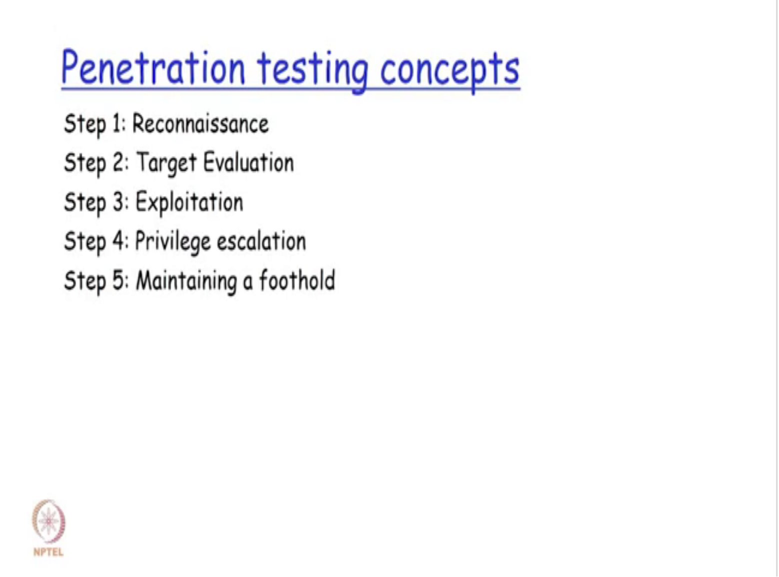
Information Security - IV
Prof. V. Vasan
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Module – 13
Lecture - 13
Penetration testing steps in Kali Linux

So, in this module we are going to actually discuss in very brief detail about the different steps, that are there as part of penetration testing. So, each of these steps, that we are going to be talking about in this module we will actually be looking at in create detail including, what tools are available in Kali Linux with the demonstration of them.

(Refer Slide Time: 00:34)



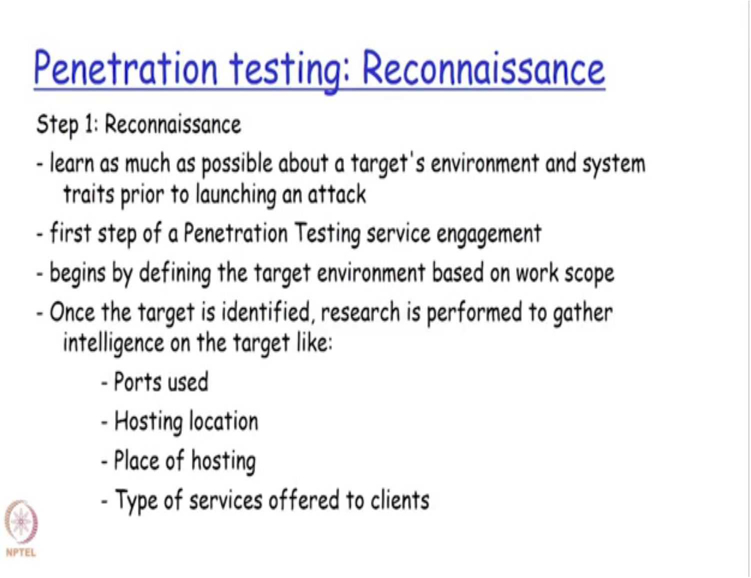
Penetration testing concepts

Step 1: Reconnaissance
Step 2: Target Evaluation
Step 3: Exploitation
Step 4: Privilege escalation
Step 5: Maintaining a foothold

So, in terms of the 5 different steps, that are there for doing the penetration testing first step is reconnaissance ah, the second is target evaluation, third is exploitation ah, 4th is privilege escalation and fifth is maintaining of foothold.

So, we will take a very brief look in this module on each of these steps and what kind of things we actually try to do in each of these steps ah, and then we will also look at subsequently, what kind of different tools are there? Which Kali Linux is providing us.

(Refer Slide Time: 01:04)



Penetration testing: Reconnaissance

Step 1: Reconnaissance

- learn as much as possible about a target's environment and system traits prior to launching an attack
- first step of a Penetration Testing service engagement
- begins by defining the target environment based on work scope
- Once the target is identified, research is performed to gather intelligence on the target like:
    - Ports used
    - Hosting location
    - Place of hosting
    - Type of services offered to clients

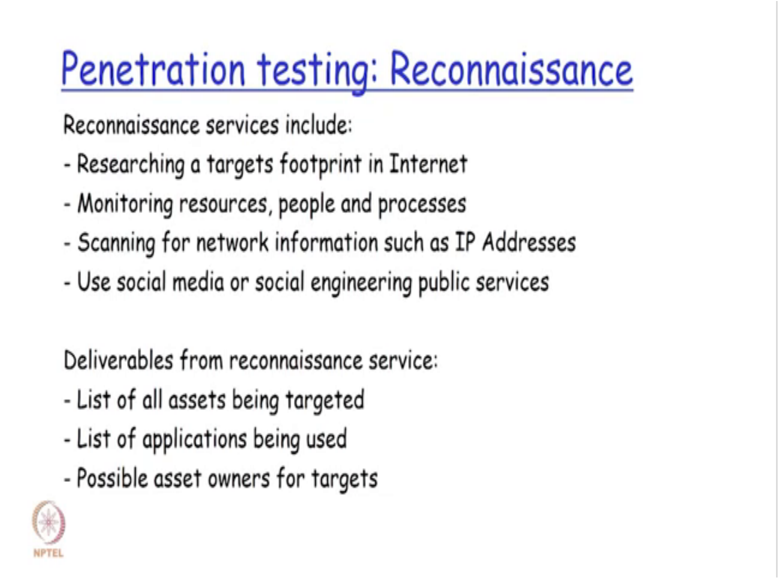
So, when you look at reconnaissance as we were discussing in the previous module reconnaissance is basically nothing but to learn, as much as possible details about a particular target ah. So, here we have identified a target and we want to know really what kind of things are being done on the target? What is the environment in which the target is operating? And what kind of very specific traits, that are there as part of that particular target, which I as a attacker could potentially make use of.

