## Lab 11: Using Scanless for Easy Anonymous Port Scanning

### Scenario

CyberHex Technologies, a mid-sized financial services company, recently noticed unusual network behavior, including unexpected external traffic patterns. While their internal systems are protected by firewalls and intrusion detection systems, they are concerned about how much of their infrastructure is visible to outsiders through open ports. Since port visibility is a key step in many cyberattacks, their cybersecurity team decided to assess the exposure of their systems.

To do this securely and without revealing their own IP address, the team is leveraging **Scanless**, a tool that allows port scanning through third-party web services. This approach helps demonstrate how attackers could map the company’s network anonymously and highlights the importance of restricting unnecessary open ports.

In this lab simulation, you will use **Scanless** on ParrotOS to perform anonymous port scans against a controlled target. This exercise will showcase how attackers can gather reconnaissance without exposing their own machines, reinforcing the importance of monitoring for external scans and hardening network defenses.

### Solution

The company hired you as a certified cybersecurity practitioner. Your primary objectives are to install and configure Scanless on ParrotOS, select and utilize various online scanners supported by the tool, perform an anonymous scan against the target system, and analyze the scan results to identify exposed ports and services. This demonstration will walk through the process of installing Scanless using pip in ParrotOS, running it with different supported scanner options, and understanding how Scanless forwards requests through external services to help maintain anonymity during the scan. Finally, the results will be reviewed and interpreted to identify open ports and the services associated with them.

By completing this lab, you will gain hands-on experience in performing **anonymous port scanning,** understand how attackers may use third-party tools to hide their identity, and recognize the importance of proactive port management.

**Scanless** is a Python-based tool that leverages multiple online scanning services to check open ports on a target. By using third-party scanners instead of direct probing, it masks the attacker’s identity and provides anonymity during reconnaissance. Since different scanners test different sets of ports, running multiple scans ensures broader coverage and helps simulate how attackers may identify weak points in a network.

**Note:** This lab is for educational and authorized testing purposes only. Never scan systems, networks, or applications without prior permission from the owner.

|  |
| --- |
| 1. Turn on the **ParrotOS** virtual machine. Open a **Terminal**, and execute the **sudo su** command to run programs with root privileges. First, we need to set up **pip**, a package manager that allows us to download and install Python-based tools. In many Linux distributions, pip is already pre-installed, but if it is missing from your system, you can install it with the following commands: **apt install pip**    2. After ensuring pip is available, the next step is to install the **Scanless** tool itself. ParrotOS uses **Debian’s Python policy**, which blocks pip install directly into the system Python to avoid breaking system packages.      We can create a virtual environment. This keeps packages isolated and avoids system conflicts. To create a virtual environment, enter: **python3 -m venv scanless-env.** To activate it, enter: **source scanless-env/bin/activate**.    3. Now, to install scanless itself, enter a simple command: **pip install scanless**    A screen shot of a computer program  AI-generated content may be incorrect.  4. Before running any scans, it is a good idea to explore the tool and understand the options it provides. Start by checking the help screen with the following command: **scanless -h.** This will display all the available commands, flags, and usage examples.    5. Once you are familiar with the help menu, the next step is to see what scanners are available through Scanless. Type: **scanless -l.** This command will display a list of supported external scanners along with their respective sources. Each of these scanners operates slightly differently, and you can choose which one to use based on your requirements.    6. Now, let us try running an actual scan. You can specify a target host (either a hostname or an IP address) along with the scanner you want to use. The command structure looks like this: **scanless -t [Target hostname or IP] -s [Scanner Name].**  Here, you would replace the placeholders with your actual target and the scanner of your choice from the list you obtained earlier. Remember, it is essential to have explicit authorization before scanning any system. Running port scans without permission is illegal and against ethical security practices.  For testing purposes, you can safely use the following site, which has been set up specifically for scanning demonstrations: **scanme.nmap.org**  7. Let us run a few scans using different scanners to see how results vary:  Using the **viewdns** scanner: **scanless -t scanme.nmap.org -s viewdns**    8. Using the **spiderip** scanner: **scanless -t scanme.nmap.org -s spiderip**    9. Using the **standingtech** scanner: **scanless -t scanme.nmap.org -s** **standingtech**  Each of these services focuses on scanning different sets of ports, which means the output will vary. Some scanners are designed to highlight commonly used services, while others dig deeper into less obvious ports.    10. One unique option worth noting is the **ipfingerprints** scanner. Unlike the others, it attempts to estimate the target’s operating system in addition to scanning ports. The results include probability percentages for its OS guesses: **scanless -t scanme.nmap.org -s ipfingerprints.** This provides an extra layer of insight about the target beyond just open ports.    11. If you would like to run a more thorough analysis, you do not have to test scanners one by one. Scanless gives you the option to run all available scanners against your target in a single command: **scanless -t scanme.nmap.org -a**      12. This way, you will get results from multiple sources at once, giving you a broader and more detailed overview of the target system. It is a convenient way to cross-check findings since each scanner may highlight slightly different information. |