Introduction to Information Security

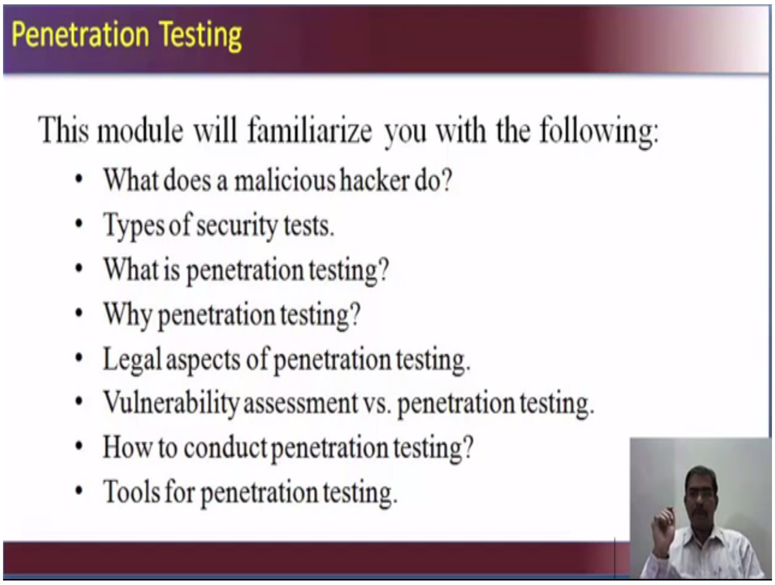
Prof. Dilip H. Ayyar

Department of Computer Science and Engineering

Indian Institute of Technology, Madras

Lecture – 46

(Refer Slide Time: 00:10)



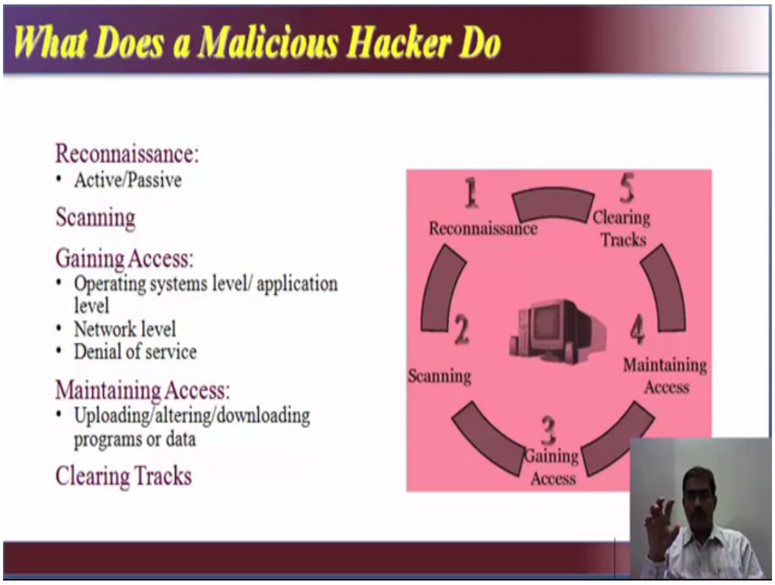
Penetration Testing

This module will familiarize you with the following:

- What does a malicious hacker do?
- Types of security tests.
- What is penetration testing?
- Why penetration testing?
- Legal aspects of penetration testing.
- Vulnerability assessment vs. penetration testing.
- How to conduct penetration testing?
- Tools for penetration testing.

Let us start with penetration testing. Now, vulnerability assessment and penetration testing are used in convincing very often. We will take a look at the difference between both, we will also see what are the types of security tests, definition of the PT and why we should conduct a penetration testing, what the legal issues are while conducting a PT and some of the popular tools related to PT. Now, this module will familiarize you with what a malicious hacker does, what are the types of security test, what is a penetration test, why do you need a penetration testing on your infrastructure, what are the legal aspects of penetration testing, then vulnerability assessment versus penetration testing. How do you conduct a penetration testing and what are the tools that are used for penetration testing.

