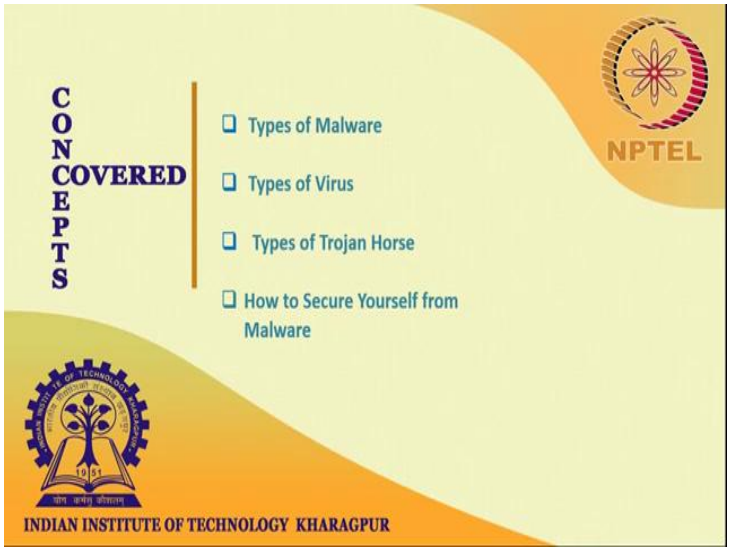
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 43
Malware

(Refer Slide Time: 00:21)

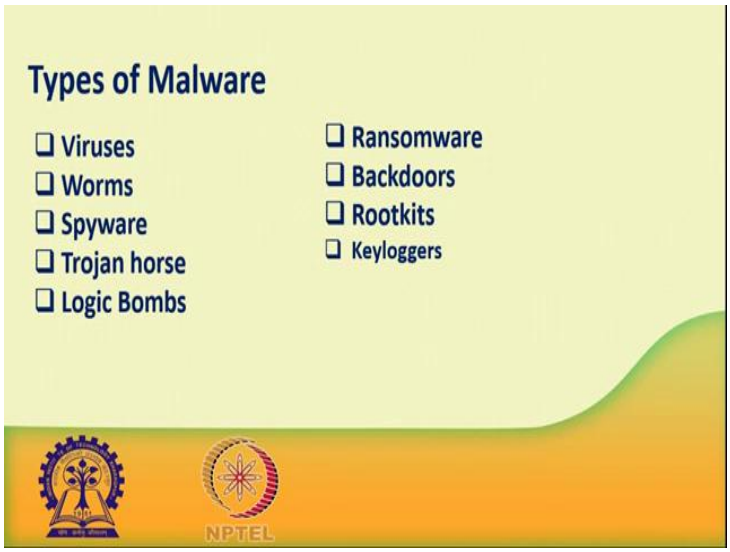


In this session, we will discuss about Malware. And we will cover the following topic, types of malware, types of virus, types of Trojan horse. How to secure yourself from malware? Malware or malicious software is an umbrella term that describe any malicious program or code that is harmful to systems. Hostile intrusive and intentionally nasty malware seeks to invade damage or disable computers.

Computer system networks tablet and mobile device often by taking partial control over device operations, like the human flu it interferes with normal function. Malware is all about making money although; malware cannot damage the physical hardware of system or network equipment. It can steal, encrypt or delete your data alter or hijack core computer functions and spy on your computer activity without your knowledge or permission.

Malware is a program designed to gain access to computer system normally, for the benefit of some third party without the user's permission. Malware includes computer viruses, worms, Trojan horse, ransomware, spyware and other malicious programs.

(Refer Slide Time: 02:01)



Now, types of malware: Viruses. Now virus is a malicious executable code attached to another executable file. The virus spread when an infected file is passed from system to system. Virus can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other program on the computer.

Worms: Worms replicate themselves on the system attaching themselves to different files and looking for pathways between computers such as, computer network that shares common file storage areas. Worms usually slowdown networks. A virus needs a host program to run but worms can run by themselves. After a worm affects the host, it is able to spread very quickly over the network.

Spyware, its purpose is to steal private information from a computer system for a third party. Spyware collects information and send it to the hacker. Trojan horse: a Trojan horse is malware that carries out malicious operations under the appearance of a desired operation, such as playing and online game. A Trojan horse varies from a virus because that Trojan burying itself to non executable files such as image files, audio files.

Logic bombs: A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer. Cyber security specialist recently discovered logic bomb that attack and

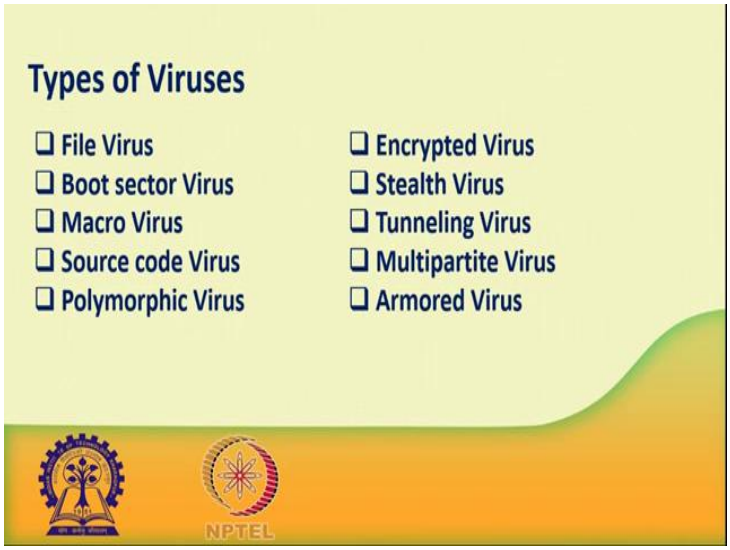
destroy the hardware component in a workstation or server including the cooling fans hard drives and power supplies.

The logic bomb overdrives these devices until they overheat or fail. Ransomware: ransomware grabs the computer system or the data it contains until the victim makes a payment. Ransomware encrypt data in the computer with the key which is unknown to the user. The user has to pay a ransom amount to the criminal to retrieve data. Once the amount is paid, the victim can resume using his or her system.

Back doors: A backdoor bypass the usual authentication used to access a system. The purpose of the backdoor is to grant the cyber criminal future access to the system. Even if the organisation fixes the original vulnerability used to attack the system. Rootkits: A rootkit modifies the operating system to make a backdoor. Attackers then use the backdoor to access the computer distantly.

Most rootkits take advantage of software vulnerabilities to modify system files. Keyloggers: Keyloggers records everything the user type on his or her computer system, to obtain password and other sensitive information and send them to the source of the key logging programme.

(Refer Slide Time: 06:05)



Viruses: A virus is a fragment of code embedded in a legitimate program. Viruses are self replicating and a design to infect other programs. They can work havoc in a system

by modifying or destroying files causing system cache and program malfunctions. There are various types of virus are there. File virus, this type of virus infects the system by appending itself to the end of a file.

It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed. It is also called parasitic virus, because it leaves no file intact, but also leaves the host functional. Boot sector virus: It infects the boot sector of the system executing every time system is booted.

Executing every time system is booted and before operating system is loaded, it infects other bootable media like floppy disc. These are also known as memory virus as they do not infect file system. Macro virus, unlike most virus which are written in low level language, these are written in high level language like visual basic. These viruses are triggered when a program capable of executing a macro is run.

For example, macro virus can be contained in spreadsheet files. Source code virus, it looks for source code and modifies it to include virus and to help spread it. Polymorphic virus, a virus signature is a pattern that can identify a virus. So, in order to avoid detection by antivirus, a polymorphic virus change each time it is installed. The functionality of virus remain same, but it signature is changed.

Encrypted virus in order to avoid detection by antivirus. This type of viruses exist in encrypted form. It carries a description algorithm along with it so the virus first decrypt and then execute. Stealth virus it is a very tricky virus as it changes the code that can be used to detect it. Steals the detection of virus becomes very difficult. For example, it can change the read system call, such that whenever user ask to read a code modified by the virus the original form of code is shown rather than infected code.

Tunnelling virus, these virus attempts to bypass detection any antivirus scanner, by installing itself in the interrupt handler chain interception programs which remain in the background of an operating system and catch viruses become disabled during the course of a tunnelling virus. Similar viruses install them self in device strips.

