Introduction to Information Security

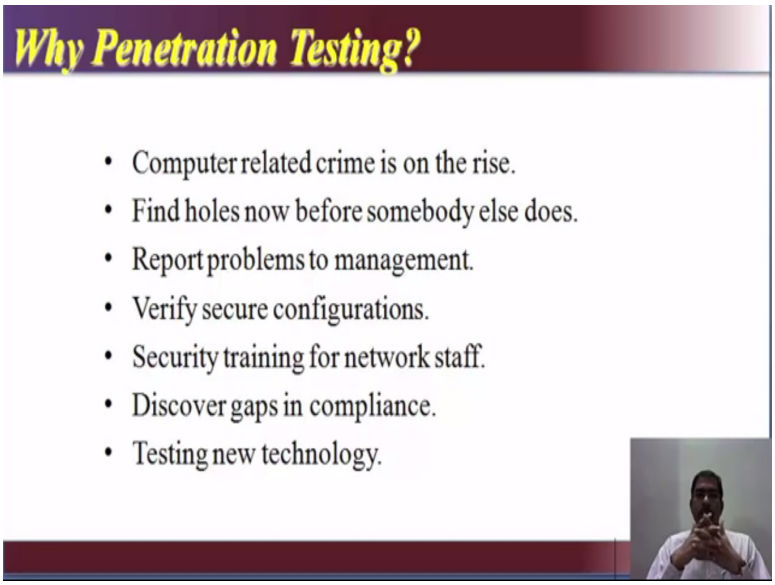
Prof. Dilip H. Ayyar

Department of Computer Science and Engineering

Indian Institute of Technology, Madras

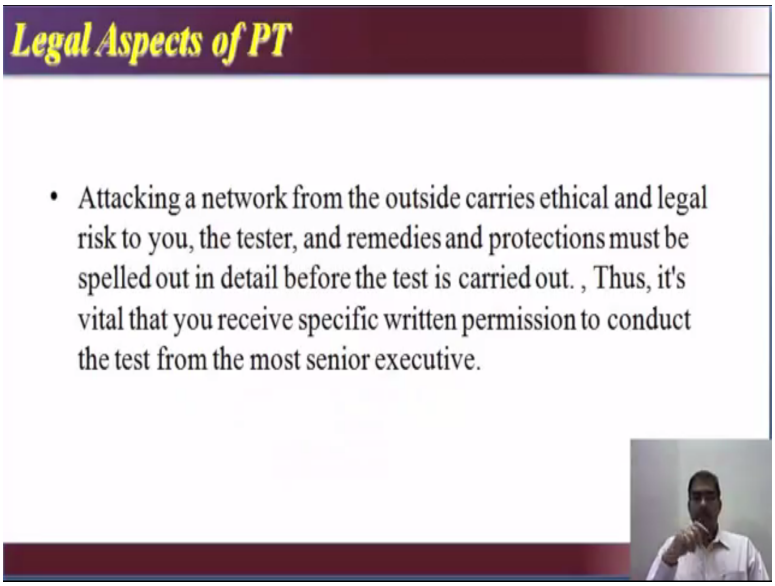
Lecture - 47

(Refer Slide Time: 00:10)



So, why do you need penetration testing because computer related crime is on the rise. To find holes or weaknesses before somebody else finds it out. To escalate the problems to the management, to take the proper action. To verify whether the configurations are secure enough, it also helps you to train your network staff on security issues, what to do, what not to do, how to implement security properly. List out the gaps in complaints against international standards which is the organization is following on or with regulatory requirement. And it is also used to test new technologies on what exposures are there which can be exploited in the technology. So, that is why people do penetration testing.