(Refer Slide Time: 01:18)



What Does a Malicious Hacker Do

Reconnaissance:
- Active/Passive

Scanning

Gaining Access:
- Operating systems level/ application level
- Network level
- Denial of service

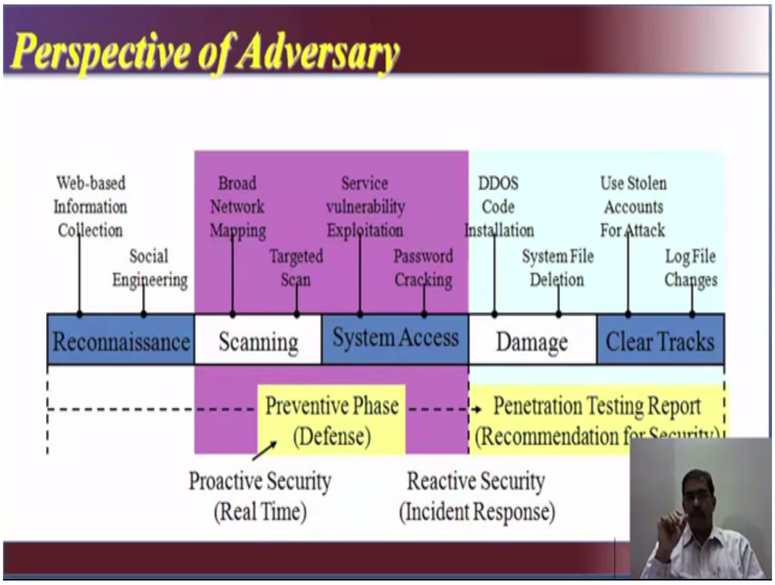
Maintaining Access:
- Uploading/altering/downloading programs or data

Clearing Tracks

We will see what a malicious hacker does. Now, if you look at the image on your right hand side you will see that there are five phases. The first is reconnaissance, the second is scanning, the third is gaining access and the fourth is maintaining access and fifth is clearing tracks. Under the reconnaissance we have active reconnaissance and passive. Then there is scanning of those services, then after identifying the vulnerabilities in the second phase the attacker tries to gain access at the operating system level at the application level at the network level. Probably cause a denial of service.

Then he maintain free access in the fourth phase, where he can upload, alter the existing files or download confidential information. That information can be programs can be data. Then finally, he clears up the track so that there is no evidence of him penetrating the network.

(Refer Slide Time: 02:29)



Perspective of Adversary

Web-based Information Collection

Social Engineering

Broad Network Mapping

Targeted Scan

Service vulnerability Exploitation

Password Cracking

DDOS Code Installation

System File Deletion

Use Stolen Accounts For Attack

Log File Changes

Reconnaissance

Scanning

System Access

Damage

Clear Tracks

Preventive Phase (Defense)

Penetration Testing Report (Recommendation for Security)

Proactive Security (Real Time)

Reactive Security (Incident Response)

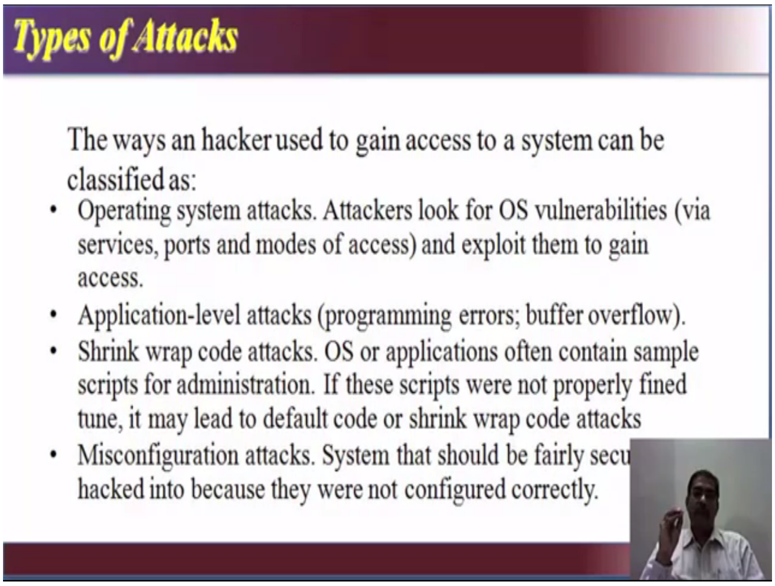
What is the perspective of an adversary? There are five phases here, in reconnaissance when you look at the slide, it is web based information collection and social engineering techniques. What is web based information collection? If there is a site posted then the adversary or the perpetrator tries to find more information on the site what is the public IP, what is using IP tools or network tools or Dns rules or simply trace route.

