NET – 332

NETWORK SECURITY LAB

Lab 7. Passive Attacks and Reconnaissance

What are Passive Attacks?

- Passive Attacks
  - Network attack to monitor target systems, through port scanning or other means to locate and identify vulnerabilities.
  - Passive attacks include:
    - Active Reconnaissance
    - Passive Reconnaissance

How is it realized?

- Scanning
  - The first active action taken against target computer/network.
  - The action taken is based on the information gathered through ‘Foot printing’
  - Scanning allows penetrating deep into target network.
  - Usually done to identify the type, size and topology of network along with live systems and technology.

Scanning

- Ports and Service Scanning
  - Ports: Can be hardware/software, allow computers to communicate.
  - Service: An application running at the network application layer and above, allows storing, presentation and logistics of data.

Port & Service Scanning

- Port Scanning:
  - Refers to running a query in target computer/network to identify which ports is the machine listening on.
    - Ex: netstat –abno OR taskmanager with port column
    - Onlineportscanner
- Service Scanning:
  - Refers to running a refined and sophisticated query using specialized tools on target computer/network to identify which services are functioning. To be addressed in Systems Enumeration

What happens in Port Scanning

Identify Vulnerabilities that can be exploited

Port Scanning an IP – Hands on

Preparation: Download Port Query from vdrive folder

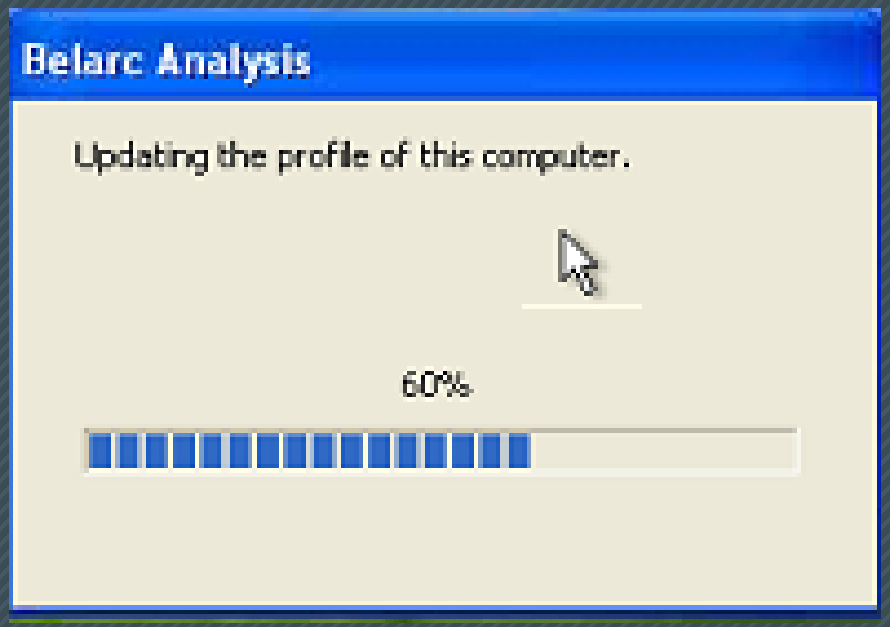
- Identify the computers in the network:
  - Open Command Prompt with Admin privileges
  - Run the command ‘Net View’
  - *Review the list of computers and select one computer as target – Note its name*
  - Unzip and Run the Port Query
  - Enter the name of the target computer in the Port Query Scanner
    - » Select ‘Manually input Query Ports’
    - » Enter ‘100-200’ in ports to query
    - » Click on Query
    - » Review the results of scan and note the port numbers on which the target computer is listening

Analysis of Port Scan

- Firewalls cannot protect the network if there are vulnerabilities in the systems:
  - Ex: Port 80 allowed through firewall
  - Anyone from outside can access this port
  - To identify vulnerabilities within the network / systems:
    - Vulnerability Scanner / Security Scanner
    - Functions exactly like hackers port scanner, used for vulnerability assessment.