Multipartite virus, these type of virus is able to infect multiple parts of a system including boot sector, memory and files. This makes too difficult, to detect and contain.

Armoured virus, an armoured virus is coded to make a difficult for antivirus to unravel and understand. It uses a variety of technique to do so. Like, fully antivirus to believe that it lies somewhere else then its real location for using compression to complicate its code.

(Refer Slide Time: 10:34)

Trojan horse: The Trojan horse is not just a single type of virus. Its also varies to its purpose. The cyber criminal can target a specific person or disseminates the Trojan horse of his choice everywhere. This list will make you understand the different type of Trojan horse backdoor. It gives malicious user remote access over the infected computer. They can do whatever they want such as sending, receiving, launching and deleting files, displaying data and rebooting the endpoint.

Exploit, it contains data or code that abuse a vulnerability with an application software that is operating on your end point. Rootkit, these are designed to hide certain objects or activities in your system. This can effectively prevent malicious programs being detected. Trojan banker, its purpose is to steal your account data for online banking system, e-payment system and credit or debit card.

Trojan DDoS, these Trojan can start up the denial of service attack. Not only it can affect end points but also websites, by sending multiple request from your computer and several other infected computers. Trojan downloader, Trojan downloader can download

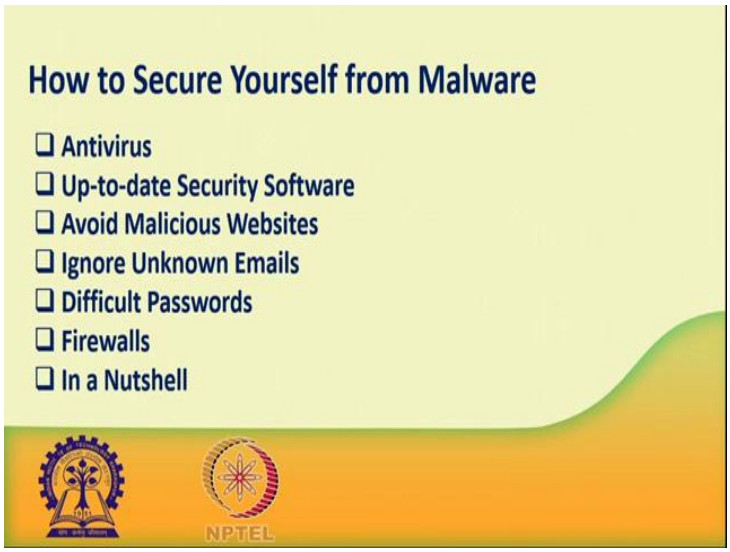
and install new version of malicious program onto your computer including Trojan and adware.

Trojan dropper, Trojan fake antivirus program copies the activities of antivirus software. They are created to extort money from you in return, they will remove the detection and threat removal, even though the threat that they report are do not actually exist. Trojan game thief if you are into gaming, you know that online gaming can also steal cash from him. Cyber criminal also crafted this Trojan virus which steal user account information from online games.

Trojan ransom, this Trojan can change data on your end point. This can lead to endpoint malfunction. The cyber criminal will demand a ransom. They will only replace your computers performance or unblock your data after you have paid them. Trojan is SMS, Trojan SMS, this Trojan can change data on your end point. This can lead to endpoint malfunction.

The cyber criminal will demand a ransom. They will only replace your computer's performance or unblock your data after you have paid them. Trojan SMS, this Trojan can be changed on your end point. This Trojan can be spread through SMS. Trojan spy, Trojan spy program can spy on how you are using your computer. For example, by tracking the data you enter in your keyboard, taking screenshot or getting a list of running applications. Trojan mailfinder, these robes email addresses from your end point.