How many hops are there to reach the particular server, then social engineering techniques. He tries to engage the internal employee of the company using false pretenses, try to gather as much information as possible. It can also be through dumpster diving, we have discussed that earlier. Then comes the scanning where a broad network mapping is used. So, tools such as NMap, Nesus are used. And it is a targeted scan to a specific IP within the network or a specific server. Then the system access where the service would be exploitation; suppose it is there that Microsoft has got a particular slot in this particular port or service. And it can be exploited this way we would have mentioned in the controller CBE, the attacker tries to penetrate that or exploit that particular vulnerability. He does a password cracking phase using different tools like Lophp crack jammed port. So, several tools are available for that. Then the actual damage happens. We can pass a Ddos attack we can install a code within the server for causing havoc later on. The attacker can delete a system file. So, damage has been done to maintain the access, when he clears the racks that is use of stolen accounts for attack.

He changes the lock file to erase the evidence of him coming in. So, these are the steps that are done by a potential attacker. Now, the first three phases that is the reconnaissance, scanning and system access is where the preventive phase comes in. So, you can actually with the help of different methodologies different tools you can provide a defense of these, which is a real time or a pro-active security. Now, in the next two phases of the penetration testing there is a report that comes out of the penetration testing.

So, the organization based on the report we will implement the recommendations. This is a reactive security or an incident response. So, what will happen if the attacker does the first three, four and five what happens. So, from the penetration testing perspective when a person who is authorized to conduct the penetration testing, finds out all these and gives a recommendation the organization and implements those measures. So, that in the event of the real attack these systems are not compromised.

(Refer Slide Time: 06:19)



Types of Attacks

The ways an hacker used to gain access to a system can be classified as:

- Operating system attacks. Attackers look for OS vulnerabilities (via services, ports and modes of access) and exploit them to gain access.
- Application-level attacks (programming errors; buffer overflow).
- Shrink wrap code attacks. OS or applications often contain sample scripts for administration. If these scripts were not properly fined tune, it may lead to default code or shrink wrap code attacks
- Misconfiguration attacks. System that should be fairly secu hacked into because they were not configured correctly.

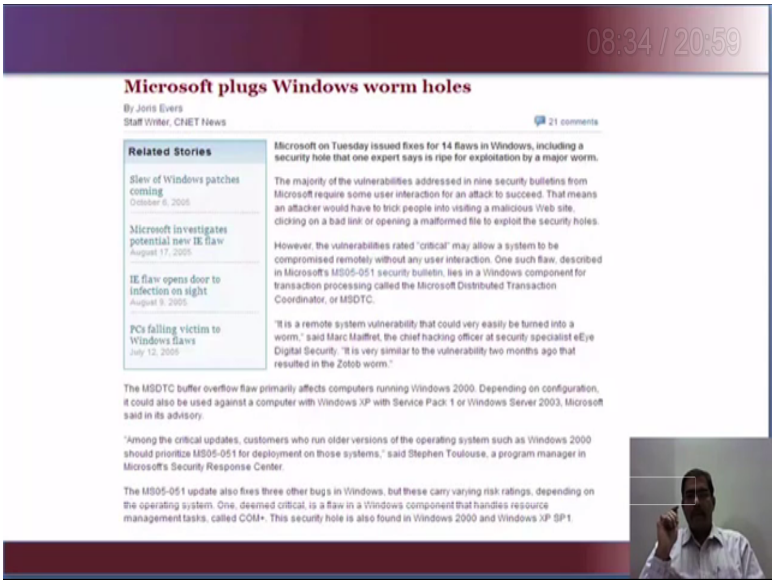
There are different kinds of or types of attack, the ways an attacker or a hacker use to gain access to system can be classified as there are several ways and methods that an attacker can get into a network or access a system. Operating system attacks are where the attacker looks for the operating system vulnerabilities, where a scanning phases where he sees what are the open services open ports, what are the methods of access and exploits them to gain access into the system.