So, the first step of a penetration testing service engagement is basically this recognizance effort, that is done especially when I am actually doing the black box testing where, the customer has not given me any kind of a detail about the target, but I just told me what I have to do I would actually end up spending as a attacker the maximum amount of time in doing the reconnaissance, right? So, I basically try to find out once the target is identified, I try to find out what kind of ports that are used on the target if at all it is applicable.

So, as we have been discussing in more previous levels a port is basically a logical port, that we would typically have it open, whenever we run an app web application on a particular server, so to say and also we will try to find out where, is the hosting location right because, once we find out what the where the hosting location is, that would basically give us some details or possible entry points that, we can try to leverage on and then, the place of hosting and also what kind of services, that are actually offered to clients.

So, if it is basically a web application service, that will give me some ideas on how potentially I can attack? If it is basically a very simple service that, just displays the data then I would possibly need to look at from a different angle on what kind of potential loophole, that I can extract and so on and so forth, right?

(Refer Slide Time: 03:22)



Penetration testing: Reconnaissance

Reconnaissance services include:
- Researching a targets footprint in Internet
- Monitoring resources, people and processes
- Scanning for network information such as IP Addresses
- Use social media or social engineering public services

Deliverables from reconnaissance service:
- List of all assets being targeted
- List of applications being used
- Possible asset owners for targets

So, as part of reconnaissance we basically try to find out details about this. So, reconnaissance services include researching targets foot print and internet, right? So, because we all would have actually found out and experienced in some form or other how much of very detailed information one can really get on internet, right? So, even if he for example, search our own names and internet, we ourselves would possibly be shocked to know how much of detail, that is actually available which we ourselves would not have realized about us possibly even thought about, there being available in the internet, right?

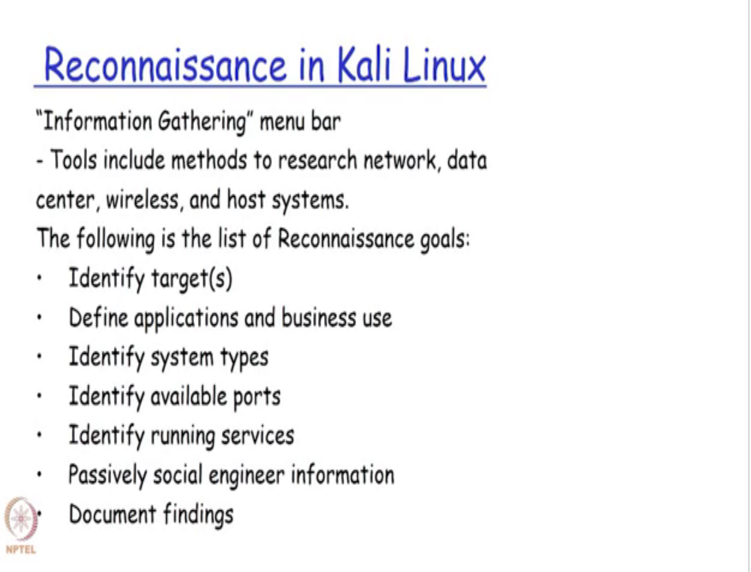
So, before I basically try to find out and try to get more details about that, particular target by trying to seek the information from the target itself one will basically try to find out more details about that, on the internet in potentially what kind of information I could gather and then, once I get those details I will basically also try to possibly do, any kind of monitoring that is possible on the resource or the people or the processors, right?

So, if I find out that the people are not very security conscious, I might try to do some techniques that, will get me some details about the network or on the system or the through them, right? And if I find that possibly the processes are not that, strict I might leverage certain loopholes in the processes to get more details as part of doing my reconnaissance, right? Or if I basically have to find out about the about the network there are different mechanisms by which I can find I can do a scan of the network to find out what kind of IP addresses are actually used, because for a attacker if the set of IP addresses have actually been received as he has actually found out, what set of IP addresses is actually used the network and if his target is potentially a device in the network.

We can very comfortably say that, 50 percent of his problem has actually been solved, right? So, one would possibly try to scan for network information as part of doing the reconnaissance and find out what is the IP address range, that is typically used in that network for us to do, more specific attack subsequently and then finally, in today’s world of social media, there are lot of information there is actually available in the twitters and the Facebook post, that could also be possibly used as part of the public information, that could have actually come in inadvertently and those information could potentially be the ones that, I am basically trying to test I mean I am basically trying to do the penetration testing of that, particular device for which information I am basically getting from my social media sites, right?

So, the deliverable typically when the reconnaissance service will be typically all kinds of assets, that are being targeted the list of applications, that are possibly being used on each of those systems if there are multiple system that, I am going to be targeting and also who are the potential owners for each of those targets because, the scope of the penetration testing could be actually to go and also bring down the potential asset owner also for that particular target device as well. So, depending on all these parameters amount of time that, one needs to spend for reconnaissance will actually be determined.

