



## 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

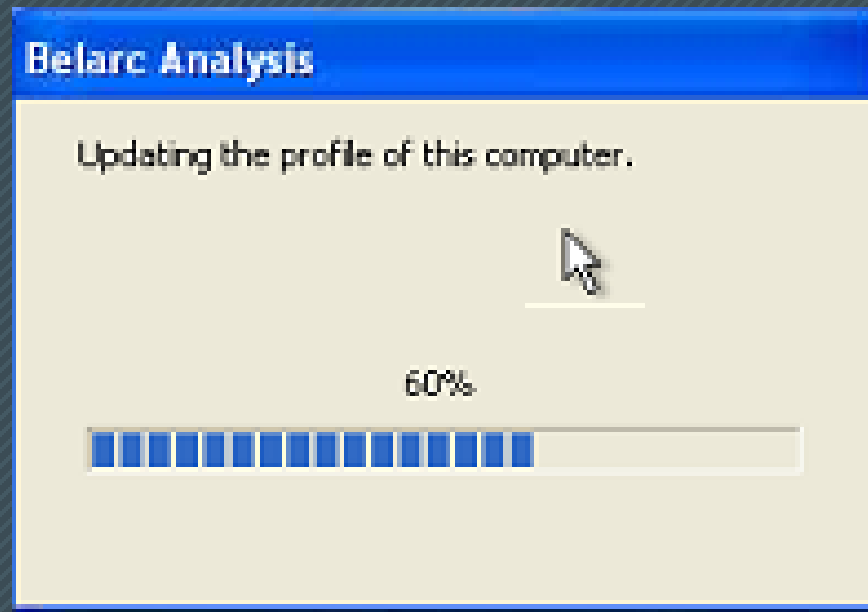
- Identify the computers in the network:
  - Open Command Prompt with Admin privileges
  - Run the command 'Net View'
  - *Review the list of computers and select one computer as target – Note its name*
  - Unzip and Run the Port Query
  - Enter the name of the target computer in the Port Query Scanner
    - » 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.

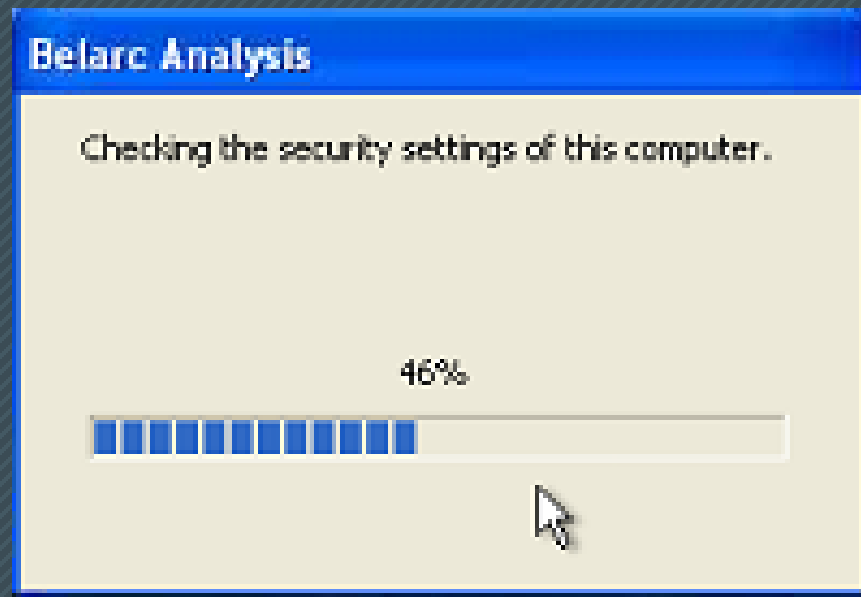
# Vulnerability Scanner – Hands on

- 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

The screenshot displays the Belarc Advisor web interface in a browser window. The address bar shows the file path: `file:///C:/Program%20Files%20(x86)/Belarc/BelarcAdvisor/System/tmp/(aman-pc).html`. The page features the Belarc Advisor logo at the top, followed by a license notice. Below this, there are three main status boxes: 'System Security Status' (marked with a question mark and noting availability for Windows 7, Vista, and XP Pro), 'Security Benchmark Score' (also marked with a question mark), and 'Virus Protection' (marked with a green checkmark and 'Up-to-date'). To the left, a sidebar contains links for 'About Belarc', 'Commercial and Government Products', 'Your Privacy', 'Software Licenses', 'Software Versions & Usage', 'Missing Updates', and 'USB Storage Use'. The main content area includes a 'Computer Profile Summary' with details like 'Computer Name: aman-pc (in AMAN)', 'Profile Date: Saturday, October 28', 'Advisor Version: 8.5c', and 'Windows Logon: Aman'. Below this is a link to 'Try BelManage, the Enterprise version of the Belarc Advisor'. The bottom section shows a table with system details under the heading 'Operating System', including 'Windows 10 Education (x64) Version 1703 (build 15063.674)', 'Install Language: English (United States)', 'System Locale: English (United States)', 'Installed: 8/6/2017 12:47:50 AM', 'Servicing Branch: Current Branch (CB)', and 'Boot Mode: Legacy BIOS in UEFI (Secure Boot not supported)'. To the right of this table, another table lists hardware details like 'Dell Inc. OptiPlex 7', 'System Service Tag', 'Chassis Serial Number', and 'Enclosure Type: Sp'. At the very bottom, a 'Processor' section is partially visible, showing '2.40 GHz Intel Core i7-3770'.

file:///C:/Program%20Files%20(x86)/Belarc/BelarcAdvisor/System/tmp/(aman-pc).html

## BELARC Advisor

The license associated with the Belarc Advisor product allows for **free personal use only**. Use on or government installation is prohibited. See the [license agreement](#) for details. The information on by the Belarc Advisor. Your computer profile was not sent to a web server. [Click here for more info](#)

[About Belarc](#)

[Commercial and Government Products](#)

[Your Privacy](#)

**System Security Status**

**Security Benchmark Score**

Available only for Windows 7, Vista, and XP Pro

**Virus Protection**

Up-to-date

### Computer Profile Summary

Computer Name: aman-pc (in AMAN)  
Profile Date: Saturday, October 28,  
Advisor Version: 8.5c  
Windows Logon: Aman

[Try BelManage, the Enterprise version of the Belarc Advisor](#)

Operating System	
Windows 10 Education (x64) Version 1703 (build 15063.674) Install Language: English (United States) System Locale: English (United States) Installed: 8/6/2017 12:47:50 AM Servicing Branch: Current Branch (CB) Boot Mode: Legacy BIOS in UEFI ( <a href="#">Secure Boot</a> not supported)	Dell Inc. OptiPlex 7 System Service Tag Chassis Serial Number Enclosure Type: Sp

Processor <sup>a</sup>	
2.40 GHz Intel Core i7-3770	Brand: Dell Inc. OptiPlex 7

# 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