Then there is application level attacks such as your programming errors your buffer overflows, all these are examples of your application attacks. So, he exploits these vulnerabilities to do an application level attack. Then there is a shrink wrap code attack which is basically OS or application which contains sample scripts for an administration which comes default shift with the system.

For example, if you have a IAS script server which is you have installed there will be certain scripts which are by default enabled in the system. So, you have to go and make the settings. So, you should not allow the default installation to remain as it is. So, that the attacker can gain access. Similarly, with Php installation or apache installation. Now, if these scripts were not properly fine tuned then it will lead to default code or shrink wrap code attack.

That is you exploit the vulnerability that is known to you because proper settings have not been done on the server on the web server. Then there is misconfiguration attacks most of the times the developers or the implementers fail to change the default settings. So, then if it stays in the default settings then attacks can be done on that because they were not configured properly

(Refer Slide Time: 08:28)



08:34 / 20:59

Microsoft plugs Windows worm holes

By Joris Evers
Staff Writer, CNET News

21 comments

Related Stories

Slew of Windows patches coming
October 6, 2005

Microsoft investigates potential new IE flaw
August 17, 2005

IE flaw opens door to infection on sight
August 9, 2005

PCs falling victim to Windows flaws
July 12, 2005

Microsoft on Tuesday issued fixes for 14 flaws in Windows, including a security hole that one expert says is ripe for exploitation by a major worm.

The majority of the vulnerabilities addressed in nine security bulletins from Microsoft require some user interaction for an attack to succeed. That means an attacker would have to trick people into visiting a malicious Web site, clicking on a bad link or opening a malformed file to exploit the security holes.

However, the vulnerabilities rated "critical" may allow a system to be compromised remotely without any user interaction. One such flaw, described in Microsoft's MS05-051 security bulletin, lies in a Windows component for transaction processing called the Microsoft Distributed Transaction Coordinator, or MSDTC.

"It is a remote system vulnerability that could very easily be turned into a worm," said Marc Maiffret, the chief hacking officer at security specialist eEye Digital Security. "It is very similar to the vulnerability two months ago that resulted in the Zotob worm."

The MSDTC buffer overflow flaw primarily affects computers running Windows 2000. Depending on configuration, it could also be used against a computer with Windows XP with Service Pack 1 or Windows Server 2003, Microsoft said in its advisory.

"Among the critical updates, customers who run older versions of the operating system such as Windows 2000 should prioritize MS05-051 for deployment on those systems," said Stephen Toulouse, a program manager in Microsoft's Security Response Center.

The MS05-051 update also fixes three other bugs in Windows, but these carry varying risk ratings, depending on the operating system. One, deemed critical, is a flaw in a Windows component that handles resource management tasks, called COM+. This security hole is also found in Windows 2000 and Windows XP SP1.

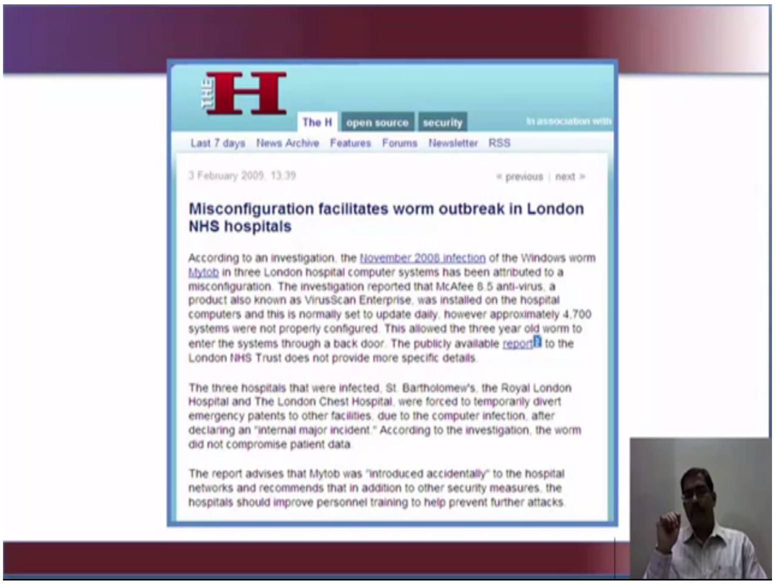
These are the simple examples how the vendors actually plug those. Now, Microsoft plugs windows worm holes. So, there were fourteen blocks in a particular version of windows including a security code that one expert says is the right for exploitation by a major worm. So, the details are given in this slide. So, this is an example for you to understand that, the once a vulnerability is found the attackers try to exploit it. They find out the means and methods to exploit that vulnerability through different factors.

