30,400 --> 01:34:31,936

4500

1244

01:34:32,192 --> 01:34:32,960

Probably.

1245

01:34:34,240 --> 01:34:35,776

That is one way of detecting it

1246

01:34:36,544 --> 01:34:37,056

But

1247

01:34:37,312 --> 01:34:38,848

The virus Maybe

1248

01:34:39,360 --> 01:34:41,408

Erasing certain

1249

01:34:41,920 --> 01:34:43,456

Less used parts

1250

01:34:43,968 --> 01:34:44,736

In the code

1251

01:34:47,296 --> 01:34:48,064

So that

1252

01:34:48,576 --> 01:34:49,856

it is still

1253

01:34:50,112 --> 01:34:52,672

4200

1254

01:34:54,976 --> 01:34:56,000

so size may for an intelligence virus. Size may stay the same.

1256

01:35:01,120 --> 01:35:03,168

So what else do you need to check

1257

01:35:04,448 --> 01:35:05,472

You need to check

1258

01:35:09,824 --> 01:35:11,360

the Added values of

1259

01:35:11,872 --> 01:35:13,152

Individual bites

1260

01:35:13,664 --> 01:35:14,944

Which is called checksum

1261

01:35:16,224 --> 01:35:17,504

or CRC

1262

01:35:19,040 --> 01:35:20,064

so that the code

1263

01:35:21,088 --> 01:35:22,368

originally

1264

01:35:23,648 --> 01:35:26,720

For example if you add all the bites in the code.

1265

01:35:28,000 --> 01:35:29,280

and obtain a number

1266

01:35:29,536 --> 01:35:31,072

That number is unique

1267

01:35:31,584 --> 01:35:34,400

for a different code even if the total sizes the same

1268

01:35:35,168 --> 01:35:37,984

you will get the different code different

1269

01:35:38,752 --> 01:35:40,544

Number because

1270

01:35:40,800 --> 01:35:42,080

The content

1271

01:35:43,104 --> 01:35:44,896

Content will be a different value

1272

01:35:45,664 --> 01:35:47,456

for Different various code

1273

01:35:48,480 --> 01:35:49,760

therefore ,

1274

01:35:51,040 --> 01:35:52,064

CRC

1275

01:35:54,112 --> 01:35:56,672

Cyclic redundancy code CRC

1276

01:35:57,696 --> 01:35:58,720

or "checksum"

1277

01:35:58,976 --> 01:36:01,536

Techniques

1278

01:36:02,304 --> 01:36:03,328

help to

1279

01:36:03,840 --> 01:36:04,864

Preserve

1280

01:36:05,888 --> 01:36:07,936

Original binary codes

1281

01:36:08,192 --> 01:36:08,960

from

1282

01:36:10,240 --> 01:36:11,520

Being infected

1283

01:36:11,776 --> 01:36:15,360

The code you download from certain sites

1284

01:36:15,616 --> 01:36:17,152

Especially free codes, you download from free sites

may contain

1286

01:36:21,248 --> 01:36:22,272

Malicious code

1287

01:36:22,528 --> 01:36:23,552

added on them

1288

01:36:23,808 --> 01:36:25,344

Such as

1289

01:36:25,600 --> 01:36:28,160

Mining tool such as free muzik tools, anything that contains free something

1292

01:36:36,096 --> 01:36:37,120

Is usually

1293

01:36:38,400 --> 01:36:40,960

has Additional code insides

1294

01:36:41,216 --> 01:36:42,240

such as a Photoshop

1295

01:36:43,776 --> 01:36:45,312

Download site

1296

01:36:45,824 --> 01:36:48,128

But it's free so why is this free

1297

01:36:49,408 --> 01:36:52,224

there is a code inside in addition to the Photoshop

1298

01:36:52,736 --> 01:36:54,016

There's an additional code

1299

01:36:54,784 --> 01:36:58,368

That tracks your activity maybe track you

1300

01:36:59,648 --> 01:37:00,416

Keyboard

1301

01:37:01,440 --> 01:37:03,744

So that captures all the information

1302

01:37:04,000 --> 01:37:06,560

I sent back to China

1303

01:37:06,816 --> 01:37:12,960

russia or whatever why do we say China or Russia because those countries are less accessible

1304

01:37:13,216 --> 01:37:18,592

through Legal system and something happens,you cannot penetrate

1305

01:37:18,848 --> 01:37:24,992

through the country.

