TTKS0700 Data Security Testing

Lab 03. Vulnerability scan

Jarmo Nevala, 10.09.2019

jamk.fi

Lab 03. Vulnerability scan

Vulnerability scan

- GOAL
  - To understand basics of the VULNERABILITY SCANNING
  - To learn basics of OPENVAS

- In this document
  - RED color = TASK
  - BLUE color = TIP
  - Green color = Example

jamk.fi

Lab 03. Vulnerability scan

Watch the tutorial!

- https://www.youtube.com/watch?v=-2vjsHmq3ak

- Follow the tutorial and get your scanner up and running!!

Lab 03. Vulnerability scan

Vulnerabilities

- Look at the following links and learn the basic/common terminology
  - https://nvd.nist.gov/
  - https://cve.mitre.org/
  - https://nvd.nist.gov/vuln-metrics/cvss
  - https://nvd.nist.gov/config/cce/index
  - https://cwe.mitre.org/data/index.html
- Terms
  - Common Platform Enumeration (CPE)
  - Common Vulnerability Enumeration (CVE)
  - Common Vulnerability Scoring System (CVSS)
  - Common Configuration Enumeration (CCE)
  - Common Weakness Enumeration (CWE)

Lab 03. Vulnerability scan

Vulnerabilities

- https://www.cvedetails.com/vulnerabilities-by-types.php

1. Use searches (or browse vulnerabilities) to look recent vulns.
2. Select one software from your computer

    Use search to find vulnerabilities related to the software/vendor

Lab 03. Vulnerability scan

Feeds

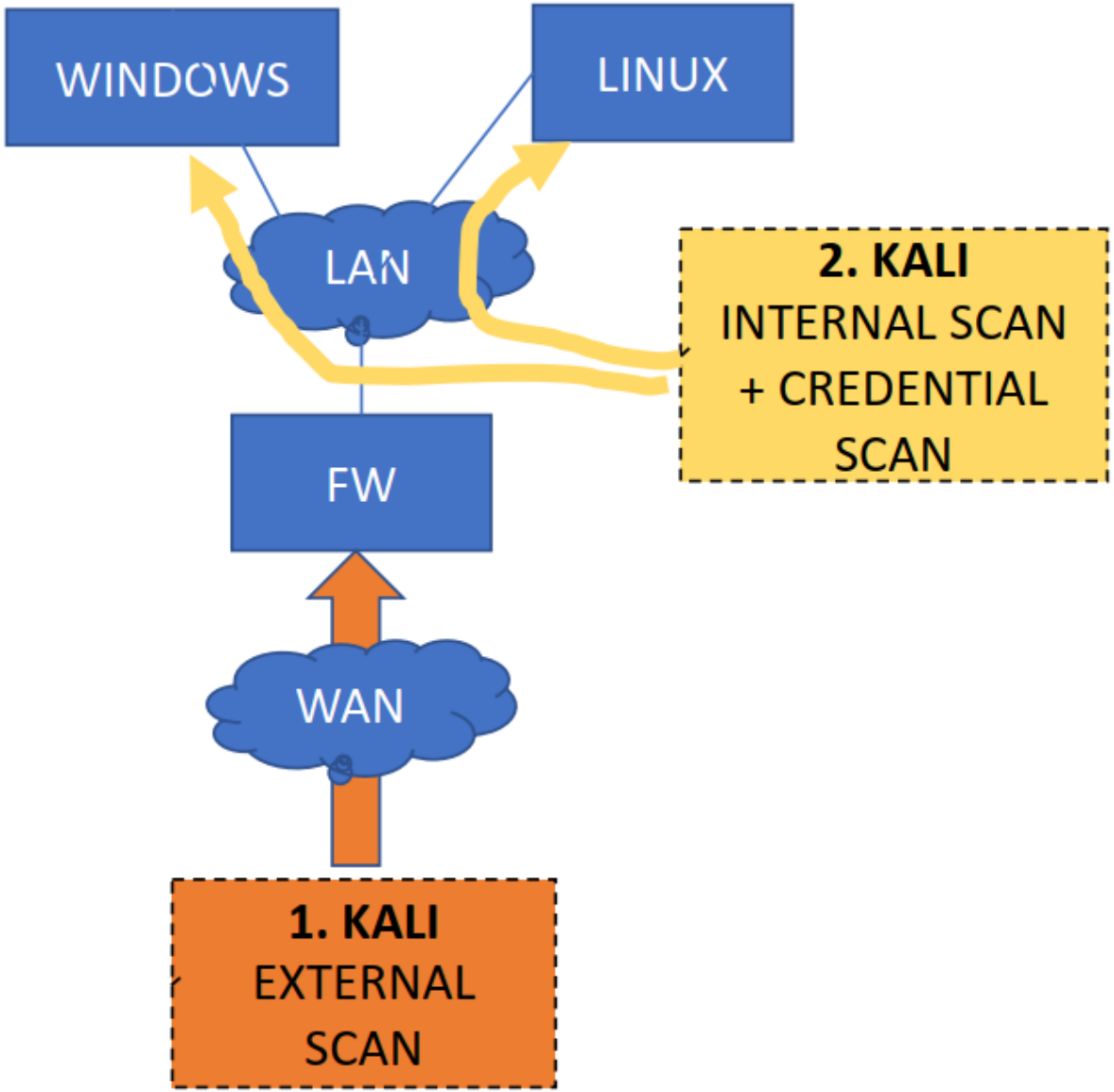
- https://community.greenbone.net/t/about-greenbone-community-feed-gcf/1224
  - Login as guest: https://secinfo.greenbone.net/

- ”It contains more than 50,000 NVTs, growing on a permanent basis”

- “For online-synchronisation use the command greenbone-nvt-sync to update your local NVTs”

Lab 03. Vulnerability scan

Setup



Lab 03. Vulnerability scan

External & Internal scan

- Run three different scans
  - 1. EXTERNAL scan from outside the firewall
  - 2. INTERNAL scan from internal network (against windows or linux – or both)
  - 3. RUN Credential scan (against windows or linux – or both)

- SELECT 3 different vulnerabilities that you found, and analyze those
  - CVSS metrics – what does it tell?
  - Look at the details of the results – what are the
    - IMPACTS
    - SOLUTIONS
    - VULNERABILITY DETECTION METHODS

jamk.fi

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences