

**Information Security: Level #4**  
**Prof. Andrew Thangaraj**  
**Prof. Prathap Haridoss**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Madras**

**Module - 12**  
**Lecture - 12**  
**Penetration Testing: An Introduction**

This module we will actually start taking a look at the penetration testing concepts and what kind of techniques are generally done including the different steps that one does as part of penetration testing.

(Refer Slide Time: 00:24)

### Penetration testing: An Introduction

Different Terms used by an organization interchangeably:  
Security Audit or Network/Risk Assessment or  
Penetration testing

Definition of:

**Security Audit:** Measurable Technical assessment of system(s) or application(s)

**Network Assessment:** Evaluation of risks/vulnerabilities in systems/applications/processes

**Penetration Testing:** Goes beyond. Would don the hat of a malicious hacker and attack those vulnerabilities



So, there are actually different terms that typically used by an organisation, you will find the a term called a security audit or network or a risk assessment as well as penetration testing being used interchangeable form. But if you strictly see there are very very subtle differences between these terms and we should be little bit careful on what with term will be more appropriate for a given context. So, when you look at a security audit, it basically means to do sort of a measurable technical assessment of a system or an application right.

So, what do you mean by technical assessment here is with respect to the security part of it, how a system or an application is secure enough or whether there are any specific

things that need to be further enhanced to take care of the fact that the security has to be strengthened as far as that particular system or application is concerned. So, the next is basically network assessment where it is more and evaluation of risk or vulnerabilities detecting in way systems or applications or processes right.

So, here the question of risk or vulnerability measurement is typically done to ensure that I have some sort of an analysis done subsequently on that vulnerability that has been found out, and how to address that subsequently. So, that network assessment part of it comes more from the perspective of trying to find out what kind of security issues that needs to be address from a network point of view.

Third one that we have going to be looking at more in detail as part of this particular course is what penetration testing which really goes beyond a simple security audit or a or as a network assessment right. So, what did actually does is this basically tries to put one into the shoes of a potential hacker who might have a malicious intent and look at the entire system from his perspective trying to identify and attack what possible vulnerabilities are present in the system at that instant of time right. So, among the three as we can very clearly see a penetration testing is something which is more involved more important from the perspective of ensuring that the security is assessed up to the maximum possible extent of a system or an application.

(Refer Slide Time: 03:00)

### Penetration testing: An Introduction

Penetration testing would attempt to verify which vulnerabilities are genuine - Real positive vs. false positive

Effective Penetration tests are those which target a specific system with a specific goal

Quality over Quantity is true test of a successful Penetration test

By carefully choosing valuable targets, a Penetration Tester can determine the entire security infrastructure and associated risk for a valuable asset.



So, what kind of things do we do in a penetration testing that would actually attempt to verify which vulnerabilities are genuine. So, while we could find out the initial list of vulnerabilities, what will typically happen is that some of the vulnerabilities would not really turn out to be a security issue. But it would be turning out to be what we referred to as a false positive where the issue would not be as it is claimed to be, but it would have been because of the fact that at that particular instant of time possibly it was acting as a vulnerability.

So, there was the differentiation of all the vulnerabilities that are identified between real positive and false positive, where in the real positive ones are the ones that need to be looked at from the perspective of trying to have an addressal will done for them, where false positives are sort of ignored at this point in time because of the fact that it is not really considered to be a very serious issue.

So, effective penetration test basically target or specific system with specific goal. So, the system here could be a standalone system or it could be one part of the network as well. And the goal will be very specific saying that I want to find out what kind of security issues are present in that particular system or in that part of the network or how could a potential hacker bring down a system or bring down that part of the network. So, essentially since a penetration testing actually tries to simulate what a malicious hacker from outside the network would possibly end up doing, you will find that the goals have to be very clearly specified for that entire testing effort to be very effective.

The next point that we will have to consider here is quality of the test cases that we are attempting to do as far as penetration testing is concerned is very very important as compared to quantity. So, it does not really matter whether we have actually run hundred different test cases. But if all those hundred cases have actually been and are not capable of having unearth some kind of vulnerabilities or a potential hacking entry points into my system or my network that I will be considered typically by the customer as sort of pretty much useless set of effort.