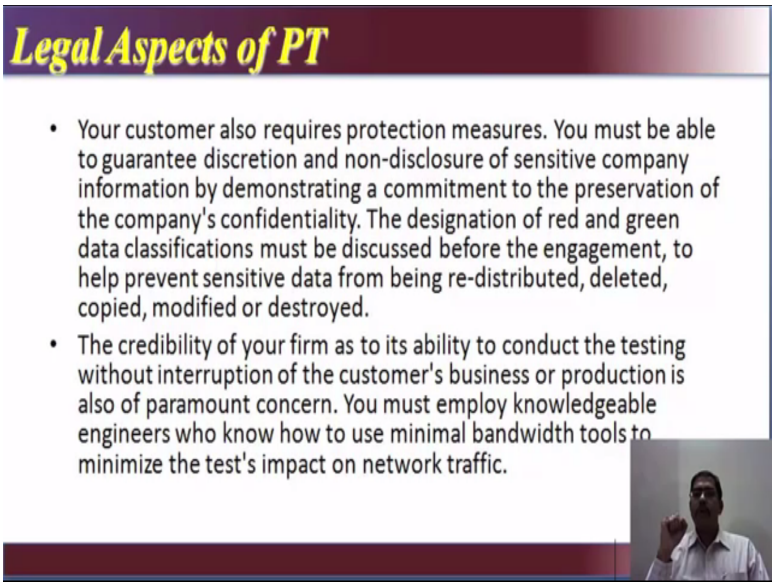
(Refer Slide Time: 01:17)



There are legal aspects also for penetration testing. Attacking a network from the outside carries ethical and legal risk to you, to the tester and the remedies and protections must be clearly spelled out in detail before the test is carried out. Thus, it is important that you receive specific written permission to conduct test from the most senior executive. Meaning this you are doing a ethical penetration testing or a penetration testing you need to safeguard yourself to the a maximum possible because if you have not taken the permission of the organization for conducting the test, then you can be in serious trouble there can be losses. The system can move down, the data loss can happen.

So, it should be very clearly spelled out what the aim of the test is, what the objective of the test is? What can be exploited? What should not be bought down? You need to have explicit written instructions for conducting a penetration test.

(Refer Slide Time: 02:30)



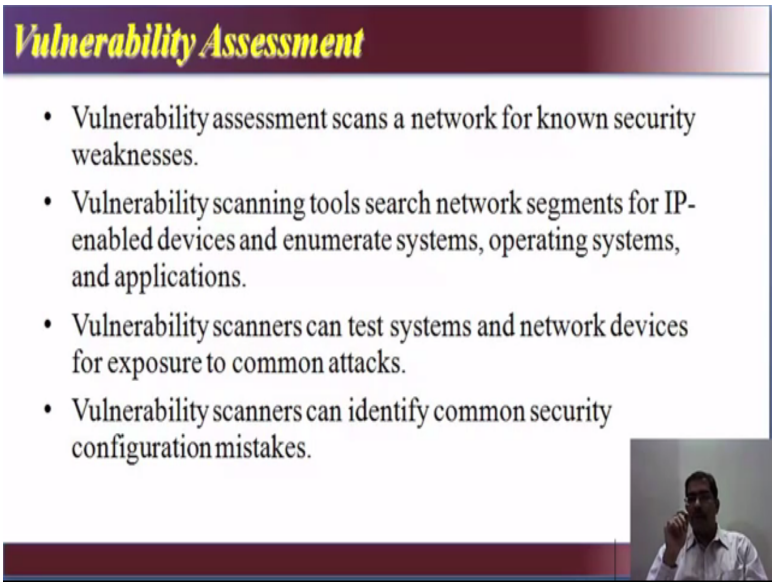
The customer also require protection measures. It is not only your side the customer also needs protection measures. You must be able to guarantee discretion and non-disclosure of sensitive information by demonstrating a commitment to the preservation of company's confidentiality. So, there should be legally enforceable NDA signed between you and the customer before doing a penetration test that will give the a customer legal view point in case any information is divulged by you.

Also the designation of red and green data classifications must be discussed before the engagement. Green data is your public data your information which is of not of much value to the organization or it does not matter to the organization if that particular information is divulged, but there are red data where it is critical or sensitive in nature where in the penetration tester should not disclose the data. That data should not be re-distributed it should not deleted, it should not be copied, it should not be modified, it should not be destroyed. Then the crucial thing is the credibility of your firm or you as an independent penetration tester and the company's ability to conduct the testing without interruptions to the customer's business is also of very serious consequence.

So, the company should engage or employ only knowledgeable engineers or security auditors, who know how to use minimal band width tools minimize the impact on the network traffic, where the test is being conducted. It should not be like when the security auditor or assessor goes for the test, he uses up all the band width by running multiple tools

on the network at the peak time let us say if it is a banking organization. When the customers are there in the branch and you conduct the penetration testing say during 9 and 11 you are running 6 or 7 different tools.Thereby using up the band width. So, the customers feel that the customer service at the branches are slow because you are eating up the band width.

