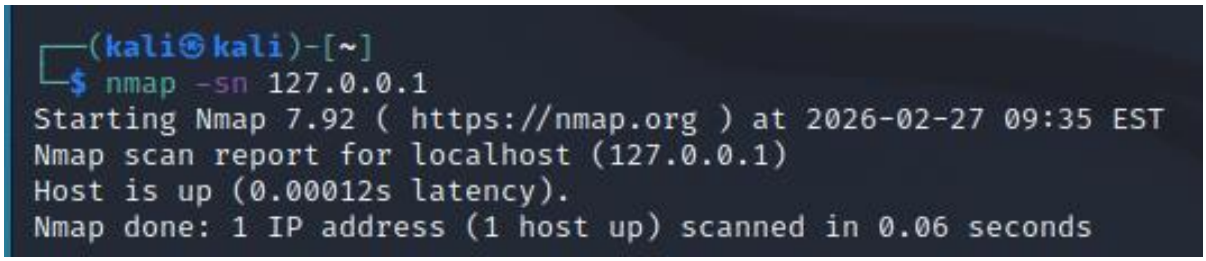
Task 1 — Reconnaissance

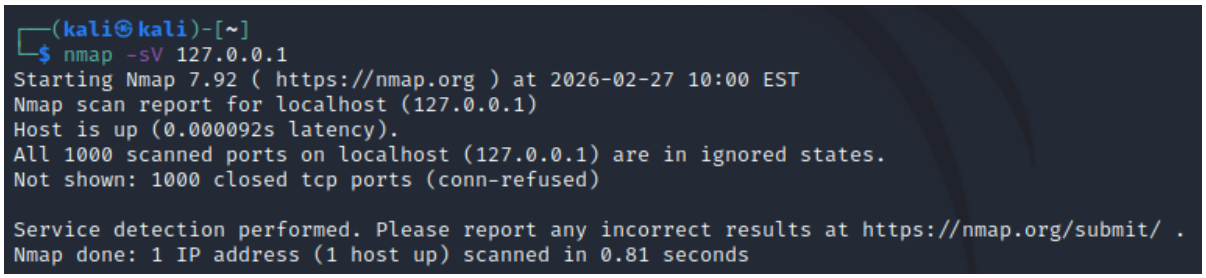
Reconnaissance tools are used to collect information about a target before attempting any form of exploitation. In this task, the **Nmap** was tested. Nmap is a widely-used network scanning tool for discovering hosts, ports and services on a network.

Host Discovery (Ping Scan)



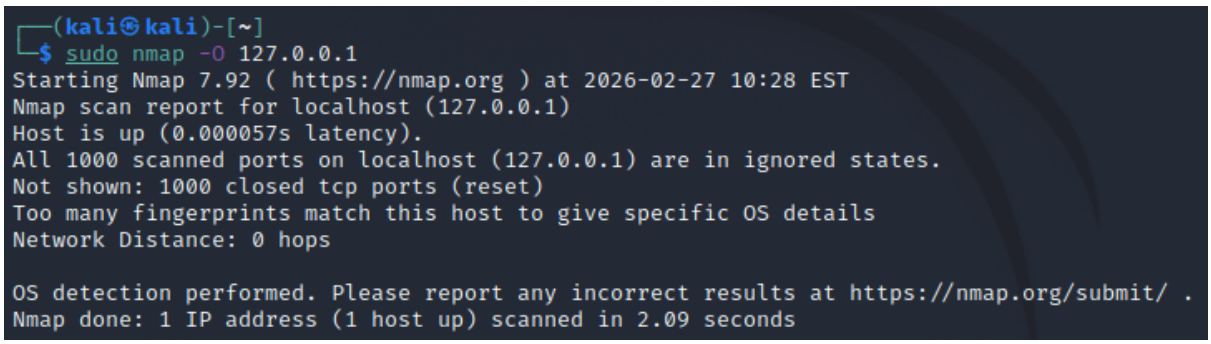
This feature identifies which devices are currently online without performing a heavy port scan, allowing for a faster and stealthier initial map of the target network.

Service and Version Detection



This scan gathers the version information for each open service to determine if the service is outdated or contains known vulnerabilities.

OS Fingerprinting

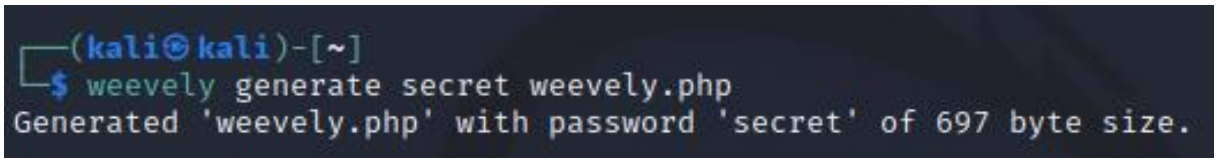


This command used to identify the operating system (like Windows, Linux or macOS) of a target device by analysing its unique network behaviour.