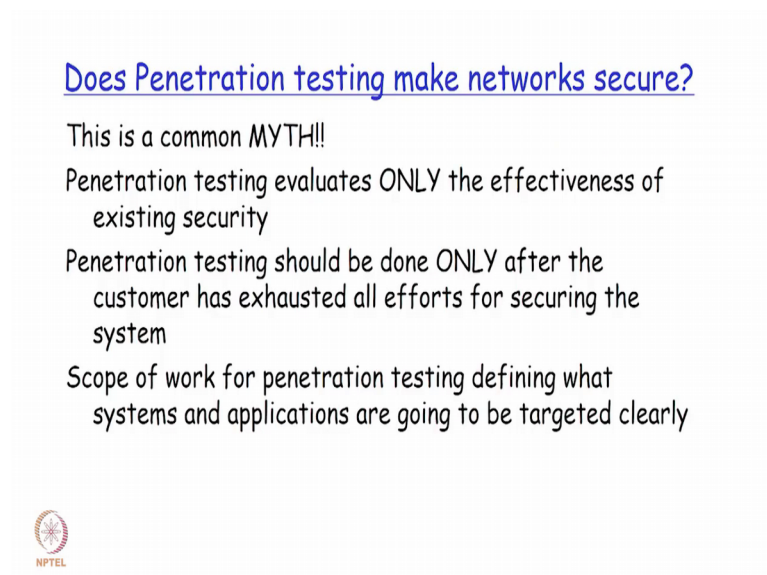
Whereas, if even if five or ten test cases have actually been covered and all of them have actually either proved the security is very good or it has actually exposed a sort of a loophole which the hacker could potentially leverage then that also would be more than sufficient as far as the completeness of the penetration testing effort is concerned. So, is

very important to note here the quality is more important than the quantity of the test cases that has actually been run. So, by choose carefully choosing valuable target, a penetration test can determine in the entire security infrastructure and associated risk for valuable asset.

So, as we will be seeing subsequently in the course, it becomes very imperative that the identification of the potential targets which the penetration tester should possibly used as an entry point into the system or into the network should be very carefully selected in order to ensure that the returns on the time and effort, the penetration tester is going to be actually employing is maximum right.

So, if I basically try to have a good set of targets that I have actually selected as a penetration tester I would possibly able to prove lot of targets loopholes that is present in the system or in the network very easily as compared to not selecting the appropriate target initially right. Where in I run the risk of not being able to have the all the all the loopholes extracted out or I would possibly be taking much more time than what is what should I have actually spent as a penetration tester to detect those loopholes, if I am not selected the targets correctly initially right.

(Refer Slide Time: 07:28)




Does Penetration testing make networks secure?

This is a common MYTH!!

Penetration testing evaluates ONLY the effectiveness of existing security

Penetration testing should be done ONLY after the customer has exhausted all efforts for securing the system

Scope of work for penetration testing defining what systems and applications are going to be targeted clearly



What are the most common myths that actually is circulating around in the entire industry is that if I do penetration testing, I can sort of assume that my network secure right. So, there cannot be a bigger myth then this because doing penetration testing and

identifying the results out of the testing whether it is telling you that all the test cases are actually passed meaning that there are no loops, there are no vulnerabilities or telling you that there are two vulnerabilities out of possible ten vulnerabilities that is there as a part of the test cases, is only a sampling that has actually been done right.

So, we will need to essentially understand that it is going to be very critical that not to have an opinion that having done penetration testing, we cannot really rest on a laurel that our network has become very secure, because it basically only evaluates effectiveness of the existing security on an auditing basis. So, I could potentially have certain things which should not have which possibly has not been evaluated by the penetration tester or something could have actually changed in my environment or in my settings. After I have done the penetration testing which could have actually opened up a loophole for hackers to get inside and there are so many other possibilities that are there.

