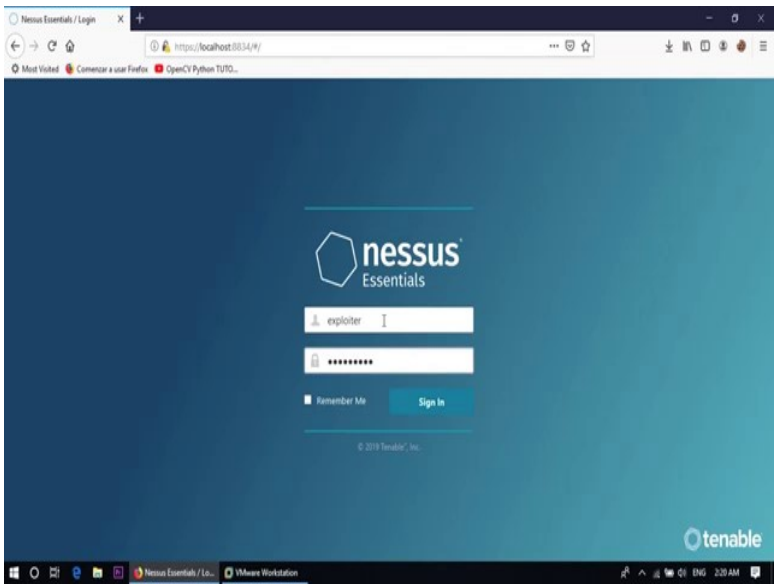
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

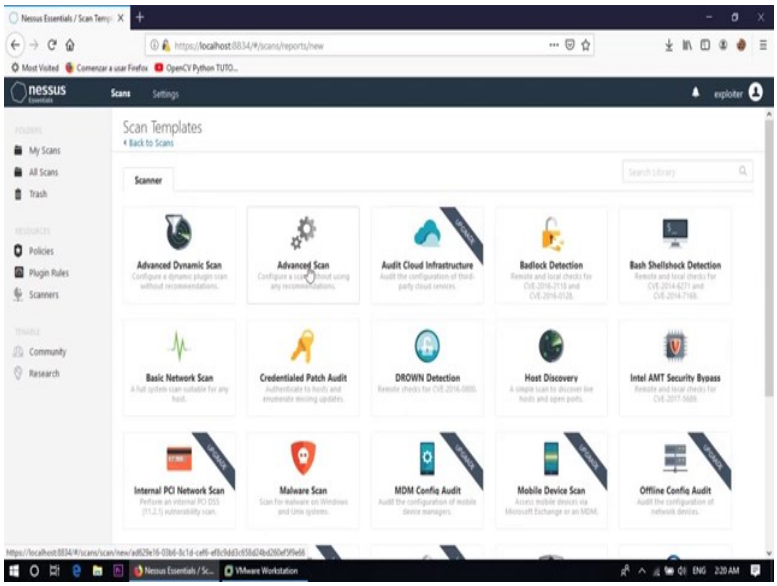
Lecture - 20
How to Use Nessus

(Refer Slide Time: 00:15)



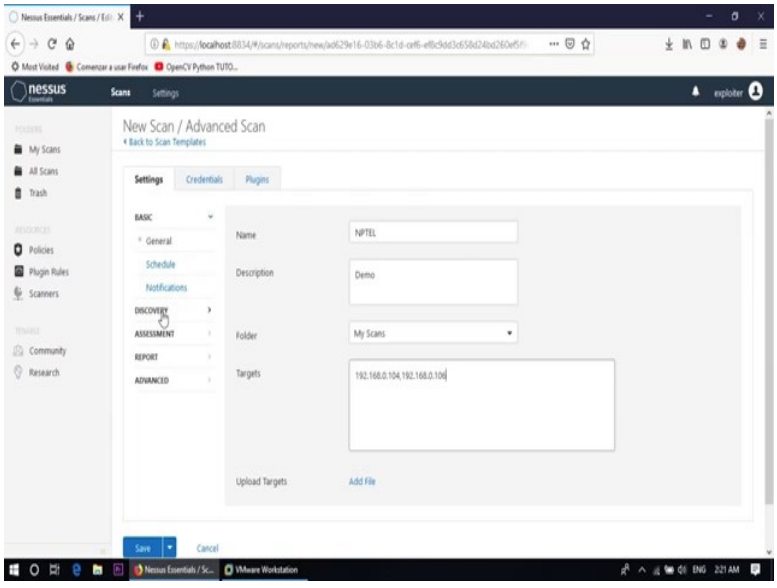
Now, today's session we will discuss about the vulnerability assessment using the tool Nessus. Here is my tool Nessus, first we need to login into the tool Nessus. So, use the login credential which you use at the time of installation.