(Refer Slide Time: 07:03)



Reconnaissance in Kali Linux

"Information Gathering" menu bar

- Tools include methods to research network, data center, wireless, and host systems.

The following is the list of Reconnaissance goals:

- Identify target(s)
- Define applications and business use
- Identify system types
- Identify available ports
- Identify running services
- Passively social engineer information
- Document findings

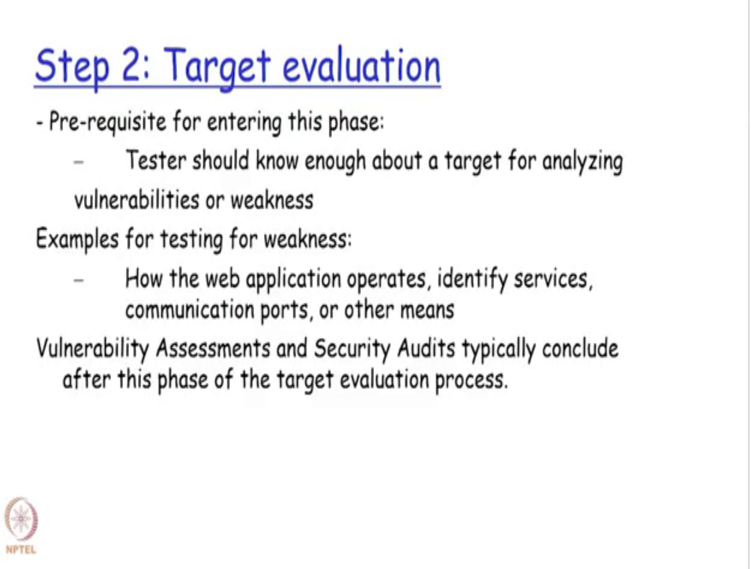
So, in Kali Linux we have a separate set of tools under a category called information gathering. So, here the tools that are include methods to research the network to collect details from a data center to do some very specific wireless network related information gathering, as well as do some very specific information gathering on whole systems, right? So, as far as the different types of reconnaissance goals are concerned one will be to identify one or more possible targets that, I will be actually looking at to successfully do an attack.

So, I will also be having the applications identified on those target systems and what kind of use that application is basically being put in to for, because depending on the use it will basically decide, how an attacker would typically target the application for attacking, then we will come the identification of the system type in this case I basically try to find out what kind of an operating system running on that particular system, right? Because, once I identify the operating system it is public information right now, on what kind of vulnerabilities are there in that operating system, which I will basically as an attacker try to keep at targeting 1 by 1 and seeing if any of them is still available on that particular system.

So, for example, if I know that, my particular targeted system is running windows 7, right? it is public information available in the internet for windows 7 what are all the known security loopholes, that is actually available and an hacker will basically try to first look at whether that, complete set has actually been sort of prevented in this targeted system or not, right? So, if not it basically becomes very easy for him to identify one set of vulnerabilities from that open list and use that, to gain an entry point into that particular target system, right?

So, they one identifies what are the available ports, that are open and then what kind of services that are running on that, and also any kind of information available by social engineering on that particular targeted system and then finally, document all these findings that are there in the previous things, that we talked about right from identification of the target. So, that a very thorough job of actually trying to look at the vulnerabilities by attacking each of those vulnerabilities can be done, right so, these are typically the goals that one tries to do as part of the reconnaissance step of penetration testing.

(Refer Slide Time: 09:54)



Step 2: Target evaluation

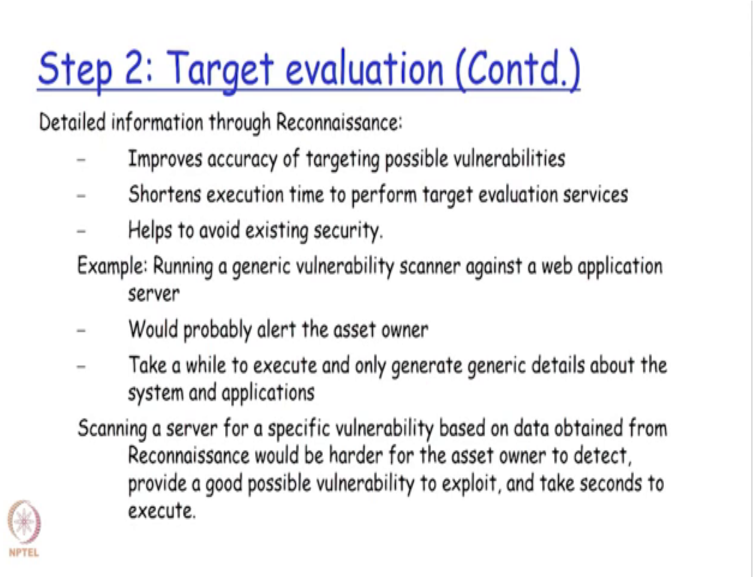
- Pre-requisite for entering this phase:
  – Tester should know enough about a target for analyzing vulnerabilities or weakness

Examples for testing for weakness:
  – How the web application operates, identify services, communication ports, or other means

Vulnerability Assessments and Security Audits typically conclude after this phase of the target evaluation process.