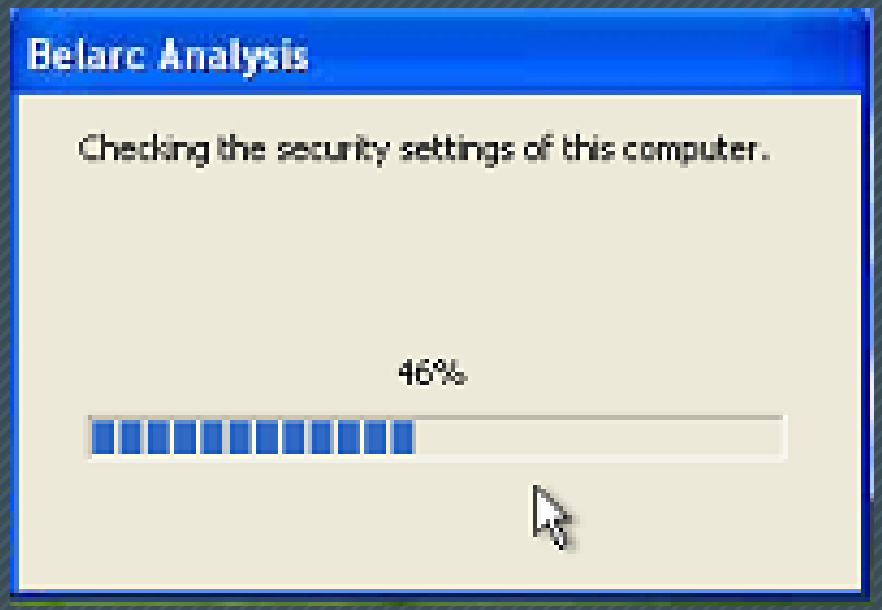
Vulnerability Scanner – Hands on

- Download *'Belarc Advisor'* from vdrive folder
  - Extract and Run the installable
  - Step 1: Allow the software to update the profile of the computer



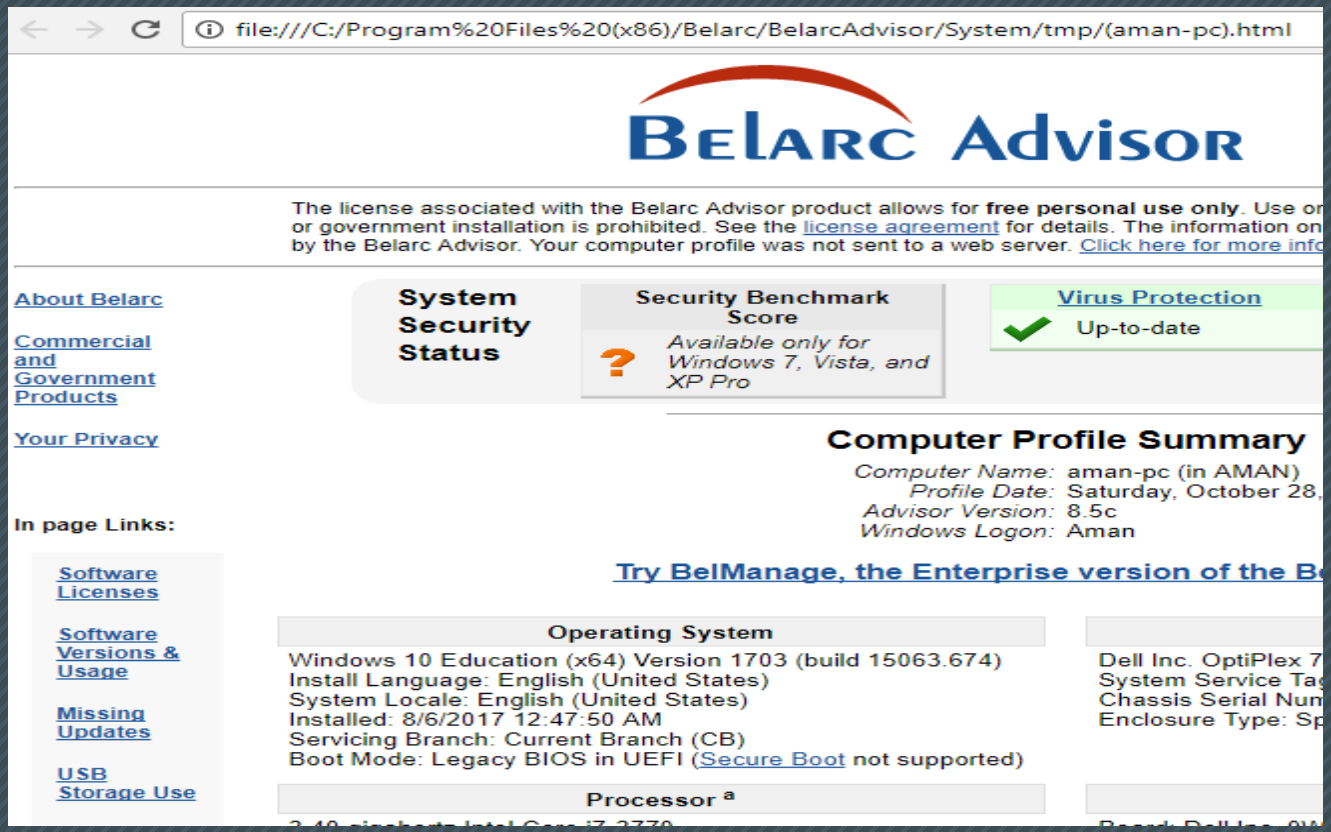
Belarc Advisor

- Post profiling the network of the computer, Belarc will start analyzing the security settings of the computer:



Reporting

- Belarc will revert with report as html file.
- Use any browser to view the report



Analysis of the reports

- Carefully review the following sections:
  - Operating System
  - Local Drives
  - Users
  - Virus Protection
  - Network Map
  - Software Installed

Report Work:

- Part A - Download the homework template from vdrive folder
  - Scan http://www.altoromutual.com using any online free port scanning tools.
  - Fill the template report with the answers.

- Part B – Scan your computer with BelarcAdvsior and prepare a report with screen shots for the following:
    - Operating System
    - Local Drives
    - Users
    - Virus Protection
    - Network Map
    - Software Installed

Questions