Now, in this particular instance because of the security code an expert has found that a worm could actually attack or exploit that vulnerability. And Microsoft windows has released some superior patches for that particular vulnerability. So, it is a constant process, there will be a vulnerability found out in a product or service. Somebody will try to exploit it, then the operating system vendor will bring out a fix or a security patch for that.

Once that patch is applied, then that particular attack can no longer happen, but the attackers will still have methods to get into the system using other vulnerabilities. The main weakness found in the networks are many of the systems or servers in the networks are not patched properly. They ultimately they blame it on the operating system vendor. So, as and when a patch is released, it is recommended that you install the patch secure your infrastructure, but many of the hacks that happen, if you see the background of the hacks you will come to know that an outdated version of windows 2003 server was used, where the latest version is Pentigo or a Windows XP machine was targeted when the latest is Windows 10 is coming in now. So, basically the reasons for exploitation is again from the human perspective that the systems are not updated on a regular basis because the developers may sometimes feel that by installing this patch the software will not work, but I have seen instances where the browser was in a application where the application works only on internet explorer 6. Where the current version of internet explorer at that time was 7 or 8. So, flaws in 6 would have been exploited by attackers.

Majority of the problem is that organizations or the team that handles security do not implement the security patches as and when they are released by the operating system vendor. So, they often blame the vendor or the maker of the product for the vulnerability that exist or they say that no by installing this patch my system will not work. So, the customer also does not know what to do. There are several issues ultimately it is the people problem and the process problem where security measures are not being followed diligently by the organization.

(Refer Slide Time: 12:13)



3 February 2009, 13:39

Misconfiguration facilitates worm outbreak in London NHS hospitals

According to an investigation, the November 2008 infection of the Windows worm Mytob in three London hospital computer systems has been attributed to a misconfiguration. The investigation reported that McAfee 8.5 anti-virus, a product also known as VirusScan Enterprise, was installed on the hospital computers and this is normally set to update daily, however approximately 4,700 systems were not properly configured. This allowed the three year old worm to enter the systems through a back door. The publicly available report to the London NHS Trust does not provide more specific details.

The three hospitals that were infected, St. Bartholomew's, the Royal London Hospital and The London Chest Hospital, were forced to temporarily divert emergency patents to other facilities, due to the computer infection, after declaring an "internal major incident." According to the investigation, the worm did not compromise patient data.

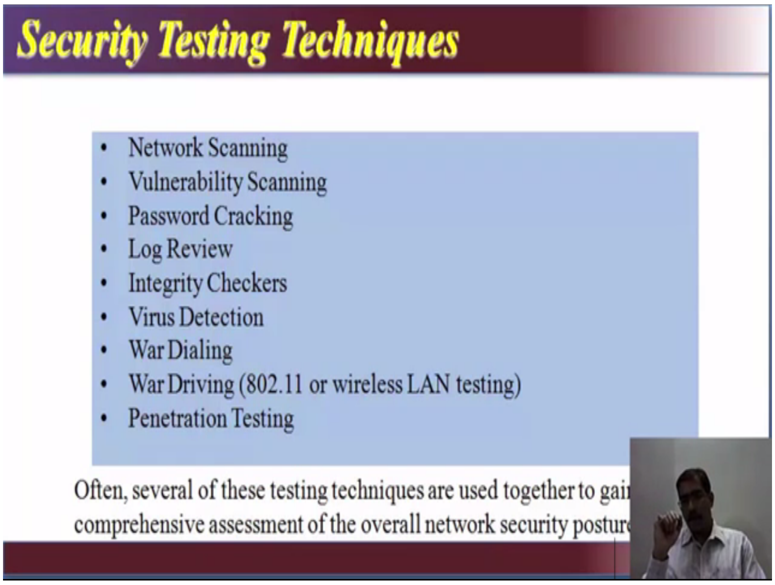
The report advises that Mytob was "introduced accidentally" to the hospital networks and recommends that in addition to other security measures, the hospitals should improve personnel training to help prevent further attacks.