And the second important point is that the penetration testing should be done only after the customer is exhausted of all efforts for securing a system right. So, for example, if the customer is just about to bring up a network. And he just connected a router, he has basically connected a set of devices into the router device, and sort of built up the network. It is actually not very useful if the first start with customer tries to basically do is hire a professional person to do a penetration testing on it right. Because there has been no security related checkpoints that are actually been put into the network or in his entire IT infrastructure for having any fruitful results of penetration testing.

So, essentially there has to be a firewall minimally right, there has to be some sort of malware protection software and so on and so forth. Only after the basic things are actually been sanitized and a customer has sort of thought through from his level and from his point of view what kind of checkpoint he has to put for protecting the entire network security. He should basically go ahead with trying to have the penetration testing effort started right.

And then the next point that we will have to also consider which is often not given that you importance is that the scope of work for penetration testing should be fine. What exactly what systems what applications running on the systems, and what part of the networks are going to be targeted as part of doing this penetration testing. Because otherwise it would basically be an exercise without a focus or without any kind of

specific targeted goal, so that is again another thing that needs to be considered very seriously. So, over the next few sessions what we are going to be actually ending up doing is that we will try to answer and learn a lot about the following questions.

(Refer Slide Time: 11:04)

### Over the next few sessions....

We will try to learn and answer the following questions:

How should the "possible targets" be researched?

How to identify potential vulnerabilities in different types of applications

How to defend applications against common attacks?

How can one offer a suite of penetration testing services?



How should the possible targets be researched? So, how do I identify what is an ideal target for a penetration testing to be done on a system or on network? How to identify potential vulnerabilities the different types of applications or different type of system that I have actually targeted out my first step? How to define the applications against a common attack? So, having identified the targets having identified what kind of vulnerabilities on existing on those identified targets, what is the steps that I need to take to sort of defend and sort of protect those vulnerabilities.

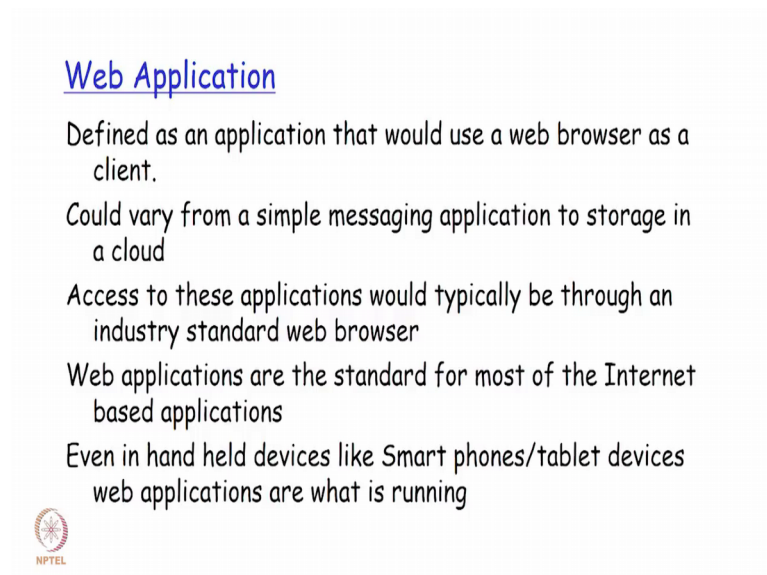
So, it could be either a patch for the application or it could be a patch on the operating system that I am running on the target or it could be a patch on my router device depending on what exactly is a system or what part of my network on which application that I have actually found the vulnerability on my target device right. And then how can I basically offer a complete suite of a penetration testing services a to a potential a customer who might be interested in ensuring that his entire system or network needs to be protected on a continuous basis.

(Refer Slide Time: 12:13)



So, we will actually take an example of a web application to discuss about the penetration, penetration testing concepts.

(Refer Slide Time: 12:16)



So, web application as we all would be knowing by now is basically an application that actually has two parts; one which is the client, and another which is a server. So, my web browser that I am running on my side of the the entire path is basically going to be the web browser, so that is going to be a my make client. It will basically tried to contact server for which I am basically trying to connect from my web browser has a client and

try to get some data or get some service done right. So, essentially it is going to be a web browser communicating to a web server on a remote side, and trying to get some data or execute some service as appropriate for the application that we are trying to.