1315

01:38:37,696 --> 01:38:40,512

Also

1316

01:38:41,280 --> 01:38:46,400

Virus is malicious

1317

01:38:51,008 --> 01:38:54,080

If it is malicious we call it as virus but

1318

01:38:55,616 --> 01:38:57,408

Sometimes it is

1319

01:38:57,664 --> 01:38:58,432

On purpose

1320

01:38:59,200 --> 01:39:00,736

such as the virus for

1321

01:39:00,992 --> 01:39:01,504

Iraq

1322

01:39:02,272 --> 01:39:03,552

there is a Virus but harmless,

1324

01:39:05,600 --> 01:39:08,160

It is only harmful when activated

1325

01:39:08,416 --> 01:39:11,488

In very limited certain cases

1326

01:39:12,512 --> 01:39:16,352

Or the virus tries to collect information from you

1327

01:39:16,864 --> 01:39:17,632

Such as

1328

01:39:18,144 --> 01:39:20,960

Your age and shoe size

1329

01:39:22,496 --> 01:39:23,520

For business purposes

1330

01:39:23,776 --> 01:39:24,800

It's Virus

1331

01:39:26,592 --> 01:39:30,944

It is propagating it replicates itself that's important

1332

01:39:32,224 --> 01:39:33,504

It is infecting

1333

01:39:34,016 --> 01:39:40,160

Continuously During certain operations

1334

01:39:40,416 --> 01:39:40,928

but

1335

01:39:41,952 --> 01:39:42,976

It has no harm

1336

01:39:43,488 --> 01:39:45,792

For many that can happen

1337

01:39:48,608 --> 01:39:52,704

"infection" is actually copying itself so

1338

01:39:52,960 --> 01:39:54,240

When you start

1339

01:39:54,496 --> 01:39:57,312

This application then you start Photoshop

1340

01:39:59,104 --> 01:40:00,128

Photoshop starts

1341

01:40:01,664 --> 01:40:06,528

when you select print for example when you select print in the Photoshop

1342

01:40:07,040 --> 01:40:07,808

First (Infection (targets/carriers)= executable files, boot sectors, documents(macros),scripts(webpages), etc. )

1343

01:40:08,064 --> 01:40:09,856

Virus code is activated

1344

01:40:10,112 --> 01:40:11,904

then print is Activated

1345

01:40:12,928 --> 01:40:13,696

In the function

1346

01:40:14,976 --> 01:40:16,000

So

1347

01:40:16,256 --> 01:40:20,096

When you print something virus code is activated and virus code does what

1348

01:40:20,608 --> 01:40:25,216

Looks for the directory books for another application tries to copy itself

1349

01:40:26,240 --> 01:40:28,800

when it tries to copy itself , it copies itself

1350

01:40:29,568 --> 01:40:31,104

then execute print

1351

01:40:31,360 --> 01:40:32,128

What happened?

1352

01:40:32,896 --> 01:40:33,664

Infected.

1353

01:40:35,712 --> 01:40:40,064

Infected another application. so that application for example Microsoft Word

1354

01:40:40,320 --> 01:40:42,624

when you click on Microsoft Word

1355

01:40:43,904 --> 01:40:45,440

it is infected no problem

1356

01:40:45,696 --> 01:40:47,488

when you click on print

1357

01:40:48,256 --> 01:40:51,072

it Tries to infect other applications.

1358

01:40:54,912 --> 01:40:56,704

So that is one way of passing infections.

1359

01:41:00,288 --> 01:41:01,568

Second, through disc locations.One of them is"boot sectors."

1360

01:41:01,824 --> 01:41:02,848

so, when you start your machine, small piece of code in the boot sector is executed.

