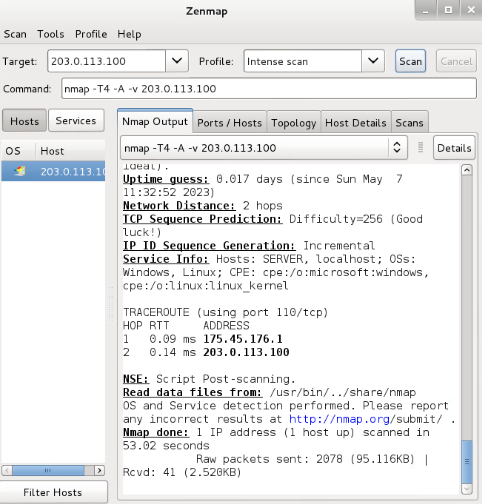
Lab 04: Remote and Local Exploitation

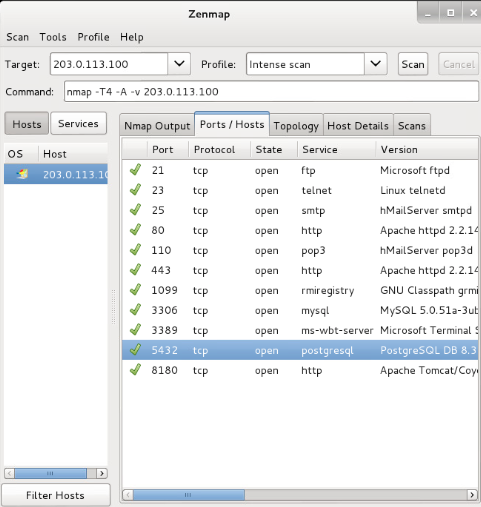
Lab report template Name: Kevin Ubilla

This Lab is required for Unit 3. It is worth 15 points. The Challenge exercise is worth 2.5 Extra Credit points.

1. **Nmap and OpenVAS, Step 10:** Please capture the portion of the display that says "**Nmap done:**" and shows the time required, and the number of raw packets sent for the scan and paste it below:

**→  ←**

1. **Nmap and OpenVAS, Step 10:** Please capture the portion of the report that shows the Host, Ports, and the Protocol, State, Service and Version for each port and paste it below:**→**Graphical user interface, text, application

   Description automatically generated **←**
2. **Nmap and OpenVAS, Step 12:** Please take a moment apart from the Lab to research what OpenVAS actually is (try Wikipedia and compare to Nessus while you are there) and discuss how OpenVAS relates to Nessus. (No more than 4 sentences, please.) Place your response below:

**→ OpenVas a GUI vulnerability scanning tool that is open sourced and uses Greenbone Community Feed to scan up to 50,000 vulnerabilities. Nessus is more of an off-the-shelf product with built in solutions while OpenVas is a better option for customization. ←**

1. **Nmap and OpenVAS, Step 13:** Please, like the prior question, take another moment to discover what Ice Weasel actually is and how it relates to Firefox. (Again, no more than 4 sentences, please.)

**→ IceWeasel is a fork of Firefox created by the GNU project. It focused on added security features that block zero length images files that create third-party cookies. Many cite the differences in name for trademark purposes as unimportant, but I think this is appropriate because Iceweasel’s patches are updated by Debian and not Mozilla’s Firefox. ←**

1. **Nmap and OpenVAS, Step 23:** Please capture the Greenbone Security Assistant report of the vulnerabilities found for **203.0.113.100** and paste it below. Just one capture, please, and just the highest-level vulnerabilities.

**→Graphical user interface, text

Description automatically generated ←**

1. **Nmap and OpenVAS, Step 25:** If you did find a "**PostgreSQL weak password**" vulnerability, click on that link to drill down to a more detailed explanation and capture it. If your report did not detect this vulnerability, click on another high-level vulnerability to display the more detailed explanation and capture it instead. Paste your capture below:

**→ Graphical user interface, text, website

Description automatically generated ←**

1. **Attacking the Target, Step 20:** Please capture the command prompt screen response after requesting postgres\_payload "**info**" and paste it below (you can stop your capture at “available targets:”):

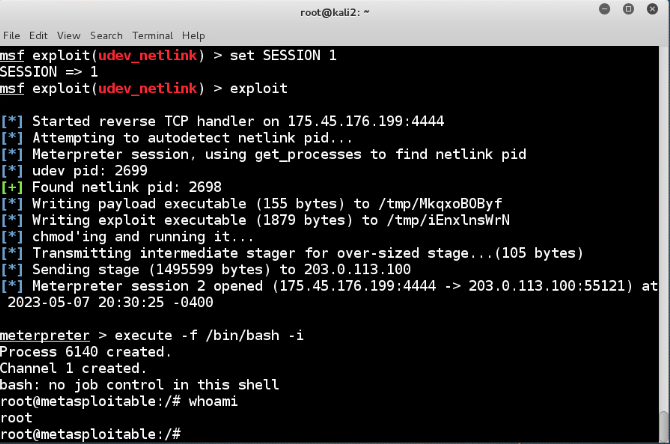
**→ Text

Description automatically generated ←**

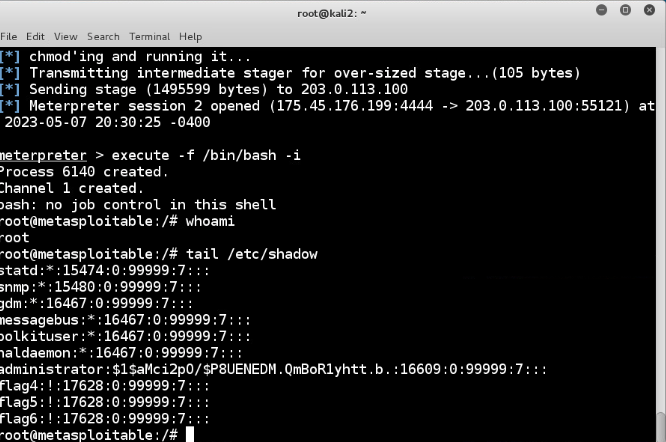
1. **Attacking the Target, whole section:** What is PostgreSQL? Place your response below.

**→ PostgreSQL is a free and open source data RDBMS or data warehouse for web, mobile, geospatial, and analytics. It supports more programming languages (Perl, C, Delphi, etc) than SQL. SQL is better for websites and online transactions while PostgreSQL is more applicable for larger, more complicated analytics. ←**

1. **Privilege Escalation, Step 7:** Please capture the response to the query "**whoami**" and past it below **(please remember to show the command as well as the response)**:

**→ ←**

1. **Privilege Escalation, Step 8:** Please capture the response to the command "**tail /etc/shadow**" in the command interface, showing at least 15 lines (or up to the next command). Paste the capture below:

**→  ←**

**If you encountered any issues, either positive or negative, with this Lab, please let me know by commenting here. (This IS an experiment, after all.) I am tuning this according to what you say.**

**→ ←**