(Refer Slide Time: 14:29)



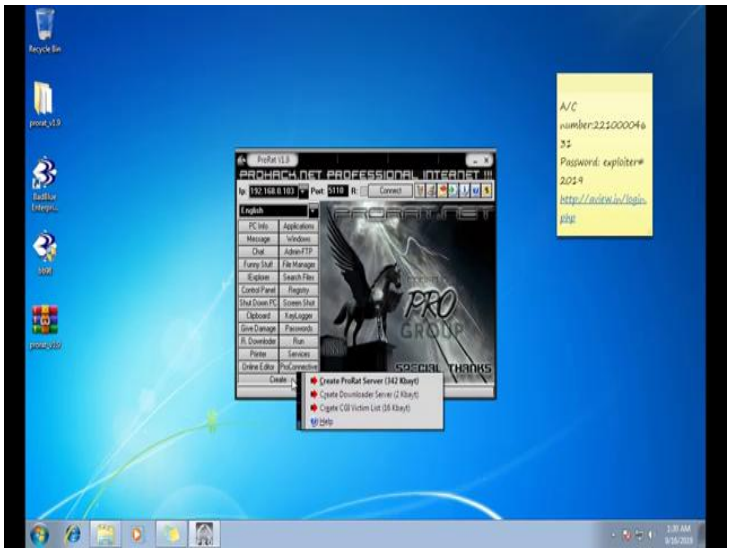
Now, the question is that how to secure yourself from Trojan horse? Here is a guide to prevent your system for malware. Antiviruses, you can use antiviruses to prevent your system from Trojan horse. A effective antivirus can alert you when there is a suspicious file on your end point. You can start using free branded antivirus offered in the Internet, up to date security software. What is the use of antivirus when it is outdated?.

Update that, when the updates are ready, it will update the software for better virus mitigation; avoid malicious websites. This spread the danger among the community of Internet users. Malicious websites mostly have popup messages that can trick you better stay out of trouble. Ignore unknown emails. When you receive an email from an unknown sender, you can just ignore them and delete them. Trojan also take the form of an email attachment.

Difficult passwords confuse your enemies. Your difficult creative password can save you from a big mess. Firewall, a firewall monitors and controls incoming and outgoing network traffic on a standardized security rule. This another protection for your own defence. In a nutshell, Trojan horse viruses can act various reset task by a cyber criminal. It is better to know, which Trojan horse virus you might encounter to prepare a security plan. Never cybercriminals take advantage of the things you work hard for.

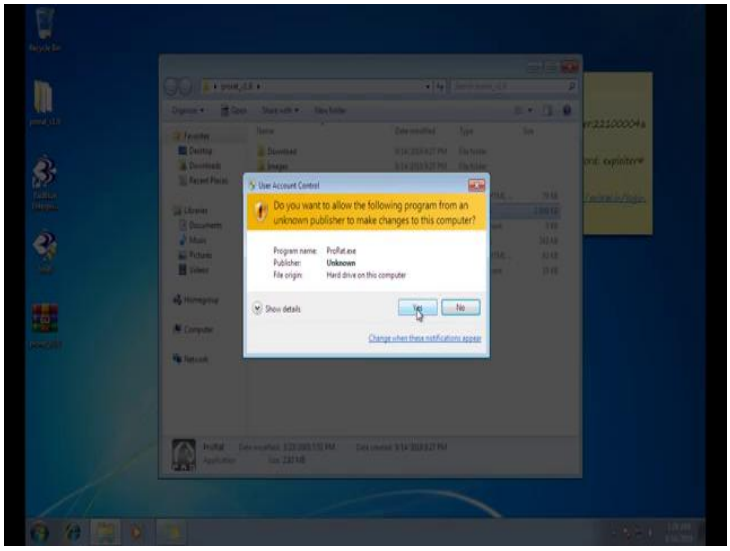
Thank you.

(Refer Slide Time: 16:34)