The next step comes a target evaluation. So, where I basically get details about, what are the information that, I have gathered as part of reconnaissance and then, I try to basically know more details about a target for analyzing what kind of vulnerabilities or weaknesses are potentially there. So, here I try to find out for example, if I am basically trying to test for weakness I try to find out here, how a particular web application is operating? What kind of services are running on that? What kind of communication ports are open? If any of those ports are open and whether I could potentially use that, port to get some sort of an entry point into the system or any of the other means that are possible.

(Refer Slide Time: 10:43)



Step 2: Target evaluation (Contd.)

Detailed information through Reconnaissance:

- Improves accuracy of targeting possible vulnerabilities
- Shortens execution time to perform target evaluation services
- Helps to avoid existing security.

Example: Running a generic vulnerability scanner against a web application server

- Would probably alert the asset owner
- Take a while to execute and only generate generic details about the system and applications

Scanning a server for a specific vulnerability based on data obtained from Reconnaissance would be harder for the asset owner to detect, provide a good possible vulnerability to exploit, and take seconds to execute.

So, again there are different kinds of tools that are actually available for doing the target evaluation, which will actually be used as part of this particular step in the penetration testing. So, detailed information through reconnaissance will actually be made use of here, so improves accuracy of targeting possible vulnerabilities because, as I was just telling you about earlier in the earlier module if I basically do not give lot of details to the tester penetration tester about what kind of system or network, that needs to be targeted I basically will try to sort of take more time as an attacker to find out because, I will basically have more reconnaissance effort that needs to be spent.

But the good point here is that, all the efforts that is actually going in through reconnaissance will be actually helping me in evaluating the potential vulnerabilities on the target because, the kind of details that I get out of that, report on reconnaissance will be useful for me to quickly zoom in on what are the vulnerabilities, that I could possibly exploit as a attacker on my targeted systems or network devices, right?

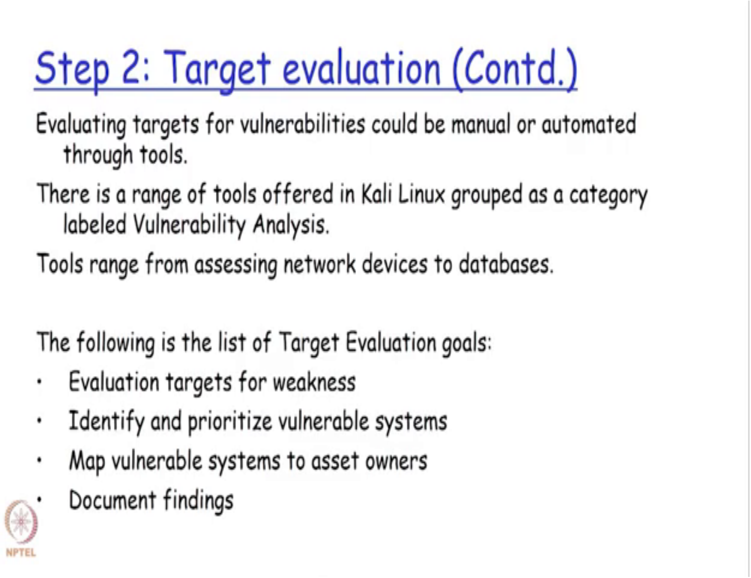
So, it basically shortens my execution time here, to perform the target evaluation services and also any kind of an existing security mechanisms that are, already sort of prevented from an attacker when prevented from an attacker making use of it would also be helpful here, because as I was just giving an example, if I know what OS is running there is a particular set of vulnerabilities, that is there in the OS out of which part of it could have been patched by the operating system vendor and part of it would be still open.

So, if those patches have already been applied and I find that those patches have already been there. So, I know that if a particular patch has actually happened then, for the evaluation of the targets I know or to the 10 listed vulnerabilities for this particular OS version phi of them are not going to be possible for me to use to get penetrate the system because, phi of them are already patched with the particular patch, that has been already applied on that particular target system, right?

And I example, that is actually given here ah. So, running a very generic vulnerability scanner against a web application server, because of the time that it is actually going to be taking a very long time would probably alert the owner and thereby giving a warning to him that ok, some sort of an activity is going behind the scenes because, as an attacker trying to take the entire resource on that, particular system by trying to find out all these kind of details would basically going to be alerting to the point of the application the actual application slowing down, right?

So, thereby it basically gives an chance for the owner to sort of get alerted and thereby prevent the attacker from actually happening whereas, if I basically have an individual reconnaissance reported has actually been done before, in which all these steps would have been done separately when I have done when an attacker does this separately what actually happens is that, the it becomes much lower chance for the owner to realize that, it is going to be possibly an attack that is actually right now happening or some effort towards an attack, that is right now happening and thereby it basically helps this step to get more successful as part of my penetration testing.

(Refer Slide Time: 14:27).



Step 2: Target evaluation (Contd.)

Evaluating targets for vulnerabilities could be manual or automated through tools.

There is a range of tools offered in Kali Linux grouped as a category labeled Vulnerability Analysis.