(Refer Slide Time: 05:14)

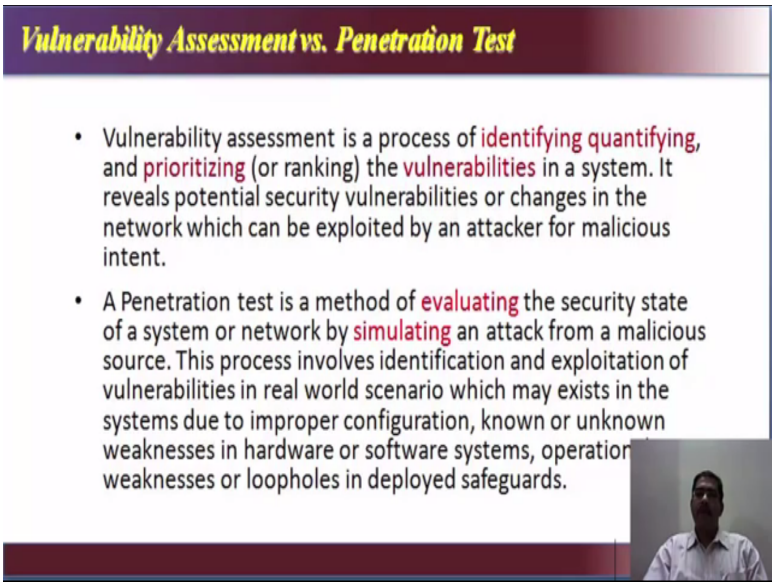


So, care should be taken to make sure that the customers are not impacted by the penetration testing that you are conducting. So, we have seen what is penetration test, what is vulnerability assessment. It stands a network for known security weaknesses. So, the initial phases of penetration testing applies to vulnerability assessment also. And vulnerability scanning tools searches the networks for IP enabled devices. So, anything which has got an IP address it suggests, that tool to search for the IP enabled devices it enumerates systems, by specifically stating that these are the number of systems found, this is the operating system installed in it, these are the applications which are installed in it. The scanners also test systems and devices for exposure to common attacks. So, the common attacks which are there for specific ports or services are tested by the vulnerability scanners. Now, the difference between this and the penetration testing module iself is that, here the vulnerability is identified and reported.

In penetration testing you take it one step further and try to exploit that vulnerability or provide a proof of concept, that it is being exploited. And the scanners can also identify common security configuration mistakes. Let us say you are running nexus, you are running

it on a windows server. And you use a plug in for testing the passwords. It will say that the password configured in the system is not as per base line requirement. So, it identifies common security configuration mistakes.

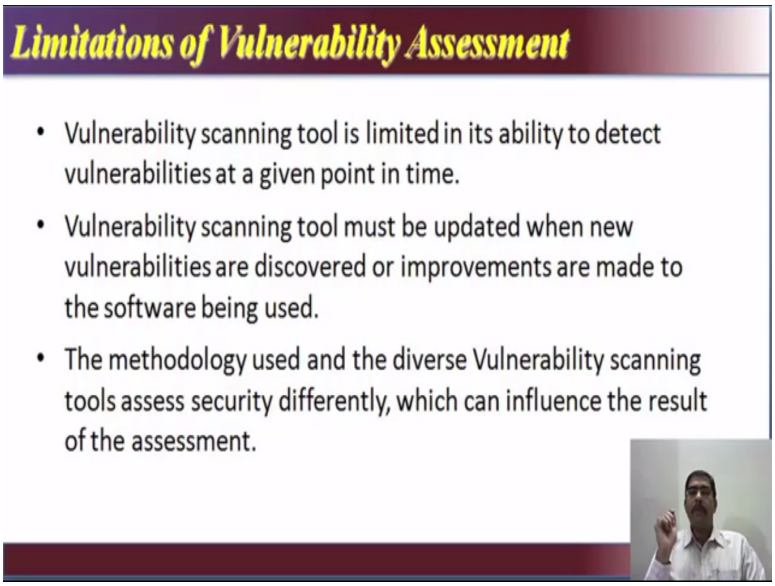
(Refer Slide Time: 07:04)



So, when you look at vulnerability assessment versus penetration test, vulnerability assessment is a process of identifying, quantifying and prioritizing or ranking the vulnerabilities in a system based on the exposure. It reveals potential security vulnerabilities or changes in the network which can be exploited by the attacker for malicious intent. Now, penetration testing is a method of evaluating the security state of a system or network by simulating an attack.