(Refer Slide Time: 00:49)



So, here is the interface to scan a system, first we need to go to the new scan. So, there are several option are available: advance dynamic scan, advance scan, audit cloud infrastructure, badlock detection, basic network scan; lots of option are there. So, for the time being we are using advance scan.

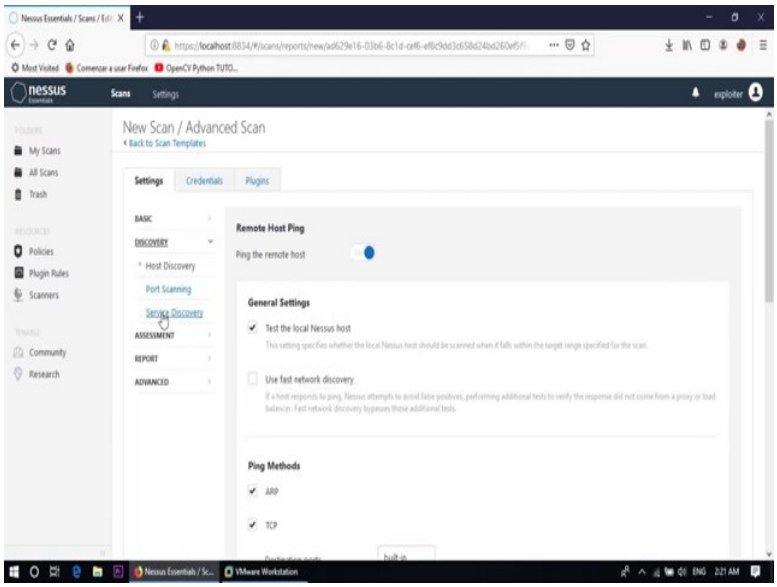
(Refer Slide Time: 01:23)



So, in these field first we need to put the name of the scan, suppose the name is NPTEL and description is a Demo, folder My Scans and target, so, in this case my target is sorry

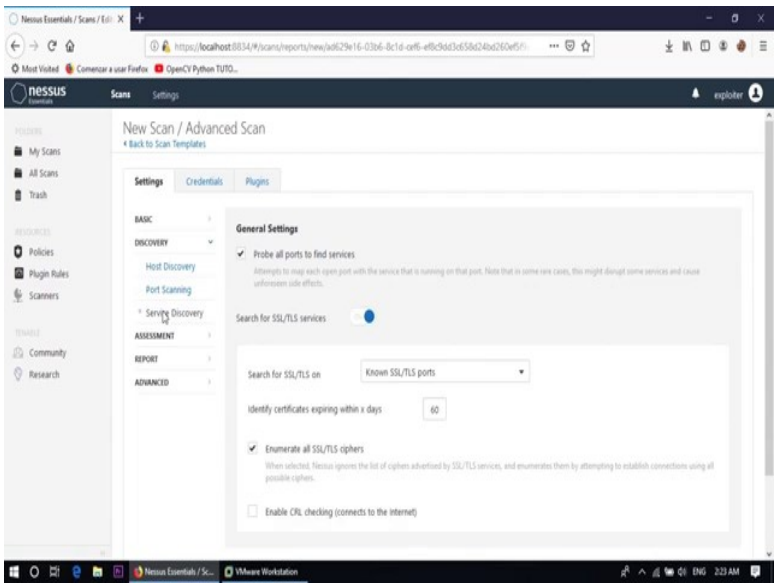
target IP address is 192.168.0.104 and 192.168.0.106. So, this way we can use multiple IP address for scanning separated by comma.