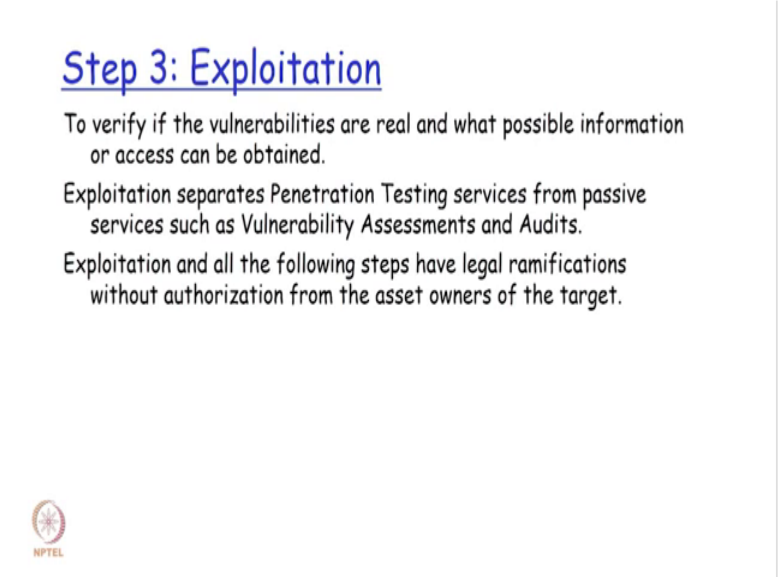
Tools range from assessing network devices to databases.

The following is the list of Target Evaluation goals:

- Evaluation targets for weakness
- Identify and prioritize vulnerable systems
- Map vulnerable systems to asset owners
- Document findings

So, evaluating targets for vulnerabilities could either be manual or automated through a different set of tools. So, again Kali Linux provides a range of tools, that we are going to be looking at in detail subsequently in our future sessions and all those tools are actually labelled under vulnerability analysis, right? So, the tools actually range from accessing network devices up to databases. So, it actually tries to cover a whole plethora of possible targets that, a penetration tester could have actually been given as possible target. So, the potential goals for target evaluation will be to identify targets for weaknesses identify and prioritize vulnerable systems, map vulnerable systems to the asset owners and again do complete document findings as we did in our first step.

(Refer Slide Time: 15:18).



Step 3: Exploitation

To verify if the vulnerabilities are real and what possible information or access can be obtained.

Exploitation separates Penetration Testing services from passive services such as Vulnerability Assessments and Audits.

Exploitation and all the following steps have legal ramifications without authorization from the asset owners of the target.

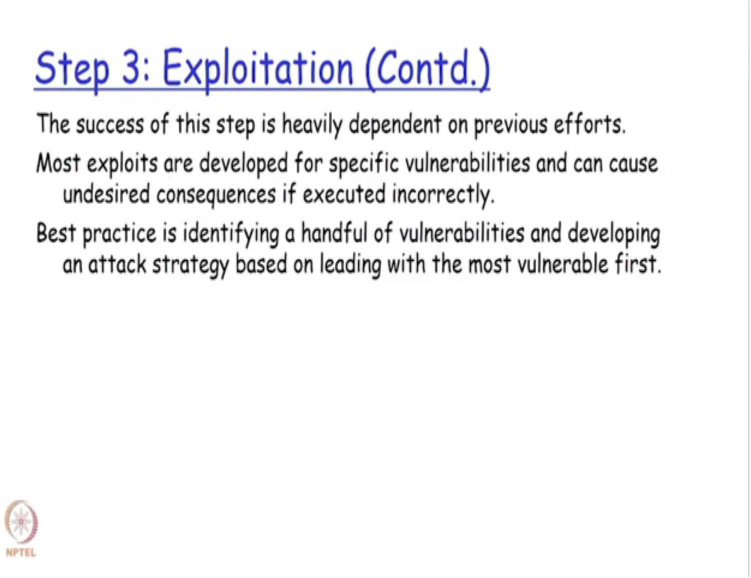
The third step is exploitation to verify if the vulnerabilities are real and what possible information or access can be applied can be obtained from the details, that that has been actually retrieved from the previous step of evaluating the target, right?

So, exploitation basically separates the penetration testing services from passive services such as, vulnerability assessments an audit. So, vulnerability assessment will not basically try to go and do the actual work of attacking, but it will only do an analysis of what kind of vulnerabilities are there, right? So, in that way it is very passive because it is not going to go and actively change or make any kind of services or processes, that is going to run on the targets by doing and vulnerability analysis because, it is only trying to gather information from there whereas, in the exploitation step the attacker will basically try to go and target the system itself completely, right?

So, in that way this is actually one step ahead of whatever we have been trying to do till the previous step of we trying to gather the details alone till of a target evaluation step, right?

So, in that way it will basically have certain legal ramifications also, which needs to be sort of documented and accepted by all these stakeholders for the penetration testing, right?

(Refer Slide Time: 16:47).



Step 3: Exploitation (Contd.)

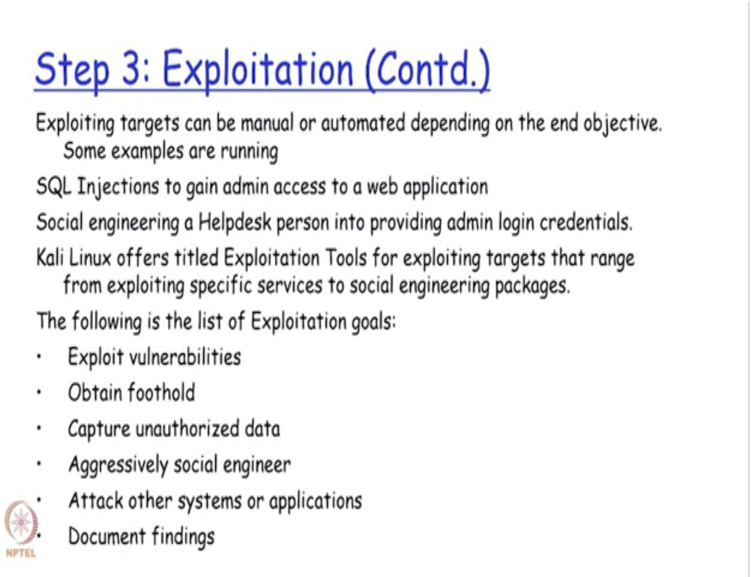
The success of this step is heavily dependent on previous efforts.