1370

01:41:23,072 --> 01:41:24,864

So if you write something there

1371

01:41:25,120 --> 01:41:26,144

as a malicious code

1372

01:41:26,912 --> 01:41:30,752

You know that it is always executed before operating system starts

1373

01:41:31,776 --> 01:41:33,568

Just right there

1374

01:41:35,360 --> 01:41:36,384

It's a boot Virus.

1375

01:41:37,408 --> 01:41:40,224

it will Execute whenever you start your machine

1376

01:41:42,272 --> 01:41:45,344

Provided that you have you have the ability to

1377

01:41:46,624 --> 01:41:47,392

write to that location

1378

01:41:47,648 --> 01:41:51,744

So you need to have administrative privileges.

1379

01:41:52,000 --> 01:41:53,792

therefore you should not run your applications with administrative privileges, bc administrative privileges can accesss certain places that may otherwise be unaccessible by regular users so if you are executing an infected application as an administrative for example,

an application that is downloaded from internet in an unknown site. And if you run it as a user mode, you will get certain errors, indicating that the program is trying to run as an administrator to infect the system.

1395

01:42:43,200 --> 01:42:49,344

and Microsoft Excel word, there are "macros" (documents) internal programs off

1396

01:42:51,392 --> 01:42:55,488

Certain applications can contain viruses so each

1397

01:42:55,744 --> 01:43:01,888

Each complex program like Microsoft Excel is a programming platform as well ,so, that programming platform

1398

01:43:03,168 --> 01:43:07,776

Allows you to write your own programs in documents so whenever you open the document,

1399

01:43:08,032 --> 01:43:10,592

The program runs

1400

01:43:11,872 --> 01:43:14,688

That may contain virus and

1401

01:43:15,712 --> 01:43:17,504

Infect other documents

1402

01:43:17,760 --> 01:43:23,904

Can copy itself other documents that you can open because you are allowed to open other documents

1403

01:43:24,160 --> 01:43:30,304

as Ahmet Mehmet etc.

1404

01:43:30,560 --> 01:43:35,168

Therefore, "Propagation" is initiated by user . “But a virus **can only propagate if it the application or code on which it resides is executed by the user** – that is, you. “ propagate=yaymak,üremek.

1405

01:43:35,424 --> 01:43:39,264

If the user is working as admin user

1406

01:43:40,032 --> 01:43:42,080

it can propogate to everybody

1407

01:43:42,592 --> 01:43:47,200

On the system.

Altını çizdiği cümle(Propagation başlığının altında) = The mechanisms are storage elements, mails, downloaded files or shared folders.

1410

01:44:27,904 --> 01:44:30,208

"Worm" Does not require user to print

1411

01:44:31,744 --> 01:44:32,768

Select the print mechanism

1413

01:44:35,584 --> 01:44:41,728

"It automatically reproduces itself over the network it doesn't need user intervention to propagate"

1414

01:44:41,984 --> 01:44:44,032

So it is more otonom(autonomous) then

1415

01:44:44,544 --> 01:44:45,312

the virus.

1416

01:44:45,568 --> 01:44:46,848

virus requires

1417

01:44:47,872 --> 01:44:49,152

An application

1418

01:44:49,408 --> 01:44:50,176

"Worm" is

1419

01:44:50,432 --> 01:44:52,224

More autonomous.

1420

01:44:52,992 --> 01:44:59,136

The infection of applications are done through "buffer overflowing" "file sharing"

"configuration errors" and other vulnerabilities. So there are many ways.

I'm going to come back to "buffer overflowing". is very interesting fact

and when we are doing Assembly programming at the beginning of the semester I have talked about "buffer overflow" little bit

1426

01:45:18,592 --> 01:45:22,176

You are passing information between

1427

01:45:22,432 --> 01:45:24,480

Function in the main program

1428

01:45:24,736 --> 01:45:26,528

through assembly stack

1429

01:45:26,784 --> 01:45:29,344

Then if the data is too big

1430

01:45:30,112 --> 01:45:33,184

Your data space may go into

1431

01:45:34,208 --> 01:45:35,488

Application space

1432

01:45:36,256 --> 01:45:38,048

So if you feed

1433

01:45:38,560 --> 01:45:40,608

Too many virus code

1434

01:45:41,120 --> 01:45:42,144

as a data,

1435

01:45:42,400 --> 01:45:45,728

that data space gets bigger bigger bigger and hit the

1436

01:45:47,264 --> 01:45:48,544

Application area

1437

01:45:48,800 --> 01:45:50,336

and the function returns

1438

01:45:50,592 --> 01:45:56,736

Sometime later it will try to execute those locations but those locations now containing

virus code.

So, this is what we call "buffer overflow".

1442

01:46:03,392 --> 01:46:09,280

Normally buffer size should be controlled by checking the size of the input

1443

01:46:10,048 --> 01:46:13,632

You should always check the size of the input in your programs

1444

01:46:14,400 --> 01:46:15,936

So that if it is too big

1445

01:46:17,984 --> 01:46:20,288

it may Expand your regular space and

1446

01:46:20,800 --> 01:46:21,824

Attached to

1447

01:46:23,616 --> 01:46:24,896

real user program can be infected.

1450

01:46:36,160 --> 01:46:37,440

Any kind of

1451

01:46:37,952 --> 01:46:39,488

Activity can be done through "worms" = "Target selection algorithm o Email addresses,DNS,IP,network neighborhood"

1452

01:46:39,744 --> 01:46:40,512

1453

01:46:41,792 --> 01:46:45,888

And the worm may contain malicious programs: 2 çeşittir : "backdoor"

1454

01:46:46,144 --> 01:46:49,472

"DDOS agent" , "backdoor" means

1455

01:46:55,616 --> 01:46:57,408

they insert a piece of code that allows hackers to enter later.

1458

01:47:02,528 --> 01:47:04,320

Maybe next year maybe never

1459

01:47:05,600 --> 01:47:07,648

but the worm Reproduce itself it

1460

01:47:08,160 --> 01:47:09,440

Opens the gate

1461

01:47:09,952 --> 01:47:10,976

Gives the key to

1462

01:47:11,232 --> 01:47:13,024

hackers and hackers keep the key.

1463

01:47:13,792 --> 01:47:17,376

sometimes they sell it to each other.

1464

01:47:21,984 --> 01:47:24,544

That is what "Backdoor" is.

1465

01:47:25,568 --> 01:47:29,152

"Trojan" = "A trojan is a software that seems useful or benign(iyi huylu,tehlikesiz), but is actually hiding a malicious functionality."

1466

01:47:29,664 --> 01:47:35,040

so you inserted yourself

1467

01:47:35,296 --> 01:47:37,088

With your own hands

1468

01:47:37,344 --> 01:47:39,392

but actually it is a bad code.

1469

01:47:40,160 --> 01:47:43,232

you think that it is something useful

1470

01:47:44,000 --> 01:47:45,792

"Backdoor" means ,

1471

01:47:46,048 --> 01:47:52,192

black-hacker places the back door so that he can access

1472

01:47:52,448 --> 01:47:53,472

the system later.

1473

01:47:59,360 --> 01:48:00,128

"Rootkits"

1474

01:48:04,224 --> 01:48:10,368

are like backdoor and Trojan horses but also modify existing programs.

1475

01:48:10,624 --> 01:48:12,160

so virus and trojan together. Programs in the operating system allows a black-hacker to control the system without being detected. A rootkit can be in user-mode or kernel-mode.

so,

1478

01:48:21,888 --> 01:48:22,912

You cannot detect

1479

01:48:23,168 --> 01:48:25,472

"Rootkits" very easily

1480

01:48:25,984 --> 01:48:29,568

Because it also modifies existing programs in the operating system

1482

01:48:35,712 --> 01:48:39,040

Social Engineering = So this is pkk issue.

1483

01:48:42,112 --> 01:48:43,136

are we that crazy? answer is yes.

1485

01:48:46,720 --> 01:48:49,280

How do I protect ourselves?