So, it could vary from a very simple messaging application to something like a storage provider on a cloud. So, the application of the web that we are actually talking about could vary in terms of simplicity and complexity on both extremes. So, it could be as simple as a small messaging application or it could be a very complicated application also trying to do lot of things that in one in one application right.

So, access to these applications would typically be through when industry standard web browser. So, some of the most common web browsers that we actually make use of our as we all know is internet explorer, fire fox, chrome, safari and so on. But being a most common popular application browsers also has advantages and disadvantages. So, advantages here would essentially mean that in terms of the installation and in terms of the wide range of a support, we would actually tend to get very good very quick feedback and very good support as well.

But in terms of disadvantages it also would essentially mean that a foreign hacker as long as he knows that these are the standard set of a browser applications browser that is going to be used for this web application, there are already an existing set of vulnerabilities that are available for those standard web browsers. And specifically for each of those browser version as well right which could potentially be very quickly leveraged by the hacker.

So, for example, if I know that a particular web application is going to be supported by let us say and IE version 6 right. I know from other sources what are the potential vulnerabilities that are existing when I use IE version 6 as a browser client software for running any kind of web application. So, the hacker would immediately tried to test out whether those vulnerabilities are potentially could be made use of for compromising that particular web application server right.

So, first and foremost how will the hacker know which browser clients work for a particular server web application server, you will find that most of the applications web applications basically print in their home page itself, what is the best browser client software version that is actually working very well with that particular server right. So,



this is a very easy a set of information that I hacker could at could potentially be a leveraging on to find out first and foremost, what is the web browser client software that issued basically need to target on right.

Even the on all the smart tablet devices like a smart phones are a tablet device, you find most of them today or web application that is actually running, but the browsers running on the smart phone devices or an handheld devices are slightly different versions as compared to what you have on the desktop run on your server right. They are actually modified versions of the standard browser versions available on the normal desktop PCs, but it is suffice to note here that those modified versions also as documented set of vulnerabilities that you can very easily lay your hands onto get details.

(Refer Slide Time: 16:33)

### Web Application Penetration testing: Scope

Non-technical areas of this project scope could include:

- Acquisition mechanisms of devices by the users
- Possible uses of device usage other than this application
- Policies related to the maintenance of the server/network



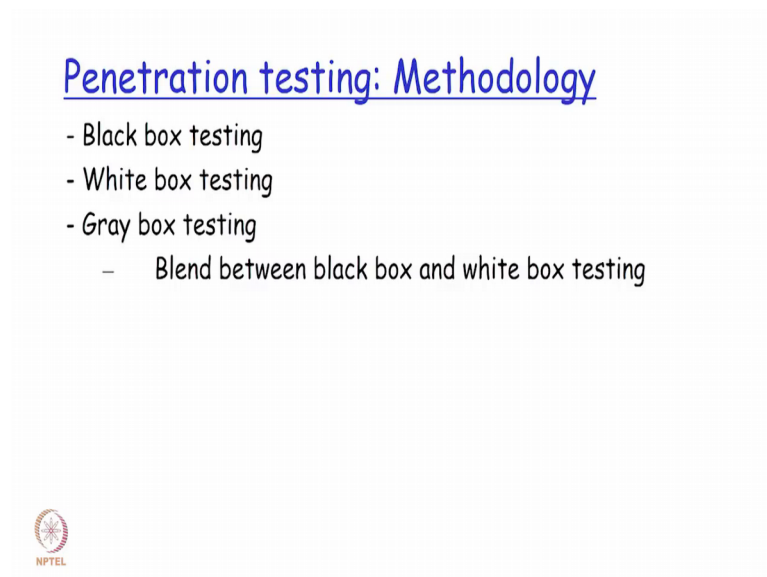
So, in terms of scope of web penetration, web application penetration testing some non-technical areas that when we need one should basically take care of his about acquisition mechanisms of devices by the user. So, other than the normal typical usage how are the device is going to be used after acquiring them by the user. So, for example, if network is going to be consisting of devices us let us say a smart tablet device or users are going to be making use of. So, we will also have to take note has part of the penetration testing where those devices are going to be made use of by the user.

