Network Penetration Testing Methodology-Internal

6 Hr 43 Min Remaining

Instructions Resources Help  100%

Exercise 3: Scanning and Building a Target Database

Scenario

Once the tools are used, a target database must be created to prioritize targets. This is a critical step in producing the final report. The objective of this lab is to help students analyze the output of a tool and check if they can start to populate the target database used to produce the report.

In this lab, you will

* Scan for targets
* Conduct the scanning methodology
* Review the data from the scans
* Analyze the scan output
* Build an initial target database

**Lab Duration**: **10** Minutes

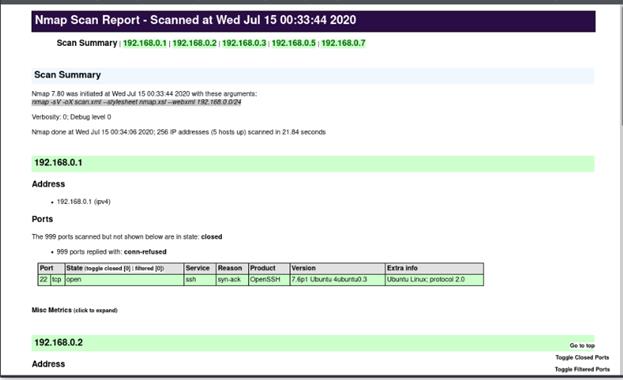
1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



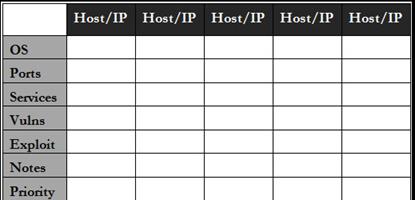
1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.



1. Launch a command-line terminal. In a terminal window, type **nmap** and press **Enter**. This exercise requires good understanding of the scanning methodology. A quick review of the commands is listed here, but not the graphic images.
2. Enter the following:
   * Live Systems: **-sP**
   * Ports: **-sS**
   * Services: **-sV**
   * Enumerate: **-A**
3. The output can be made into an XML format by adding “X” to the output option. This requires converting the output to HTML. Prior browsers could render the XML format, but this not reliable, since most browsers no longer allow such rendering owing to security settings.
4. Convert the file to HTML using the xsltproc command. Enter **xsltproc -o ~/scanresults.html /usr/share/nmap/nmap.xsl scan.xml**.
5. An example of the XML-formatted output is shown in the screenshot.



1. The XML format is a good choice for preparing and creating the database.
2. Next, populate the target database. For this, the following database information is required:
   * Host/IP
   * OS
   * Ports
   * Services
   * Vulnerabilities
   * Exploit
   * Notes
   * Priority
3. The database table key is as follows:
   * Host/IP: Include both items if available, or only the IP
   * OS: Include all information available in order to provide specific service packs, so that the target selection is easier
   * Ports: If too many ports exist, only include those relevant
   * Services: The service and the version to the best of knowledge
   * Vulnerabilities: The vulnerabilities discovered either with a scanner, manually, or through personal research
   * Exploit: Any exploit that can be linked to a vulnerability for the targets; if successful, write it in red
   * Notes: Any additional information discovered about the target
4. An example of the above is shown in the screenshot



1. From this point forward, create a target database for every opportunity, range, or environment.
2. This concludes the lab exercise.