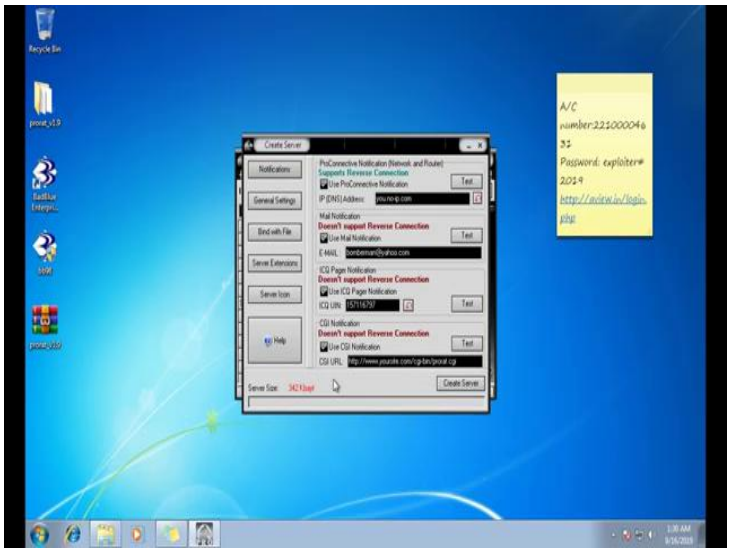
In this session, I will show you a RAT, remote administrative tool to compromise a victim system. So, now, consider our target system IP address is 192.168.0.106. Now I am using ProRat.

(Refer Slide Time: 17:12)



So, here is my ProRat and open the tool ProRat.

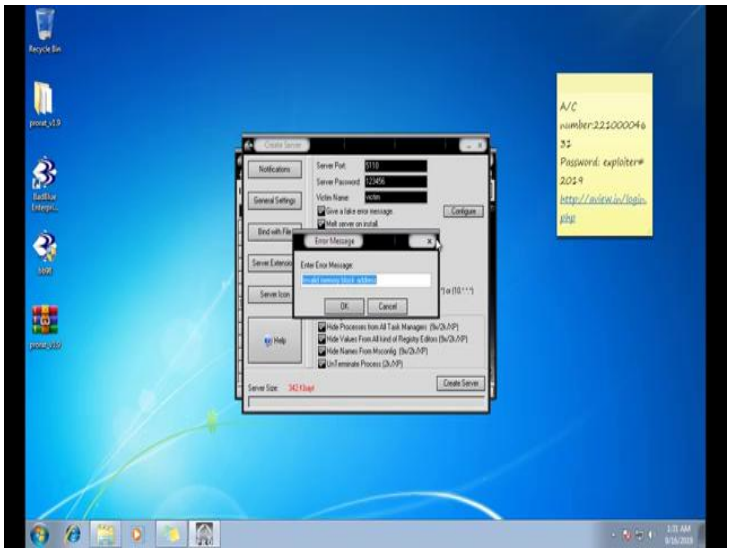
(Refer Slide Time: 17:31)



So, every remote administrative tool have two parts. One is the client part and another one is the server part. So, in attacker machine, the client part is running and in the victim machine we need to run the server part. And after executing the server part in the victim machine, it will connect with the client part which is running in the attacker machine. So, now, we need to create the server part.

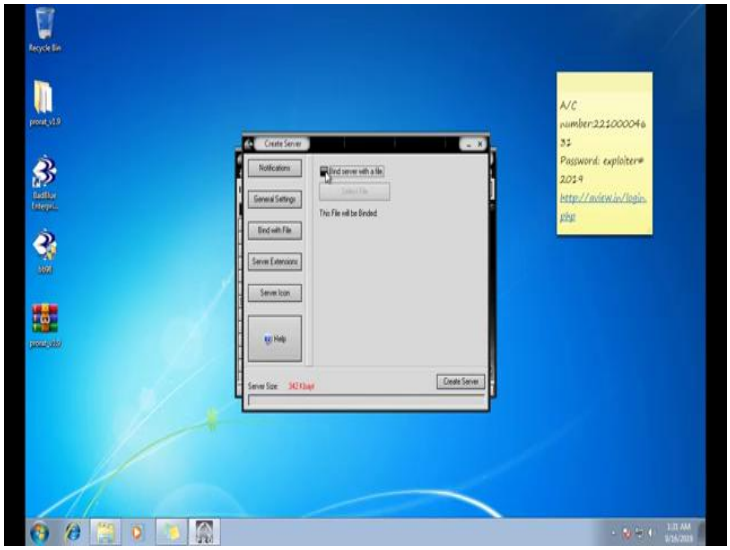
So, go to create and then create product server. Now, there are some settings like notification. So, notification details is here.