Most exploits are developed for specific vulnerabilities and can cause undesired consequences if executed incorrectly.

Best practice is identifying a handful of vulnerabilities and developing an attack strategy based on leading with the most vulnerable first.

So, the success of this step is heavily dependent on the previous efforts. So, the more amount of effort that has actually been put in previously, the quicker will be the time and the energy, that needs to be one needs to spend in this particular step of exploitation, right? So, as long as we are actually targeting some very specific vulnerabilities with different exploit scripts then, we will find that the success levels are much higher with some good ground work done in the previous 2 steps.

(Refer Slide Time: 17:16)



Step 3: Exploitation (Contd.)

Exploiting targets can be manual or automated depending on the end objective. Some examples are running

SQL Injections to gain admin access to a web application

Social engineering a Helpdesk person into providing admin login credentials.

Kali Linux offers titled Exploitation Tools for exploiting targets that range from exploiting specific services to social engineering packages.

The following is the list of Exploitation goals:

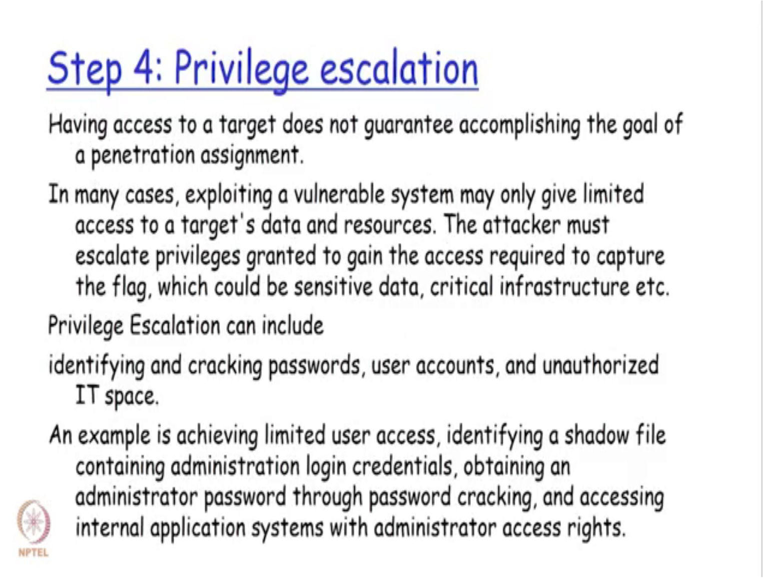
- Exploit vulnerabilities
- Obtain foothold
- Capture unauthorized data
- Aggressively social engineer
- Attack other systems or applications
- Document findings

So, exploiting targets again could either be manual or automated just like our target evaluation step and some examples could be there could be an SQL injection that could be done to get an admin access to a web application. So, as we look at some examples of some of the vulnerability analysis tools available in Kali Linux, we will see in detail how this is actually working I could for example, as an attacker try to do get some details about a helpdesk person from social engineering websites, that could give me some kind of an admin login credential.

So, for example, if I find that a particular social engineering website does not have very good security and I find out what is the login access that, particular admin person of this particular device targeted devices using on that, particular social engineering website and if I try to pa ex exploit the lack of security on the social engineering website and try to find out what is the password for this person on that site, I could gather some kind of details of how this admin person is setting his password and then, try to apply some very similar mechanisms to get admin access into this particular device, right?

So, using all these kind of details I could get access very quickly as part of the exploitation step in the penetration testing and again Kali Linux offers exploitation tools, category tools category under which there are different tools, that I could potentially make use of for exploiting some very specific vulnerabilities, right? So, the different set of exploitation goals is also mentioned here ah. So, exploiting vulnerabilities obtaining a foothold capture unauthorized data aggressively, try to gather details from social engineering websites attack other systems or applications and finally also document the findings for subsequent usage.

(Refer Slide Time: 19:12).



Step 4: Privilege escalation

Having access to a target does not guarantee accomplishing the goal of a penetration assignment.

In many cases, exploiting a vulnerable system may only give limited access to a target's data and resources. The attacker must escalate privileges granted to gain the access required to capture the flag, which could be sensitive data, critical infrastructure etc.

Privilege Escalation can include

identifying and cracking passwords, user accounts, and unauthorized IT space.

An example is achieving limited user access, identifying a shadow file containing administration login credentials, obtaining an administrator password through password cracking, and accessing internal application systems with administrator access rights.

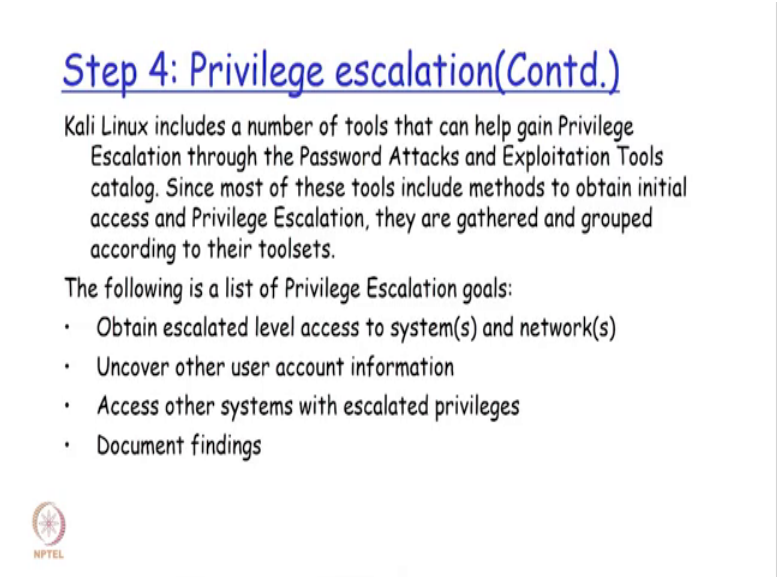
So, the next step is a privilege escalation where, most of the times what we will find out is that, if I if the attacker is basically successful in exploiting a vulnerability by exploiting of that vulnerability alone, he might not succeed in this objective of attacking and bringing down at that particular target, right?

So, because the vulnerability; might not give the attacker administrative privileges for bringing down a system or an application or a resource, right? So, once a vulnerability has been used for by the attacker to get into the system the attacker has to ensure the escalation of the privilege actually happens where, in with the escalation of the privilege the attacker will be successful in achieving his target of basically bringing down the identified target, right? So, in this particular case for example, let us say that, if attacker has actually exploited a vulnerability and got inside a Linux system the vulnerability has basically given him only a non-root access, right?

So, there are a very standard established known procedures, by which on a non-root admin access the administrator can actually try to get a super user access, right? So, there are different types of possibilities that are there, some of which could not be could not be successfully attempted on that particular system and some of which could be successfully attempted. So, the attacker would as a next step of doing the privilege escalation, will try to get a sort of a super user privilege on that particular system through, which he has no obtained the entry point of getting into the system by making use of some vulnerability, right?, but as I was telling you right now, that vulnerability has given him only access to a non-super user or non-admin privileges, but with that non-admin privileges he has to do something to ensure that, he basically gets a escalation of privilege to an administrator level, right? So, this step basically tries to find out what kind of things he could actually do.

So, some of the things, that could potentially can try to do is identifying and cracking the password with different kinds of password cracking programs try to penetrate different type of user accounts and also trying to get into unauthorized it space from this particular entry point, that he has got into the network, right? So, there are different tools, that are again available as part of the Kali Linux for doing the privilege escalation and we will again be seeing all these tools and understanding how they work to get a good idea about the about those tools.

(Refer Slide Time: 21:56)



Step 4: Privilege escalation(Contd.)

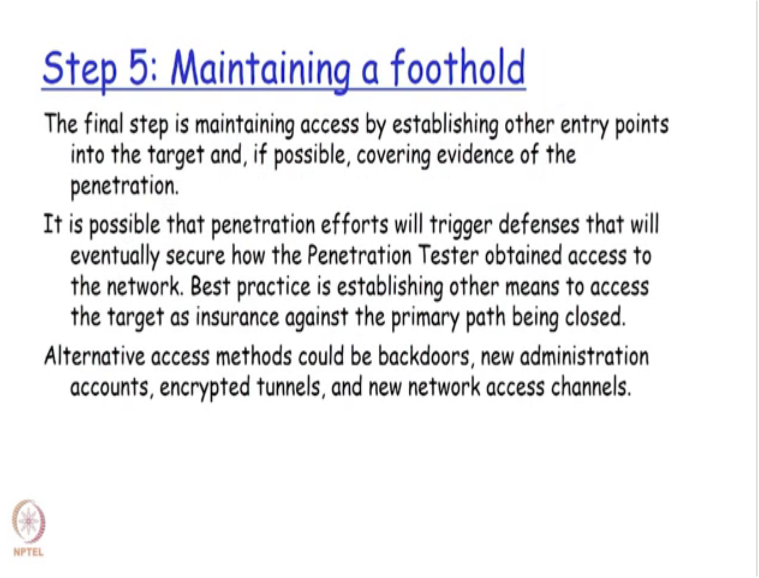
Kali Linux includes a number of tools that can help gain Privilege Escalation through the Password Attacks and Exploitation Tools catalog. Since most of these tools include methods to obtain initial access and Privilege Escalation, they are gathered and grouped according to their toolsets.

The following is a list of Privilege Escalation goals:

- Obtain escalated level access to system(s) and network(s)
- Uncover other user account information
- Access other systems with escalated privileges
- Document findings

So, as far as the different goals are concerned very clearly the goal is to obtain escalated level access to system and network. So, uncover other user account information, access other systems from the system which has been exploited with the potential vulnerability and again with escalated privileges and also do a complete documentation of all the findings in this particular step.

(Refer Slide Time: 22:27)



Step 5: Maintaining a foothold

The final step is maintaining access by establishing other entry points into the target and, if possible, covering evidence of the penetration.

It is possible that penetration efforts will trigger defenses that will eventually secure how the Penetration Tester obtained access to the network. Best practice is establishing other means to access the target as insurance against the primary path being closed.

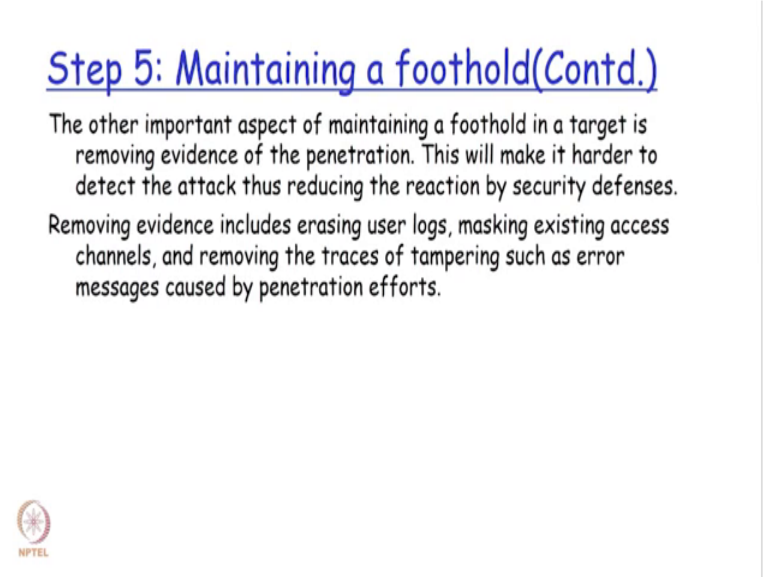
Alternative access methods could be backdoors, new administration accounts, encrypted tunnels, and new network access channels.

So, the last step as part of penetration testing is maintaining a foothold. So, what we mean by maintaining a foothold here is that? Once we basically exploit a vulnerability and penetrate the system we will have to do a couple of things mandatorily one we will have to ensure, that the attacker basically tries to cover up the all the entry points I mean clear up all the logs ah, that has been used by him or her to enter the system. So, that the owner basically finds it difficult to find out about what kind of mechanisms was used to penetrate into the system and then.

Secondly, also have some sort of other backdoors created. So, that even if this potential vulnerability has been, which has been exploited has been fixed by the owner of this particular target device this attacker could actually make use of other backdoors, that he has created as part of his access into the system currently, that we will actually can make use of in a subsequent attacks later on, right?

So, for example, if the attacker has actually come in as successfully penetrated of vulnerability today into the system and he wants to keep doing this penetration periodically, hence 4th also what attacker will actually try to do here is that, he will create other backdoor entries on that compromised system today. So, that even if the vulnerability, that he had used today to enter the system has been fixed by the by the owner of that, particular targeted device the backdoors that he has created today as part of his access could be used potentially by him tomorrow to get access into the same system. So, that is basically what we mean here by maintaining a foothold.

(Refer Slide Time: 24:21)



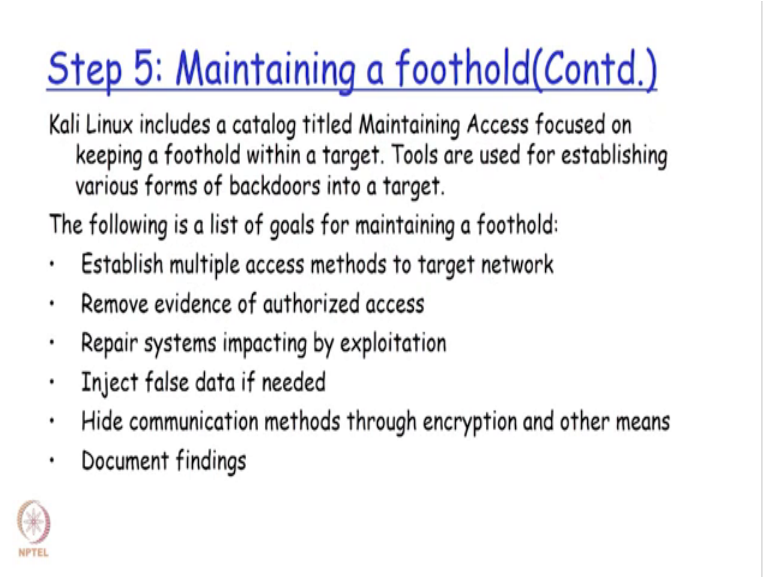
Step 5: Maintaining a foothold(Contd.)

The other important aspect of maintaining a foothold in a target is removing evidence of the penetration. This will make it harder to detect the attack thus reducing the reaction by security defenses.

Removing evidence includes erasing user logs, masking existing access channels, and removing the traces of tampering such as error messages caused by penetration efforts.

So, removing evidences including erasing the user logs is one aspect, that the attacker will actually try to do masking the existing access channels and removing the traces of tampering such as, error messages caused by penetration efforts, right, will also be done by the attacker as part of this particular step.

(Refer Slide Time: 24:43)



Step 5: Maintaining a foothold(Contd.)

Kali Linux includes a catalog titled Maintaining Access focused on keeping a foothold within a target. Tools are used for establishing various forms of backdoors into a target.

The following is a list of goals for maintaining a foothold:

- Establish multiple access methods to target network
- Remove evidence of authorized access
- Repair systems impacting by exploitation
- Inject false data if needed
- Hide communication methods through encryption and other means
- Document findings

So, the different goals, that are there as part of maintaining a foothold is to establish multiple access methods to target method as we were discussing now, removing the evidences of the authorized access, remove repairing the systems impacted by the exploitation.

So, inject the false data if needed basically to sort of unnecessarily divert the owner if the owner is basically trying to do an investigation of this attack. So, hide the communication method through encryption other means that the attacker is potentially using and also finally, document the findings as we have been doing in the other steps.

Thank you.