(Refer Slide Time: 02:33)



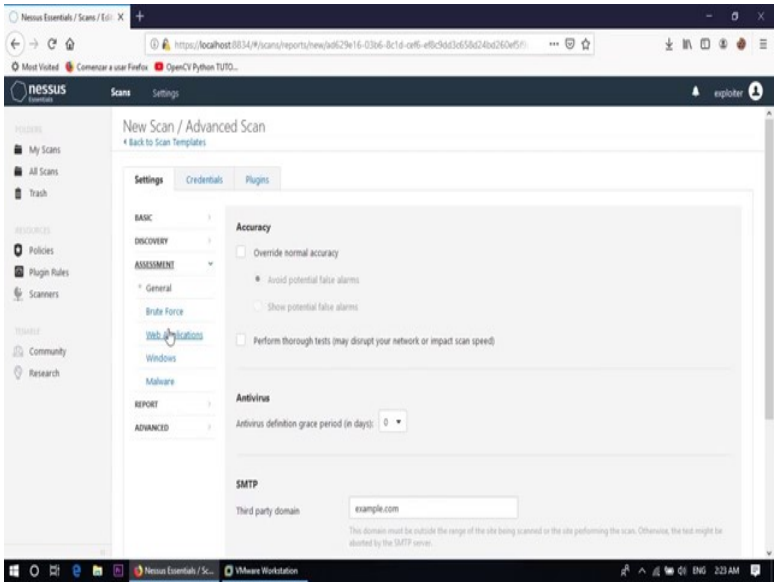
Now, where is all the option for discovery? Discovery option is a ping method, ARP and TCP and it also use the ICMP and maximum number of tries is 2; that means, it try twice for a particular request. Then port scanning part is also there to enumerate the local port to use SSH and WMI, SNMP and only run network port scanner, if local port enumeration failed.

(Refer Slide Time: 03:35)



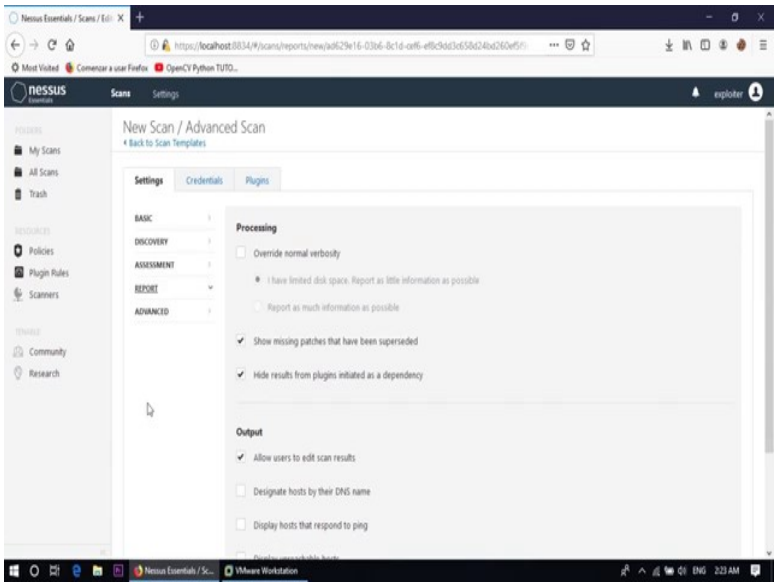
So, you can choose your own option, then service discovery enumerate all SSL or TLS cipher.

(Refer Slide Time: 03:47)



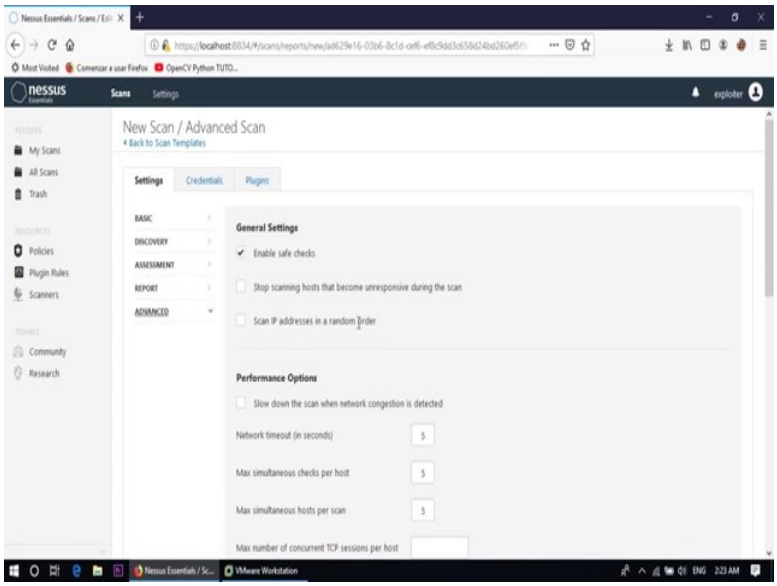
Now, assessment part is there and in assessment part Brute force assessment, web application assessment, then Windows assessment and malware assessment. All options are there, you can choose your own option; for the time being I am of the scan for malware.