So, for example, will the user take the device out from the premises to their let us say to their homes and also operate that same device from the network there right. So, in that

case we will actually have to have a mechanism ensure that certain type of application do not run on the devices it is actually taken out of the premises and then used outside the premises right. So, in that way, we will also need to have details about how and where the devices are also going to be made use of.


So, possible uses of device usage other than this particular application that is being targeted for penetration testing. What kind of other usages that this particular device is going to be put into use for. And then what kind of maintenance policy is that are there of the server or the network if the scope of the penetration testing is covering them right. So, when the maintenance testing is being done, when the maintenance is actually being done on that particular server or on the network, what kind of things are going to be done which could potentially expose a vulnerability or introduce a new vulnerability after this particular penetration testing effort has actually been completed.

(Refer Slide Time: 18:30)



Penetration testing: Methodology

- Black box testing
- White box testing
- Gray box testing
  - Blend between black box and white box testing



So, in terms of methodology you actually have different types of penetration testing, and you have a black box testing, white box testing; and blend between black box and white box testing called as a grey box testing that is there.

(Refer Slide Time: 18:42)

### Penetration testing: Black box testing

- Tester does not possess any knowledge of target network, company processes or services
- Requires a lot of reconnaissance
- Longer engagement since the real hacker can spend a lot of time studying targets before launching attacks



So, when you talk of black box testing, the tester the penetration tester will not actually have any idea of the target network or the company processes or the services right. So, the entire system the entire the topology sort to say will be a complete black hole for him, where in because of the fact that it does not have any detail at all about it, he would require a lot of reconnaissance that has to be done right.


So, subsequently in our later sessions we have going to look at in great detail about what reconnaissance is all about, and what kind of techniques are generally adopted to find out details about the entire system, and what is the methodology by which are you can get the complete details. But essentially in the black box testing because of the fact the tester is not going to have any details about what is being given as a target for testing there is a lot of effort and time that a hacker has to actually put in before the platform is there for him to actually launch the attacks finally right.

So, in that sense a black box testing for a hacker could actually turn out to be ending up having a requirement to send spend a lot of time for him to finally complete and sort of achieve his subjective of attacking the intended the target. So, in this case, he does not have any detail at all whatsoever about the entire system of about the entire network and he just told that this particular set of things has to be attack, and ask him to see whether how successful he is doing the attack.

(Refer Slide Time: 20:39)

Penetration testing: White box testing

- Tester has intimate knowledge of the system.
- Tester is provided with a lot of details about the system, network topology, company processes etc.
- More focussed on meeting a compliance need rather than a generic assessment
- Typically performed by inner security testing groups



So as compared to white box testing, where the tester I actually got a very intricate knowledge of the entire system. Tester is also provided with lot of details about the system about the network topology, so what kind of company security processes are there, what kind of operating systems are running on the servers and so on and so forth right. So, there is very little detail that a white box penetration tester need to sort of find, it very hard to get it because all the things are provided all the details are provided to him on a platter.

And then is basically asked to only do the testing from the perspective of what kind of vulnerabilities of possible given all these details to him right. So, this is not typically done by somebody outside the system, but this kind of white box penetration testing is done typically by the security team that is possibly there inside the organisation. And this will actually be done very very periodically much more periodically as compared to let us say doing a black box testing from outside.

(Refer Slide Time: 21:50)

### Penetration testing: Gray box testing

- Falls in between black box and white box testing
- Owner feels that some unknown information might be discovered by the penetration tester and tells a particular part to be skipped.
- Provided basic details of the target but privileged information is not shared



So, in between black box and white box testing you have a grey box testing, where the customer or the owner will feel that some part of the information that does not been disposed publicly could potentially be made available made detector mean will possibly be detected by the penetration tester. And therefore, tells one part of the entire system or the network or one part the application whichever is a target that is being tested right now need not be tested at all, so that basically gets removed from the scope of the testing. So, because of this particular detail the we cannot really call that the penetration tester is actually doing a black box testing because some part has actually been explicitly told by the customer now that needs not need not be tester. So, that means essentially the tester has been given some details in directly about what is the portion of that particular target right. Ah

And again looking at it from another perspective other than this portion that needs to be taken out of the scope the tester does not have any other details pertaining to the target under testing right. So, from that perspective, it turns out to be a black box. So, since it is partly a white box and partly a black box, this is the reason why something like this kind of a testing is referred to as a grey box testing right.