(Refer Slide Time: 18:38)



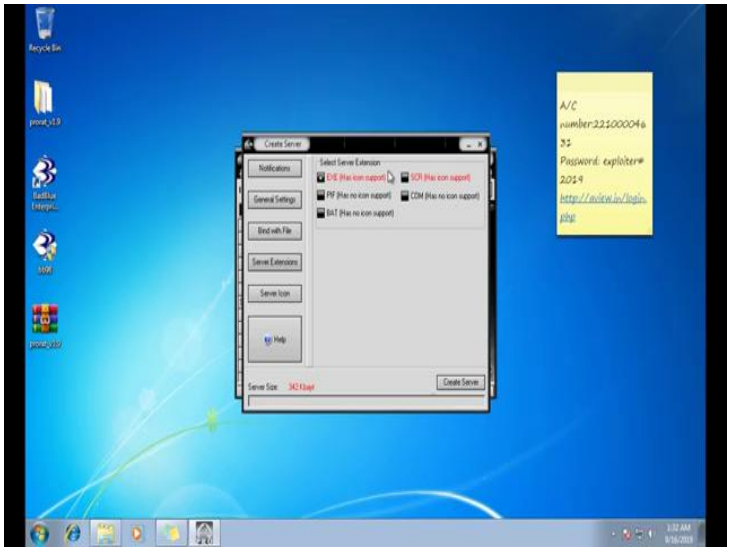
Then general settings is there. The server port, in which port you want to establish the connection and server password. So, that means this password is needed to connect with the server, then this is the victim name and fake Error Message you can also configure your own fake Error Message. Then other details are here. You can check each and every details.

(Refer Slide Time: 19:14)



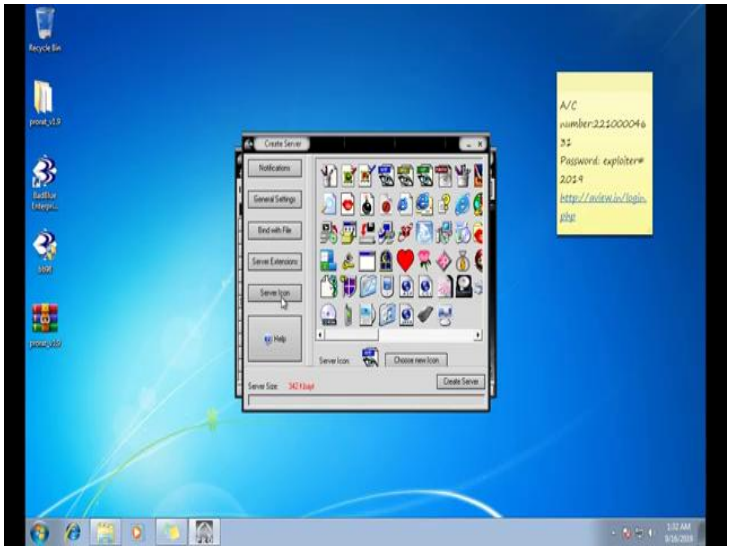
And you can also bind the server part with a legitimate file and you can select the file from your computer for the time being I am not binding with any file.

(Refer Slide Time: 19:32)



Then server extension, all this extension are available EXE, PIF, BAT, SCR, COM. Now for the time being I am using the file format EXE.

(Refer Slide Time: 19:45)



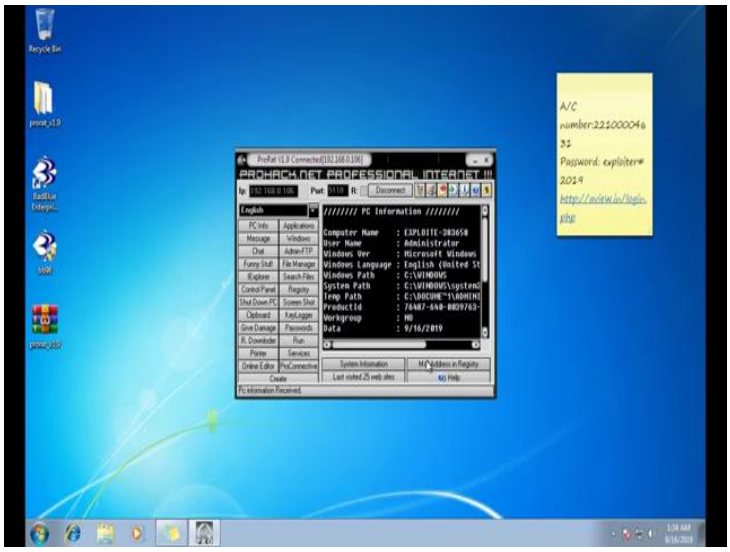
And server icon, you can choose any icon from the list; otherwise, you can also choose your own icon from your computer. So, now, suppose I am choosing the icon. This one and create server. So, server has been created with your settings, in the current directory. So, now, check in the current directory server is ready.

See, you can also rename this for social engineering kind of catalog that means, it become very easy to execute in the victim machine. So, for the time being we are transferring the server part in the victim machine directly by using the, a pen drive. And after executing this EXE file in the victim machine, we will try to connect the attacker machine with the victim machine.

So, now we already execute the server part in the victim machine. And now I am trying to connect the client part with the server part which is running in the victim machine. Now, victim machine IP address is 192.168.0.106 and the port is 5110. So, I am using the same port and then try to connect. So, it will ask for the password. So, if I put the wrong password, suppose 12345, then it will not connect with the server part.

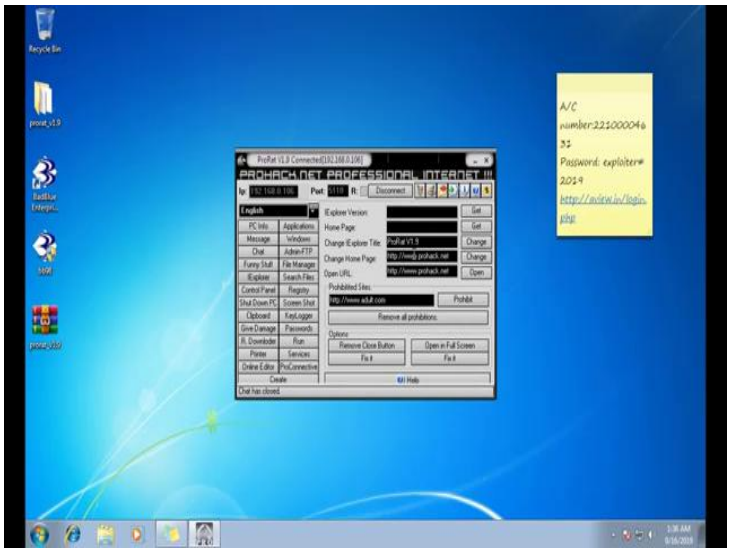
So, now, get the correct password 123456 which will authenticate your connection and then click on Password Correct Entrance Complete. So, after entering inside the victim machine, you can perform all this task which is available in the client part.

(Refer Slide Time: 22:10)



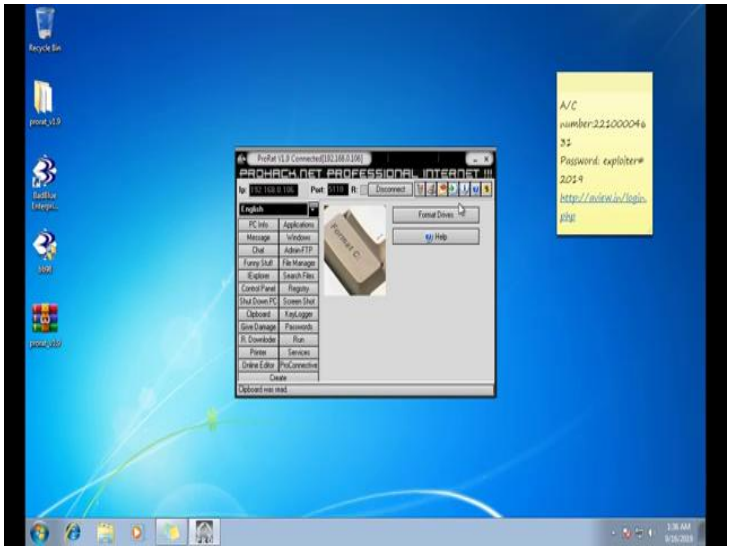
Now, PC Info, you can check PC Info, system information is here, mail address in registry that is also there. Last visited 25 websites that is also there. Then, messages you can also send any messages to the victim machine. Then chat, you can also use the chat. So, open chat then some funny stop is also there, hide desk stop icon, hide start button, hide taskbar, open CDROM, crazy keyboard lights and violet display, add a tail to mouse, lock mouse, make mouse go crazy, flipscreen.

