NetSys Mapper

Intro to Cyber + Linux Fundamentals Project

NetSys Mapper is a three-phased reconnaissance mission.
Phase 1, "Network Mapping," commands a detailed survey of the internal network terrain, identifying all devices, their communication protocols, and strategic infrastructure points.

Phase 2, "External Intel Gathering," deploys digital surveillance via Shodan and WHOIS, examining the network's public presence and analysing traffic for operational security. Execute with precision to secure a comprehensive battlefield overview.

Phase 3, "Gather System Info." This task involves creating a smart script to dig into the system and pull-out key details. You'll need to find out network info like IP and MAC addresses, check how the system is running by looking at CPU and memory use, and figure out which files and folders are the biggest. Your mission is to do this neatly and efficiently, giving us a clear picture of what's going on inside the system.

Project Structure:

Phase 1

1. Map the Network - Present a network map showing ALL the devices in your home network.

1.1. Display Devices IP Address.

1.2. Display Devices MAC Address and Vendor (First 3 blocks, e.g. 12:4F:C2:XX:XX:XX).

1.3. Display the Router's Internal and External IP Addresses (Last 1 block, e.g XXX.XXX.XXX.123).

1.3.1. Use [ ] to wrap around each . (e.g. 10[.]123[.]123[.]123)

1.4. Display Device Names.

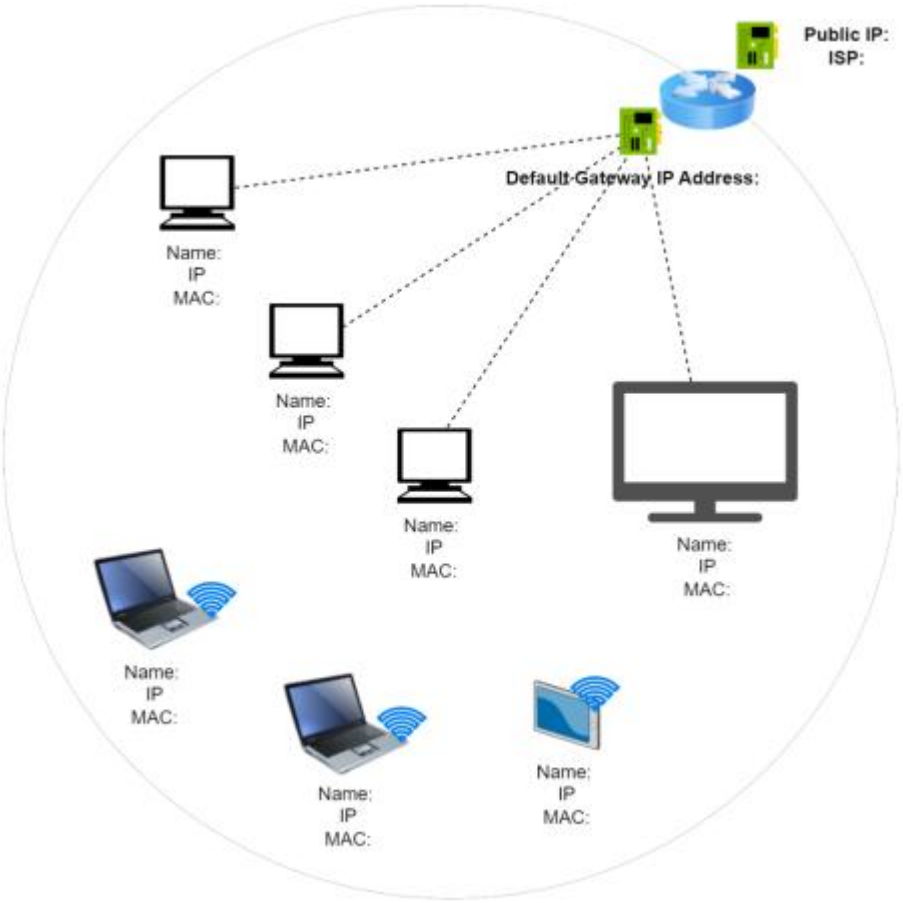
1.4. Display the DNS and DHCP IP Addresses in your Network.

1.5. Display your Internet Service Provider (ISP).

1.6. Display if the Device is Connected via Ethernet or Wireless.

1.7 Display the Operating system (OS) and version of your devices.

Sample Network Map



Phase 2: Collecting Information

2.1. Use Shodan to Check Your Public IP Address.

2.2. Use WHOIS to Check Who is Registered on Your Public IP Address.

2.3. Sniff Your Network and Identify Three (3) Used Protocols.

2.3.1. For Each Protocol Explain Its Usage.

2.3.2. For Each Protocol, Find the Used Port Number.

General Websites available: shodan.io, viewdns.info, draw.io

Phase 3: Automated System Info Extractor

Create a bash script that does the following:

3.1. Identify the system's public IP.

3.2. Identify the private IP address assigned to the system's network interface.

3.3. Display the MAC address (masking sensitive portions for security).

3.4. Display the percentage of CPU usage for the top 5 processes.

3.5. Display memory usage statistics: total and available memory.

3.6. List active system services with their status.

3.7. Locate the Top 10 Largest Files in /home.

General Tools and Commands: curl, ifconfig/ip addr, top, ps, du, find, standard Bash scripting utilities.

Project Deliverables:

1. **Script (Phase 3):**
    - Make use of the scripting techniques learnt — variables etc
2. **Comments (Phase 3)**
    - Use comments in your code to explain what you did so that yourself and the reader understands what you are trying to achieve
    - If you are using code from the internet, add credit and links. In the script, write the student's name and code, the class code, and the lecturer's name.
3. **PDF Report:**
    - Submit a PDF document providing an introduction to the project, the project objectives, methodologies, and outcomes. It should also include your network schema and the network details for Phase 1.
    - Documentation explaining the purpose and usage of each command.
    - Include screenshots of the command used or the process that shows the necessary information such as IP address etc.
4. **Video Recording of Individual Presentation**.
    - Submit a .mp4 video recording of your project presentation, showcasing the project, the methods used such as walking through your code and show your script in action and the final results.
    - The video should not exceed 5 minutes, keep it concise and clear.
    - Your face should be in one of the four corners of the video to prove that this is your personal work.
5. **Submission**
    - Submit the Source code (.sh) (Phase 3) and a PDF file with Network Map (Phase 1) and all other screenshots proving the methodology and script work (All 3 phases).
    - File Naming: UNIT.STUDENT (e.g. CCK1_240101.s5.pdf, CCK1_240101.s5.sh etc.)
    - Upload the project to your individual google drive folder
    - Last Submission: 23:59 of the project submission deadline. Folder will be denied access thereafter.