Task 2 — Maintaining Access

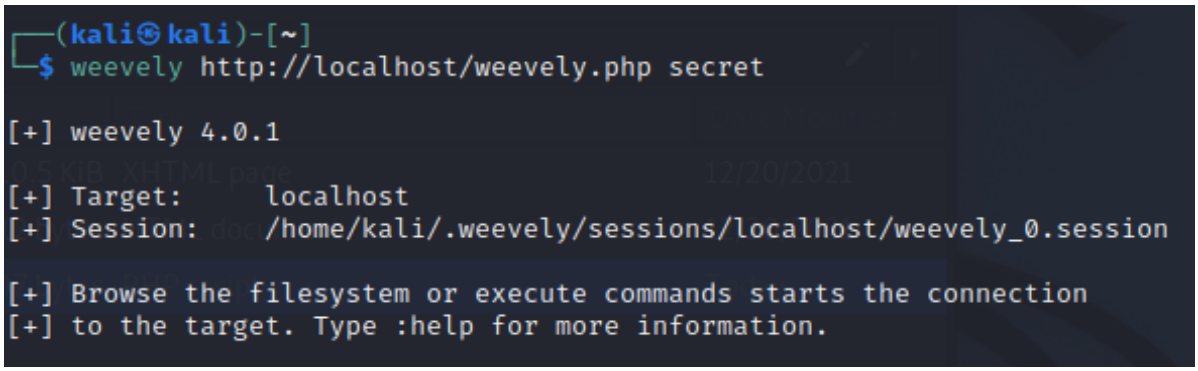
The Maintaining Access phase is critical for ensuring that a penetration tester can remain inside a target system for an extended period, even if the system is rebooted or the initial vulnerability is patched. For this task, **Weevely** was tested. Weevely is a stealthy PHP web shell used to maintain a persistent, telnet-like connection to a compromised web server.

Backdoor Agent Generation



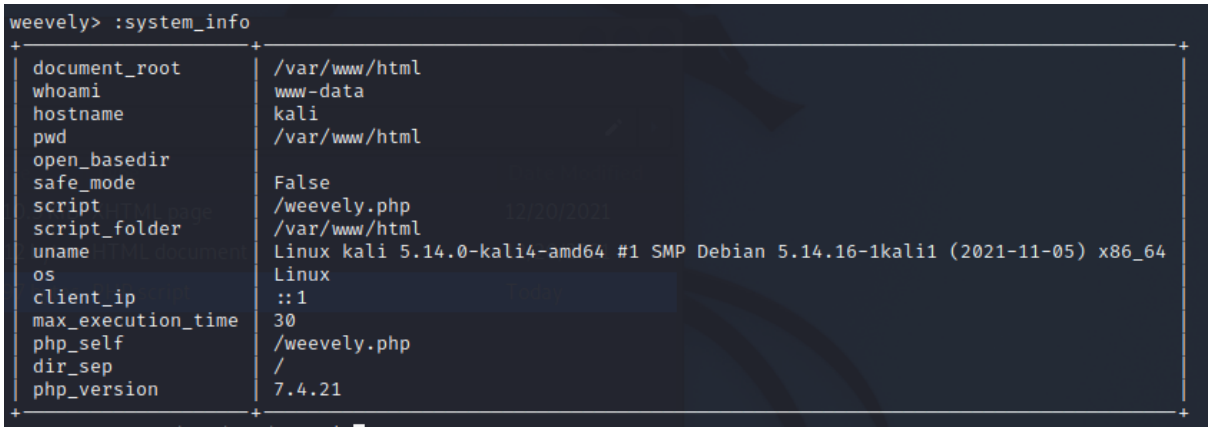
This creates a small, obfuscated PHP script that acts as the "agent." Its polymorphic nature makes it difficult for antivirus software to detect.

Remote Terminal Connection



This feature establishes a persistent communication channel over HTTP. By tunnelling the shell access through web traffic, it allows the tester to maintain access through firewalls that only allow web traffic (Port 80/443), making the remote control session appear as legitimate web activity.

Internal System Enumeration



This used to profile the target environment by identifying server configurations, PHP restrictions and operating system details necessary for further administration or post-exploitation.

Comparison of Tools

Feature	Nmap (Reconnaissance)	Weevely (Maintaining Access)
Primary Goal	External discovery and mapping of the attack surface	Internal persistence and remote system management
Visibility	Active scanning can be detected by firewalls	Highly stealthy, obfuscated code designed to bypass security filters
Usage Context	Used at the very beginning to find a way into the system	Used after exploitation to ensure the tester isn't kicked out
Communication	Direct network probes (TCP/UDP packets)	Encapsulated commands inside standard HTTP web traffic

Conclusion

In this Assignment 1, I learned that both tools are very important for a pen tester. **Nmap** is used first to collect information and find a way into the target. **Weevely** is used later to make sure we do not lose access to the system. Using both tools together allows a tester to plan an attack and then stay in control of the target safely and quietly.