(Refer Slide Time: 04:13)



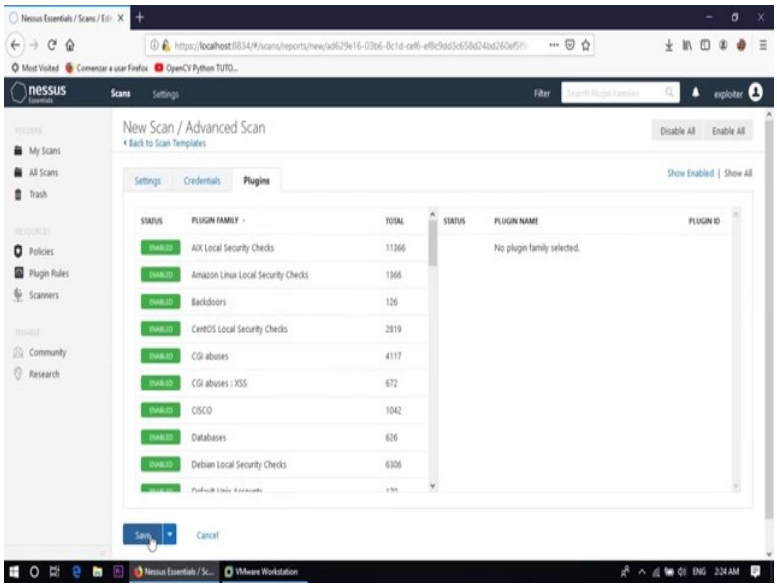
Then report we can also use this option to generate the report.

(Refer Slide Time: 04:19)



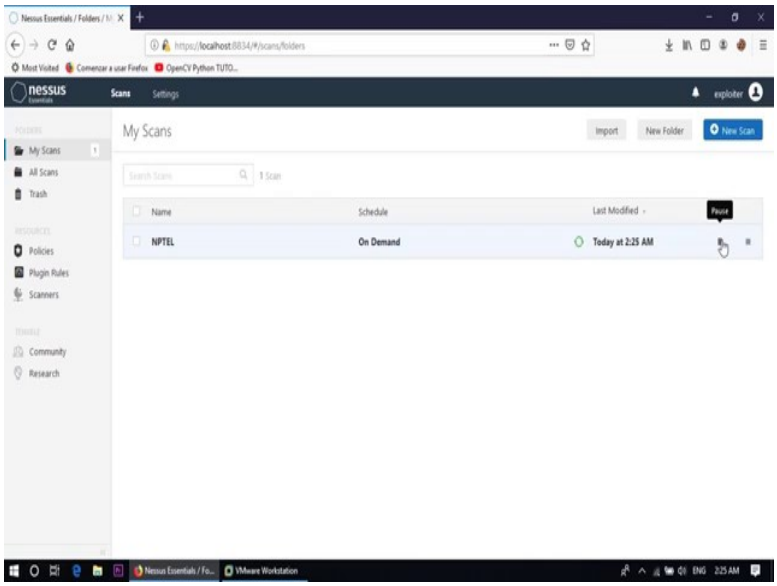
And in advance part there are some options are also there, network timeout; here network timeout is 5 and a maximum simultaneous check per host that is also 5. Maximum simultaneous host per scan that is also 5, you can also change your own option.

(Refer Slide Time: 04:41)



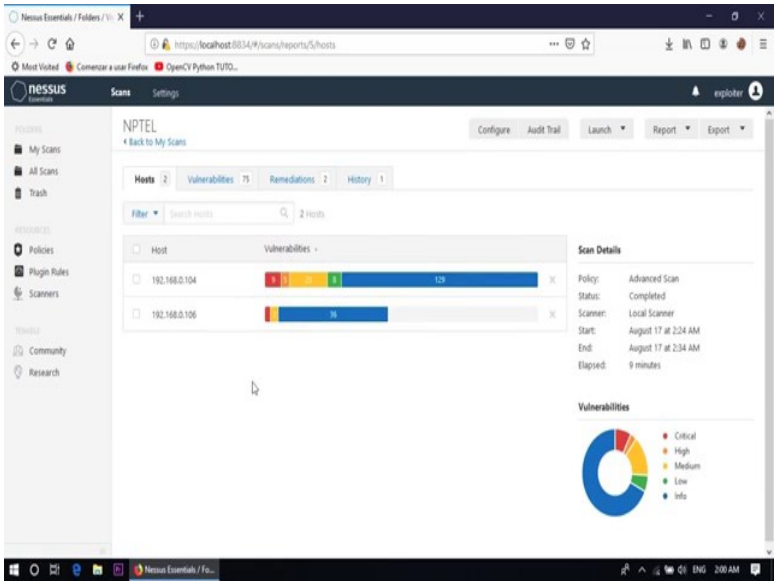
Now, where presidential is there and plug in part are also there. So, you already install plug in part which is show in the tool installation part. So, all the plug in are here which can help us to find out the different vulnerability right; save this scan.