So, the subtle difference here is here in penetration testing an attack is simulated from a malicious source. This process involves identification and exploitation of vulnerabilities in a real world scenario, which may exist in the system due to improper configuration known or unknown software or hardware weaknesses, operational weaknesses or loopholes in the deployment of safeguard system.

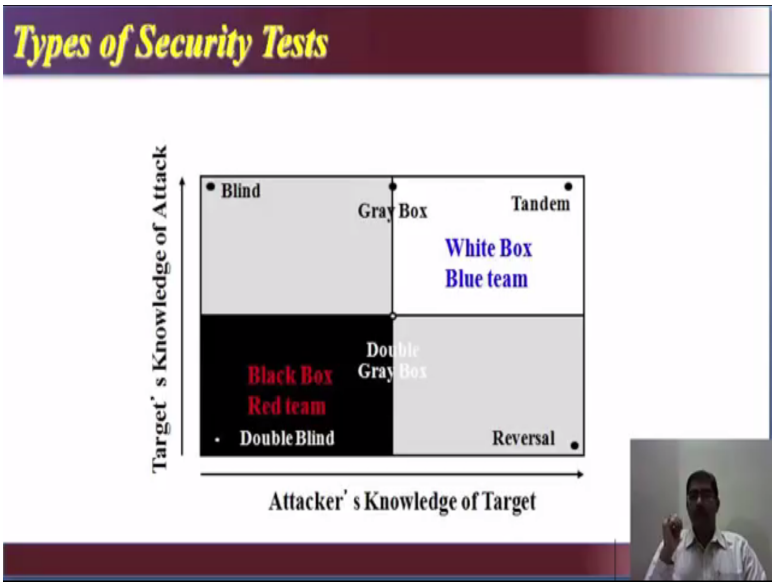
(Refer Slide Time: 08:08)



There are limitations of vulnerability assessments also. The scanning tool is limited in its ability to detect vulnerabilities at a given point in time. If a scanner is not updated properly or if there is a vulnerability that has come in, say last night. Your scanner will be limited in identifying that vulnerability because it does not know that vulnerability exists or zero regrets. Then the scanning tool must be updated when new vulnerabilities are discovered or improvements are made to the software.

Then the methodology we use and the diverse vulnerability scanning tools assess security differently. Now, your NSS may detect it differently or NESSUS may detect it differently or your GFI languard may detect it differently. So, which will have an impact on the result of the assessment. There are different types of security tests.

(Refer Slide Time: 09:17)

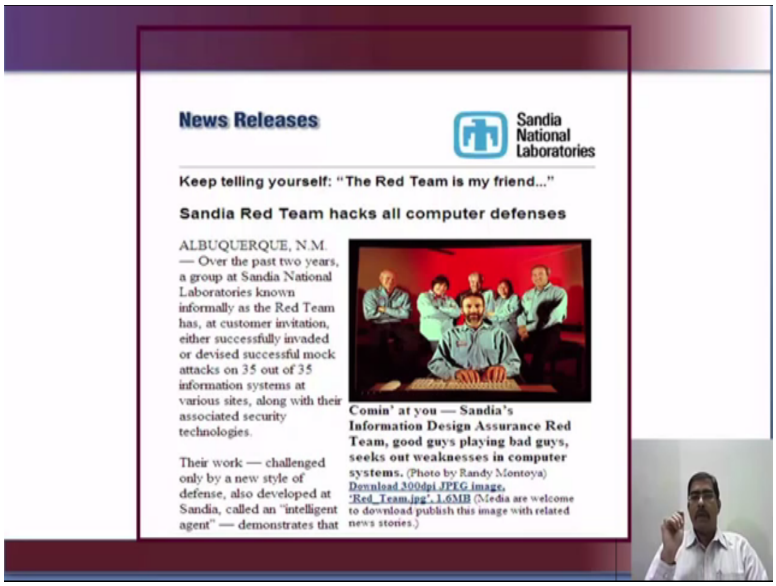


Like your blind, grey box, white box, blue team, black box or red team, double blind reversal. So, here we can see that the attackers knowledge of the target increases as we go further right and targets knowledge of attack also increases when you go vertically. Grey hack is a cracker or a hacker who exploits the security weakness in a computer system or a service or a product, in order to bring out the weakness to the attention of the organization.

