امنیت شبکه

فعالیت شماره 2

In this project, you will learn:

* The vulnerability scanning concepts
* The vulnerability databases and OVAL
* The Metspolitable platform used for evaluation purposes
* How to set up OpenVAS with Web-based interface
* How to configure vulnerability scanning scope
* How to view and interpret the results of a vulnerability analysis

1. Review the attached slides on vulnerability scanning.
2. Install Kali Linux, Metasploitable and A Windows VMs in your computer.

Kali is a Forensic Linux distribution with many built-in information security tools.

After you turn on these machines, log in with default user name and password (note that the metasploitable machine displays the default user name and password when you turn it on). Then, check their network connectivity and their IP address. You can use “ifconfig” command for this purpose. If your machine has a valid IP address, record their IP addresses and you are set up for the next stage. If not follow the instructions to set up networking of your machines:

* In a command terminal, type:
  + ifconfig eth0 up (press enter)
  + dhclient eth0 (press enter)

1. Instructions on how to set up OpenVAS in Kali Linux:

OpenVAS is a powerful industry grade vulnerability assessment tool that is updated to latest vulnerability definition databases.

The procedure in **Kali** is as follows:

-open a terminal window (the installation process takes about half an hour)

-type: **openvas-initial-setup** 🡪 enter “toor” when asked for a password (the associated user name is “admin”)

-type: **openvas-check-setup** 🡪 wait until it is finished (it downloads plug-ins)

-type: **openvas-feed-update** 🡪 wait until it is finished (it downloads OVAL definitions)

-type: **openvas-nvt-sync** 🡪 wait until it is finished (it downloads NVT (Net Vul. Test) definitions)

# -type: openvas-scapdata-sync 🡪 wait until it is finished (it downloads SCAP (Security Content Automation Protocol) data

# -run: openvas-start 🡪 to start the above services (if you got error starting opnvas manager and administrator, try stopping and starting again: openvas-stop followed by openvas-start)

# C. Configure and run a vulnerability scan

# - Go to Applications>Internet>Iceweasal Web Browser> <https://127.0.0.1:9392/>> log in as admin

# -In the browser window: follow the Quick Start process, enter the IP address of your Metasploitable machine to scan.

# -Too see what type of scanning is running, click on Scan Management, click on Tasks, click on Immediate Scan of …, click on Full and Fast, review the list of scheduled tasks in this scan

# - After the scanning is complete, click on purple magnifier button to see report details, click on download full report to see the generated report.

# - Repeat the last three steps for Win XP machine.

# D.Prepare a report of your investigation including at least one screenshot in each of the above steps (A-C) (15 points). Include the final report of scanning and comment on the findings (5 points).