This is not a example which is because of a misconfiguration facilities or misconfiguration which facilitated a worm outbreak in London hospital. Again this configuration we spoke about it just a few seconds ago. People fail to understand the implications of the security intrudes. Security is only the last options for organizations they say my priority is not security my priority is to see that I develop the software and sell or implement.

So, more often than not you find that most of the software developed are of poor quality which do not have proper security implementation because we do not involve security experts in the design phase. And then they spend a lot of money for rectification, once a hack has happened or once it is made mandatory by a regulatory body that we should have a software audited only then we will purchase. So, then they wake up to the fact that security is an aspect, but in Indian scenario secure coding is never followed because the developers do not want to waste time.

Second, they do not know the implications of having a secure software or secure framework in place, by closing this particular thing what will happen to my software whether it will work or not. So, the involvement of security teams are also not there. Even large organizations where we have seen the chief information security officer talks quite a lot, but does not know technical aspects. More often he just handles the processes or the documentation part and this trueness about what is actually happening within the network, what are the techniques of security testing.

(Refer Slide Time: 14:22)



Security Testing Techniques

- Network Scanning
- Vulnerability Scanning
- Password Cracking
- Log Review
- Integrity Checkers
- Virus Detection
- War Dialing
- War Driving (802.11 or wireless LAN testing)
- Penetration Testing

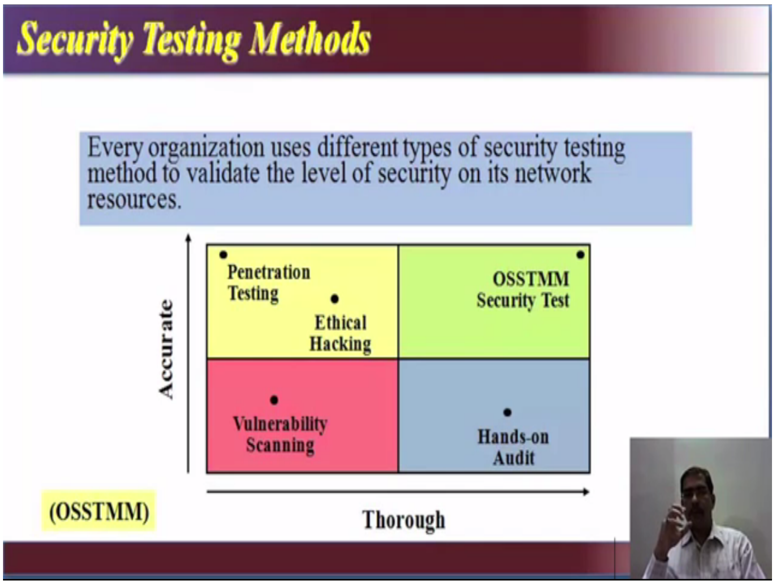
Often, several of these testing techniques are used together to gai
comprehensive assessment of the overall network security postur

They are network scanning, vulnerability scanning, password scanning or cracking. Review of logs it can be a manual review of logs which can be very monotonous or it could also be through a SIM tool, when there are integrity checkers. Then virus detection, war driving and war dialing then of course, penetration testing. Now, several of these testing techniques are used together to understand or gain more comprehensive assessment of the overall network security posture of the organization.