This is unlike a black box, a grey hack, hacks without the malicious intent the goal of the grey hack is to improve the system and network security, but by publishing a vulnerability the grey hack may give a clue to the potential attackers, or an opportunity for others to exploit that particular vulnerability that he has found. This is a way differs from the white hack who alerts system owners and vendors that a vulnerability is there, without actually exploiting it in public.

So, that is a subtle difference between black grey and white hack. You can there are extensive documentation available in the internet regarding these four types of testing.

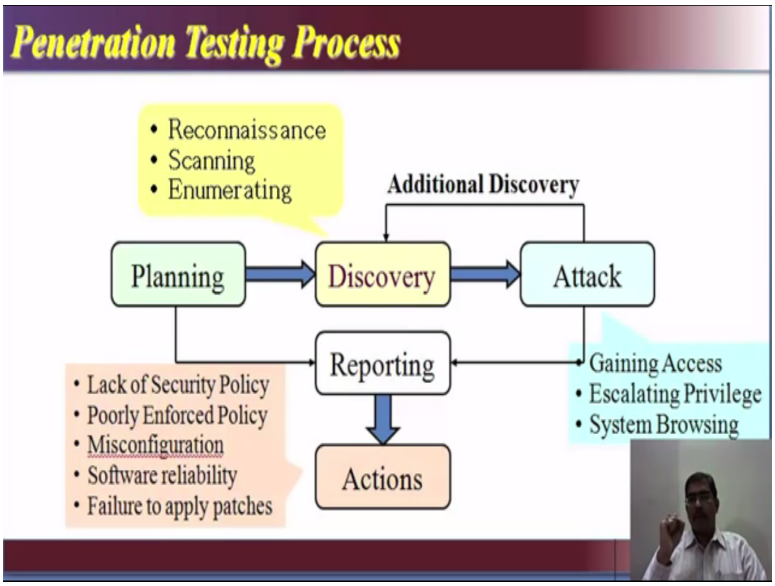
(Refer Slide Time: 11:00)



You can learn more by googling. This is an example that the red team hacks all computer differences. So, you can keep telling yourself that your red team is a friend, but there was an instance in Canada, in New Mexico where the red team itself attacked the network, it is a very interesting article. You can it is a news release also again you can google this and read more about this. The basic goal of penetration test or pen test or pt., it is also called ethical hacking, is to examine the current state of security of the IT infrastructure. So, by performing the controlled tests or attacks a penetration test or a PT uncovers the security clause in a very realistic way. The spectrum of tested system also ranges from simple online jobs to complex company databases and networks. The attack method also manifold and encompass everything from passive information gathering to targeted attack from the internet and the identification of weaknesses.

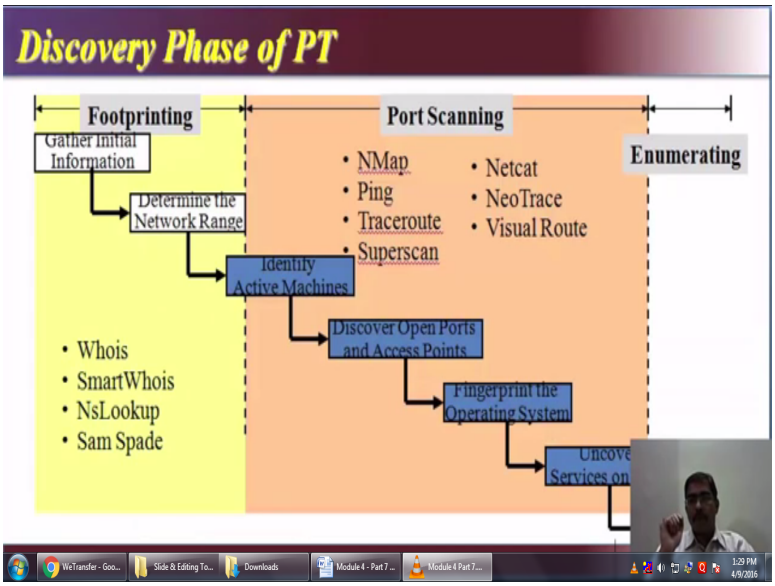
Hence, the adaptation of penetration test, to the customers requirement guarantees the practical relevance of the test. So, for this reason even before a client decides to work with the red team, a preliminary meeting is held with the potential customers to discuss how to organize their pen test for optimal results.

(Refer Slide Time: 12:58)



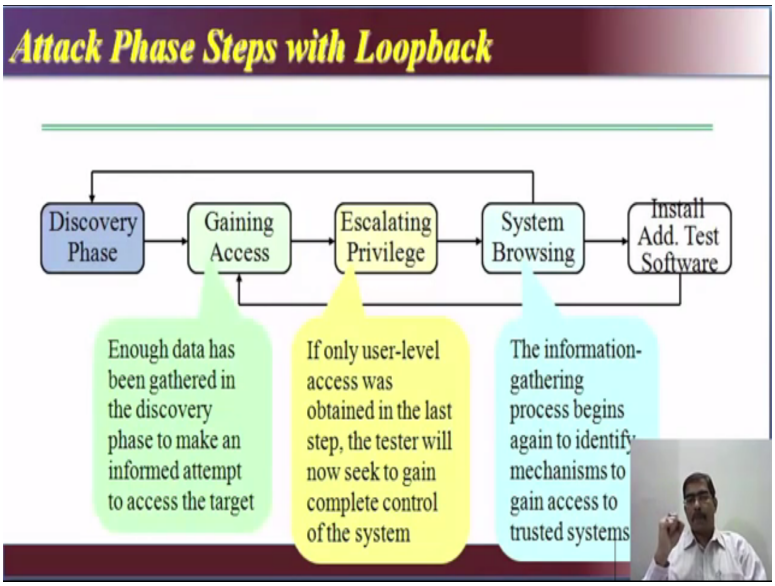
Now, the process for penetration testing, we have seen in the previous slides. There is reconnaissance phase there is a scanning and enumeration phase, then in the planning phase we plan on what systems have to be tested? What are the scopes of the penetration tester? Classification of green data and red data. Then you go for the discovery phase where you discover the number of servers the number of network devices, the applications which are installed. Then comes the attack phase or additional discovery phase, where certain instances may crop up, then goes the reporting phase, then the action that are to be taken to protect the network. So, basically you have in the discovery phase reconnaissance, scanning and enumeration. In the attack phase you gain access you escalate your privileges then do a system browsing to see what is there and what is not there. In the discovery phase you have a lot of systems that will be identified. And in reporting you have or in actions taken you have results or the results of the test will reveal lack of security policy or orally enforced policy, misconfiguration of systems or settings then reliability of the software itself and also failure to apply patches that the systems unpatches them, or the systems not patched properly for security vulnerabilities.

(Refer Slide Time: 14:51)



All these will be evidenced see if we go a little bit further. We will see in the discovery phase of PT. First is your foot printing where you gather the initial information. And determine the network rate, some of the tools which are used are, Whois, SmartWhois, NsLookup, Sam Spade. Then in your port scanning phase, you will have identification of active machines we discover the open ports and access points, you fingerprint the operating system, you uncover the services on the port. So, these four phases will come under port scanning. Some of the tools used are NMap, Ping, Tranceroute, Superscan, NC or Net Cat, Neo Trace, Visual Trace Route. Then in the enumerating phase you map a network. Now, that you have foot printed and done a port scanning you will have an idea of what a network is.

(Refer Slide Time: 16:01)