(Refer Slide Time: 23:12)



So, all this funny staff is also there. Internet explorer, you can also open any website using internet explorer. Then you can also shutdown the PC and from there is a clipboard and from clipboard, you can also read all the things which is stored in the clipboard.

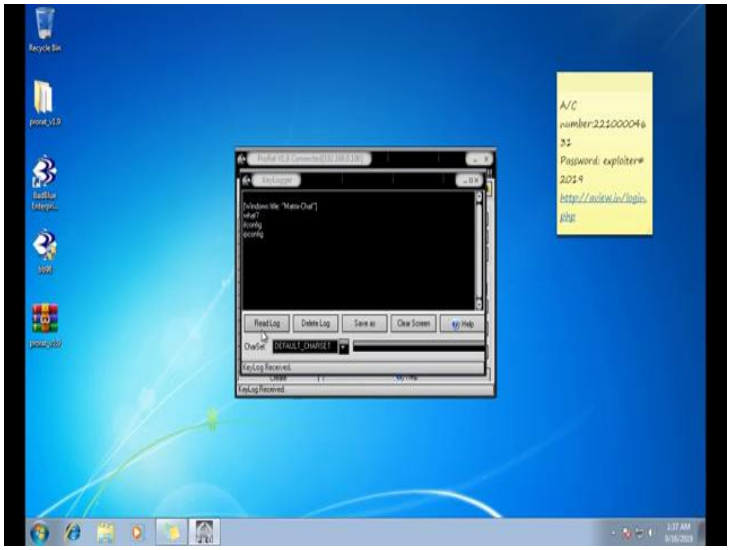
(Refer Slide Time: 23:34)



Give damage, you can also format the drive printer, online editor application. Then you can kill any process, kill all process. Then windows, you can refresh, you can hide, you can minimise. Then admin FTP, you can also connect with the file transfer protocol.

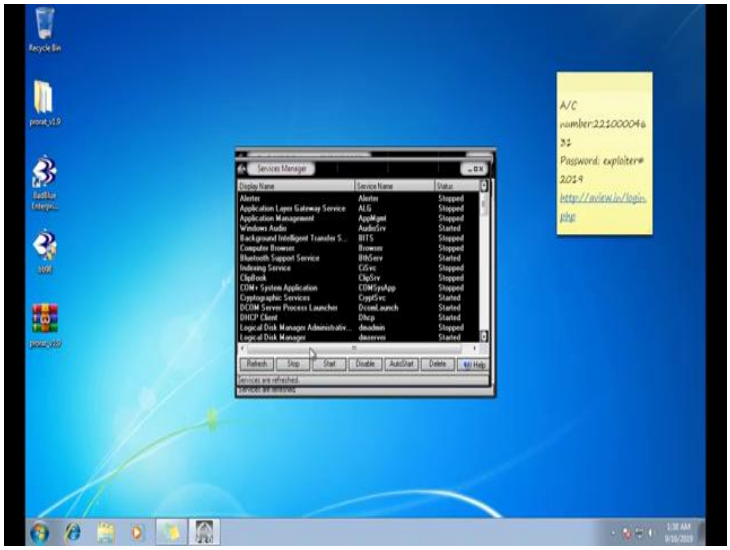
Then, file manager you can download, upload, delete or rename or create directory in the victim machine.

(Refer Slide Time: 24:16)



Screenshot, you can also take screenshot. Registry is also there. You can also check the registry of the victim machine. Key logger, you can also read the, all the key which is paste by the victim in password is also there. You can also check the password.

(Refer Slide Time: 24:44)



Then services, all the list of services are there, which is running. You can refresh, you can stop, you can start, you can disable or auto-start or even also delete any services. So,

by using the client part, you can perform all this tasks, once you connect with the server part which is running in the victim machines. So, this way by using a RAT, remote administrative tool we can compromise a system.

Thank you.