(Refer Slide Time: 23:18)

### Real attackers: Profile

- Tend to have some information about a target before making attacks
- Attackers choose a specific target
- Highly motivated and would have interacted with the target in some way possibly before the attack
- Since Real attackers use the Gray box attack typically, the penetration testers also tend to follow the gray box testing methodology



So, coming down to actually understanding who are the kind of people who will come and attack a system right. So, the real attackers typically tend to have some kind of an information about the target before they make an attack right.. So, it could be very very generic detail or it could be a very specific detail also that could have been actually source through non technical means maybe through contacting a friend on the phone and trying to get some details on the phone, or contacting the somebody over cup of coffee in a coffee shop and getting some details and so on and so forth right. So, they will try to have some kind of information about a target before trying to start making the attacks. And attackers will specifically choose a one single target at any point in time.

So, if they know that for an organisation, a mail server for example, is something which is very critical that could potentially be the first entry point that they might try to target to gain entry into the entire network or to sort of bring down the entire network in first shot itself right. And from a personal personality point of view, we will always find that the real attackers are highly motivated and charged ok. And this would be reflecting in them putting in some die hard effort ensure that they do not rest till they succeed in their mission of having a successful attack done on that potential target that has been identified.

And then most of the time will you find that with the initial information they have actual gathered through other non technical means, the real attackers would side will try to start

off do a grey box initially, but you will also find that when they are not been able to get the details from other non technical means initially the real attackers would also have enough motivation and inner enough charge in them to ensure that they actually spend all the time that is required to do black box testing even by spending hours and hours in doing the initial reconnaissance.

(Refer Slide Time: 20:36)

### Penetration testing : Scope contents

- Target System(s) identification
- Workframe time requirement
- Evaluation of targets
- Software and Tools used for penetration testing
- Stakeholders of this penetration testing
- Initial access level that is provided to tester
- Target space definition - What parts of the target is the testing to target?
- What is the level of compromise on the targeted system?
- Deliverable from the penetration testing



So, in terms of scope contains for the penetration testing, the initially the identification the target system then what kind of time frame moulded be potentially required to be spend and what will be willing, what will be the customer be willing to give them. So, what kind of targets and how to do an evaluation of them; so and what kind of software and tools that they are going to use for penetration testing right.

So, one point that we will have to note here is that while intuitively we might find the remind feel that a penetration testers will not basically disclose what kind of software and tools they are using for penetration testing, you will find the requirement for them to be making it public will be much more higher for the customers to get confident feeling that yes these report that have been submitted finally by the testers can be taken at face value right. So, you will find that the software, the tools the versions also are explicitly mentioned and decided upfront by the penetration tester after the targets have been potentially identified.

Then it also will basically talk about the stakeholders or penetration testing and what kind of initial access level that to be provided to the testers. So, this will basically determine whether it is a full black box, full white box or a sort of a grey box testing in the middle right. So, target space definition in terms of what part of the target is the testing to be done on the target right. So, if I am going to be basically targeting a particular network. So, should I basically concentrate on the core router or should I concentrate on the entire set of routers that is there a part of network and so on and so forth right..

Similarly, if I am basically going to be given a target for a particular application, so should I be basically bothered and try to attack only having the application successfully authenticate me or should I sort of go and attack till the application itself is brought down successfully by me as an unauthorised user right. So, this is basically what we mean by target space definition right. So, what is the level of compromise the target system and final deliverable from the penetration testing? So, all these will typically form part of my scope right. So, in the subsequent sessions, we will talk more about how penetration testing is done with the different kind of steps.

Thank you.