Sections

Privilege Escalation

After gaining an initial Meterpreter shell on the Blue machine, we began the privilege escalation process to achieve NT AUTHORITY\\SYSTEM access.

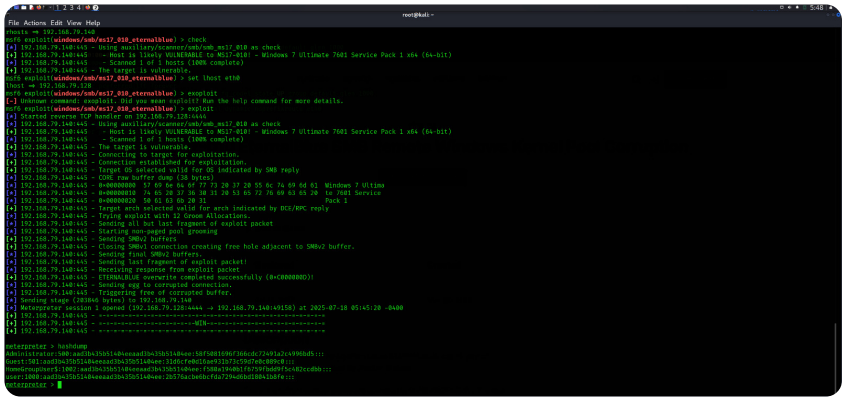
First, we confirmed our current access level and system information using `getuid` and `sysinfo` within Meterpreter.

Next, we used the **local exploit suggester** module in Metasploit to identify possible vulnerabilities that could allow privilege escalation:

```
run post/multi/recon/local_exploit_suggester
```

Based on the results, we executed a suitable local exploit (e.g., ms10_092_schelevator). This successfully created a new Meterpreter session with full SYSTEM access.

The command `getuid` then returned **NT AUTHORITY\\SYSTEM**, confirming the escalation.



Download PDF Report