(Refer Slide Time: 05:03)



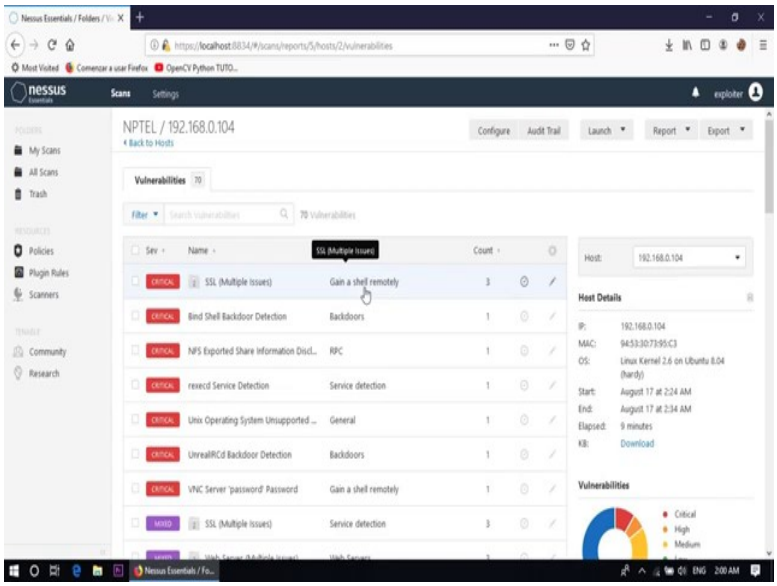
Now, I am starting the scan by clicking on the button launch, scan already started and it will take some time to complete the whole scan. And, once we got the scan result and by analyzing that result we can only find out the vulnerabilities and using that vulnerabilities further we can try to penetrate inside the victim machine. So, let us wait for some time to get the result of vulnerability scanning, now see Nessus complete the scan. So, let check the result.

(Refer Slide Time: 06:05)



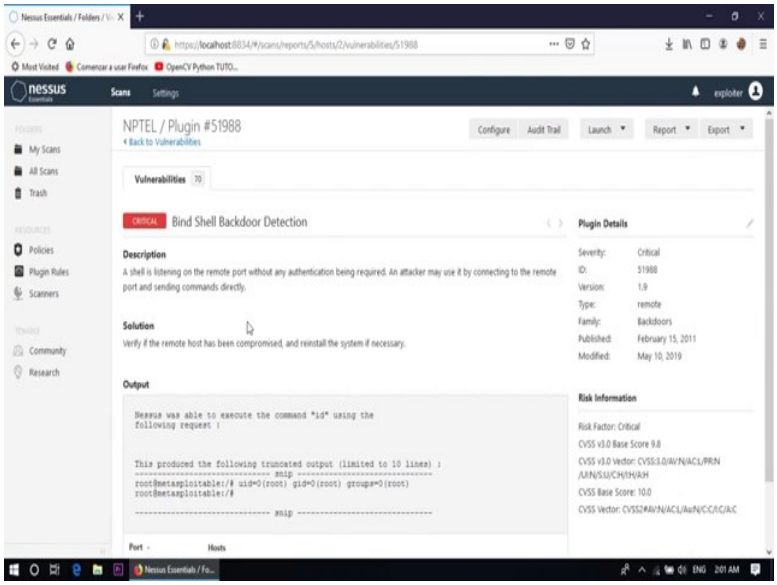
So, you basically scan for 2 systems, one is with the IP address 192.168.0.104.

(Refer Slide Time: 06:17)



And, it has several vulnerabilities, total 70 vulnerability is there and out of this 70 vulnerability 9 critical vulnerability is there, 5 high vulnerability is there, 23 medium vulnerability and 8 low vulnerability is there and 129 that all are the information. And, here is the details of all the vulnerability SSL multiple issues and a bind shell backdoor detection.

