Lab 17.05.23 – Data Exfiltration and Password Hash Dumping

Profile: WinXPSP2x86
Suggested Plugins: malfind, vaddump, windows, connscan, sockets, consoles, mftparser, userassist, screenshot, cmdscan, printkey, hashdump

1. What tool was used to compromise the system?

   ____

2. What was the IP address of the attacker's machine?

   ____

3. What directory was created to store the files before exfiltration?

   ____

4. Where was data exfiltrated from?

   ____

5. How was exfiltration performed?

   ____

6. How was persistence maintained?

   ____