So, by doing a combination of this the organization knows where they stand with all the security regards. So, here there is something called an integrity checker because it is very difficult to compromise a system without altering a system file. So, these file integrity checkers become an important capability in the intrusion detection systems. The file integrity checker computes a checksum for every guarded file and stores it in its database. At a later time one can compute the checksum again and test the current value with the original computed value, but one of the problems of using a file integrity checker is that, there can be a lot of false positives.

So, when you update files or when you apply system patches. This changes the file right, it changes the checksum, it changes the cache. So, it should be constantly updated to prevent the false positive problem. There are several integrity checkers Tripwire is one of them. We can google Tripwire and learn more about integrity checkers what the Tripwire tool itself is. What are the methods for security testing?

(Refer Slide Time: 16:29)



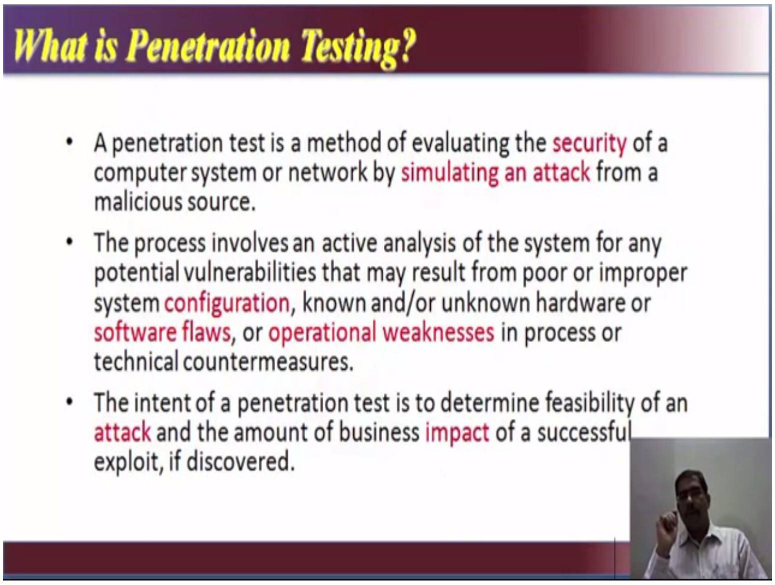
Security Testing Methods

Every organization uses different types of security testing method to validate the level of security on its network resources.

So, every organization uses different types of security testing to validate the level of security on its network resources. If you see that on the right, the arrow those that is your OSSTMM and hands-on audit is very thorough. Accurate is your penetration testing is your ethical hacking along with vulnerability scanning this is basically taken from the OSSTMM site. In 2001, ISECOM, that is institute for security on open methodologies started with the release of OSSTMM which is the open source security testing methodology manual.

It was a move to improve how security was tested and how it was implemented. Many researches form various fields contributed because they saw the need for an open method. The one that was directed towards the group and not for commercial gain or political agendas. And it is not enough to just find the facts. We need to find ways to apply those into the world that we live in. So, it needs to be a security philosophy and it needs to make sense. And that is what ISECOM did by bringing in OSSTMM framework. Now, it helps millions of people around the world from the governments, from businesses to schools and to regular people like us, so, that we can make better sense of what security is in the real world.

(Refer Slide Time: 18:29)



What is Penetration Testing?

- A penetration test is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source.
- The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures.
- The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered.

Now, we will see what is penetration testing? It is a method for evaluating the security of a computer system or a network. Network is a collection of computers or devices and or devices by simulating an attack from a malicious source. From a source which is not authorized to come into the network. This process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration.

So, here we have to note, one is evaluating the security it is in red. Simulating an attack poor or improper configuration, known or unknown hardware or software flaws, operational weaknesses which is the processes that are followed, in process or technical counter measures. And what are the intent or intention of your penetration test. It is determine feasibility of an attack, whether the attack can happen and the impact that can be caused by the attack being materialized.

So, that is what is penetration testing. What you need to understand is it is a method for evaluating security by simulating an attack, by testing for vulnerabilities because of improper or poor configuration, unknown or known hardware or software flaws or through an operational weakness. And to determine feasibility of an attack, to see what is the impact on the business.