1486

01:48:49,536 --> 01:48:50,560

Basically

1487

01:48:51,072 --> 01:48:54,144

Creating passwords that is hard to guess

1488

01:48:54,656 --> 01:48:58,240

And working with passwords all the time

1489

01:48:58,496 --> 01:49:01,568

never using same passwords

1490

01:49:02,080 --> 01:49:02,848

In

1491

01:49:04,384 --> 01:49:06,432

Different places

1492

01:49:07,712 --> 01:49:08,992

I, use myself

1493

01:49:09,248 --> 01:49:15,392

Use certain type of passwords in certain places

1494

01:49:15,648 --> 01:49:16,160

but other type of passwords in other places .

1495

01:49:17,184 --> 01:49:19,232

So secondary places like

1496

01:49:21,024 --> 01:49:27,168

School account Etc is usually have different

1497

01:49:27,424 --> 01:49:33,568

System of generation

bank accounts have different system of generations. so, if they catch my school account, they cannot catch my bank account since they are different and system of generation is also different

"Password Attacks", "Password Guessing": = ineffective except in targeted cases. “Dictionary Attacks” = Password are stored in computers as hashes, and these hashes can sometimes get exposed to check all known words with the stored hashes.

if you have easy passwords,

1504

01:50:28,096 --> 01:50:28,864

That's a threat

1505

01:50:29,888 --> 01:50:30,656

Sometimes

1506

01:50:30,912 --> 01:50:32,448

Hackers try to

1507

01:50:35,776 --> 01:50:36,544

Try

1508

01:50:36,800 --> 01:50:37,824

a lot of

1509

01:50:38,336 --> 01:50:39,616

Well-known passports for

1510

01:50:42,688 --> 01:50:48,576

Entering the system so in order to stop that after 5 trials you need to

1511

01:50:48,832 --> 01:50:51,392

Modify your system to wait 5 minutes

1512

01:50:51,648 --> 01:50:56,768

So the attacker cannot try multiple passwords very frequently

1513

01:50:57,280 --> 01:50:58,560

So you should slow down

1514

01:50:58,816 --> 01:50:59,840

an attacker

1515

01:51:00,096 --> 01:51:06,240

For preventing multiple trials, one after another one after another..

1516

01:51:06,496 --> 01:51:12,384

So after three trials, after three failures usually systems wait for 5 minutes

1517

01:51:12,640 --> 01:51:15,712

That is for the "dictionary attacks"

1518

01:51:20,320 --> 01:51:26,464

"Rainbow Tables" = "Trade off storage and computation - uses a large number of pre-computed hashes without having a dictionary"

such as "14 character alphanumeric passwords are found in about 4-10 minutes of computing using a 1GB rainbow table.

1523

01:51:42,848 --> 01:51:45,152

so, it is like Bitcoin mining

1524

01:51:45,408 --> 01:51:46,944

Normally when you have a

1525

01:51:49,248 --> 01:51:52,320

If your passport is Ali for example,

1526

01:51:53,344 --> 01:51:54,624

Your password is Ali

1527

01:51:56,160 --> 01:51:57,440

It is converted with an algoritm

1528

01:52:00,768 --> 01:52:01,792

Such as RS8 to yw8

1531

01:52:12,032 --> 01:52:12,544

So

1532

01:52:13,056 --> 01:52:16,384

Rainbow table contains these (yw8'i gösteriyor).

1533

01:52:18,432 --> 01:52:19,200

rather than Passwords.

1534

01:52:19,968 --> 01:52:21,504

they check against this.

1535

01:52:26,368 --> 01:52:27,904

Sometimes they catch

1536

01:52:28,160 --> 01:52:28,928

the password.

1537

01:52:32,256 --> 01:52:34,560

Sometimes they catch the password

1538

01:52:35,072 --> 01:52:36,096

therefore

1539

01:52:36,608 --> 01:52:38,144

They don't have

1540

01:52:38,656 --> 01:52:40,704

Dictionary but they use

1541

01:52:40,960 --> 01:52:44,032

a large number of "pre-computed hashes" without having a dictionary

1542

01:52:46,080 --> 01:52:52,224

It's like reverse trying.

1543

01:52:52,480 --> 01:52:58,624

Let's stop here