**DAY-10**

Now we are on the dashboard of Nessus web client

🡪Nessus is a vulnerability assessment tool

🡪Nessus gives some scanning policies to scan

Vulnerability assessment:

🡪It is a phase of scanning where we analyse the weaknesses, loopholes, vulnerabilities which might lead the hacker to attack and gain unauthorised access

Few vulnerabilities assessment types:

1.Active assessment

The ethical hacker/pentester directly interacts with target network and devices to find vulnerabilities

2.Passive assessment

The ethical hacker/pentester will perform sniffing the target network and analyse the data to find vulnerabilities

If you forget your Nessus credentials:

cmd(admin)🡪open Nessus folder where it is installed🡪cd “Nessus path”

🡪nessuscli lsuser

🡪nessuscli chpasswd “username”

New password: “Enter new password”

New password (again): “Enter password again”

Each and every vulnerability is categorised based on its risk factor

Vulnerability scoring system:

🡪A number given based on risk factor

**COMMON VULNERABILITY SCORING SYSTEM (CVSS)**

INFO (0.0-0.9)

LOW (1.0-3.9)

MEDIUM (4.0-6.9)

HIGH (7.0-8.9)

CRCITICAL (9.0-10.0)

Common Vulnerability and Exposure (CVE)

🡪Available in cve.mitre.org

🡪This organisation categorises vulnerabilities based on CVSS

🡪This organisation will assign a CVE number for each and every vulnerability in the following format

**CVE-YYYY (year)-NNNNN (number)**

and the vulnerability details are available at cvedetails.com

Nessus is an automated tool to perform vulnerability assessment.

On dashboard of Nessus after login

1. Click on new scan

2.Under vulnerabilities section click on advanced scan

3. Enter Name, Description(optional), and target ip or domain

If domain name does not respond give it as www.domain.com

To check whether the domain responds or not just ping it once

Modify the below changes before scanning:

Under Discovery section:

In host discovery:

🡪Disable ping the remote host

🡪Select all fragile devices

In port scanning:

🡪select all options of local port enumerators

🡪In network port scanner:

Select override automatic firewall detection

Select disable detection

In service discovery:

🡪Select probe all ports to find services

Under assessment section:

In general:

🡪Select override normal accuracy

Select avoid potential false alarms

In web applications (for web assessment):

🡪Enable scan web applications

Under report section:

🡪Select override normal verbosity

Select report as much information as possible

Under advanced section:

In general settings:

🡪select all

For multiple domain scanning disable “stop scanning hosts that become unresponsive during the scan”

Click on save

On dashboard:

Your scan is available. Click on it and launch it

After the scan is completed, you can generate a report in on of html, pdf and excel format.

Click Report and select pdf

Click generate report