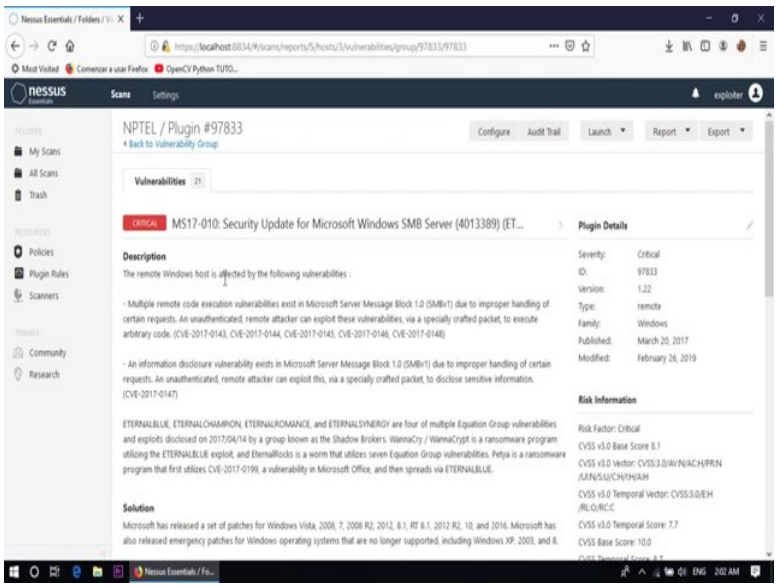
(Refer Slide Time: 06:53)



A shell is listening on the remote port without any authentication being required, an attacker may use it by connecting to the remote port and sending command directly. So,

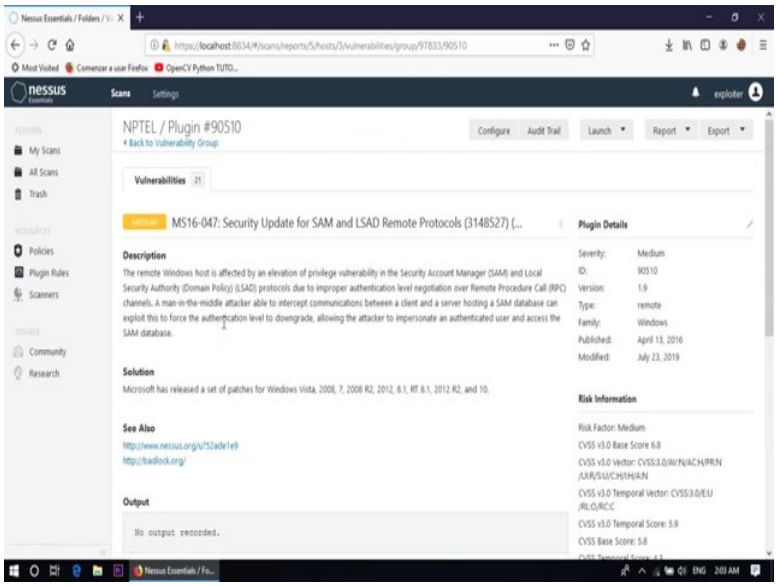
using this vulnerability one can attack to the victim machine and some other vulnerabilities also there. Let us check the other IP address 192.168.0.106, but I have total 21 vulnerability and 1 critical vulnerability is there and 2 medium vulnerability is there and 36 information is there.

(Refer Slide Time: 07:41)



And, see $MS17-010$ security update for Microsoft Windows SMB server and the remote Windows host is affected by the vulnerability with the CVE number $2017-0143$, $CVE\ 2017-0144$, $CVE\ 2017-0145$ and also $CVE\ 2017-0146$ and $CVE\ 2017-0148$. An information disclosure vulnerabilities also exist in this machine and some other vulnerability is also there.

(Refer Slide Time: 08:27)



Like in medium vulnerability $MS\ 17-047$ is also there, remote Windows host is affected by an elevation of privilege vulnerability in the SAM and local security authority. So, all the vulnerability and the possible solution are listed here. So, this way we can find out all the vulnerability using the tool Nessus and further we use all these vulnerability to penetrate inside the victim machine. So, this phase is basically call vulnerability assessment phase and in vulnerability assessment phase, we find out all the possible way by which a attacker can penetrate inside the victim machine.

But in the next phase; that means, in penetration testing phase a attacker can try with all these vulnerability to check which vulnerability is working and which one is not; so, that is called penetration testing. So, in the next week, in next tutorial I will show you how to use all the thing, all the information gathering part which we covered in this week and using all that information how can one penetrate inside the victim machine.

Thank you.