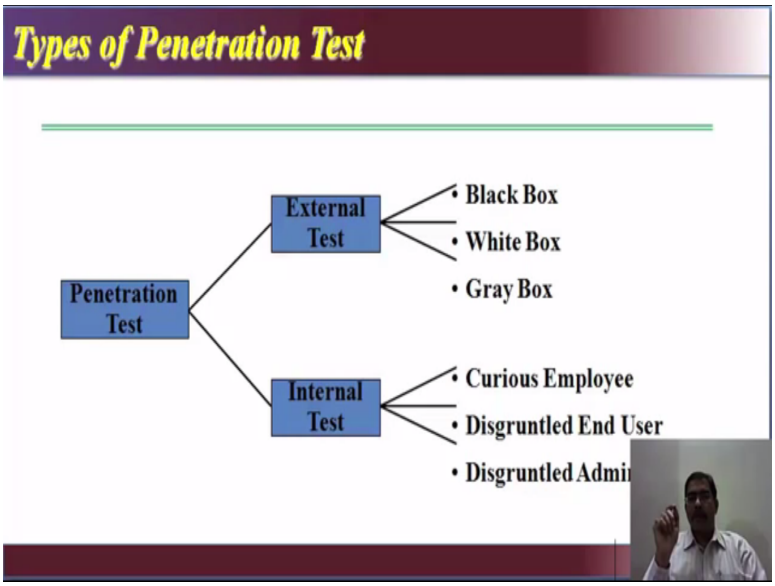


So, you will map the network then we attack phase steps will move back. Now, the discovery phase we have seen in the gaining access phase enough data has been gathered in the discovery phase to make an informed attempt to access the target. So, in the gaining access phase, you have sufficient information and gather during the discovery phase. So, that you make an in found attempt to access the target itself.

Once you have done that then you go to the escalating privilege phase where if only user level access was obtained in the last step, the tester will now seek to gain complete control of the system. So, in the gaining access phase if a user account has has been compromised or if the attacker gets the user account. His next intention is to get complete control of the system by getting the group privileges or administrative privileges.

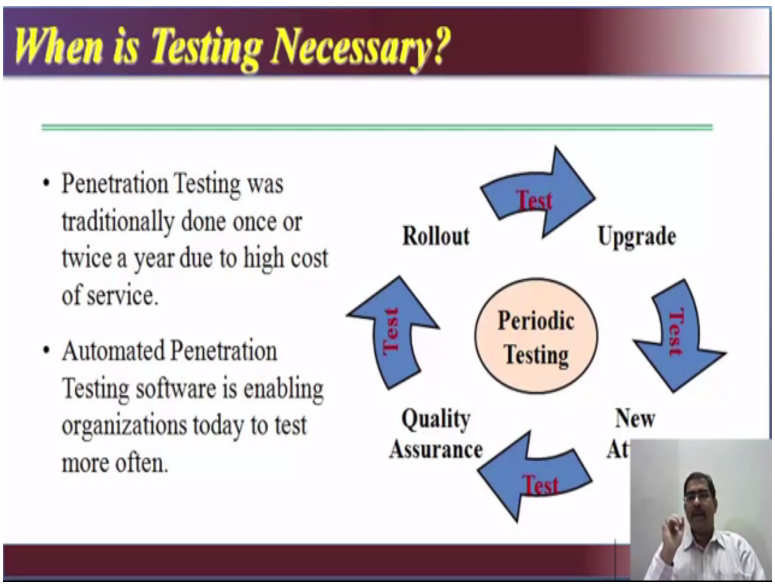
Then comes the system browsing phase. The information gathering process begins again to identify mechanism to gain access to trusted system. So, if once he gains full control of the system, again the information gathering process begins to try and find out mechanisms to gain access to trusted systems. Then you install add, test the software test the final phase. Why it is called the loop-lag phase is, once you come into the system browsing phase you go back to the discovery phase and fine tune your results or fine tune your scanning. And once you install and add your test software, you again go back to the gaining access phase and repeat the process. So, that is why it is called an attack phase step with loop-lag.

(Refer Slide Time: 18:03)



We have seen in brief the types of penetration tests. You can broadly classify again into external test and internal test. Under external test you have black white and grey box testing. Internal testing can be done by a curious employee, who just wants to know what the security concern is or disgruntled end user again this is a dangerous type of test. Disgruntled administrator since he already has administrative privileges the damage caused can be huge. It can be also done by internal auditors to test the security posture of the organization.

(Refer Slide Time: 18:45)



Now, when is testing necessary or required. It was traditionally done once or twice a year because of the high cost of service. The penetration testers are expensive commodity. So, testing was done on a limited period may be half yearly or may be once a year. Now, because of the automated penetration testing software, the cost have come down the time has come down, time for conducting a pen test. So, again the organizations can afford to test the security posture more frequently.

The periodic testing will involve your testing is across or as a cycle when a new attack comes. When you need quality assurance that your network is safe, when you roll out a new product, when you upgrade an existing product. So, it is a cycle, it is a cycle where you can do a penetration test at different junctures of implementation. It can be a new attack to test whether a new attack is affecting our organization, to ensure the quality of products and services. To have a roll out of a new product or a software or service.