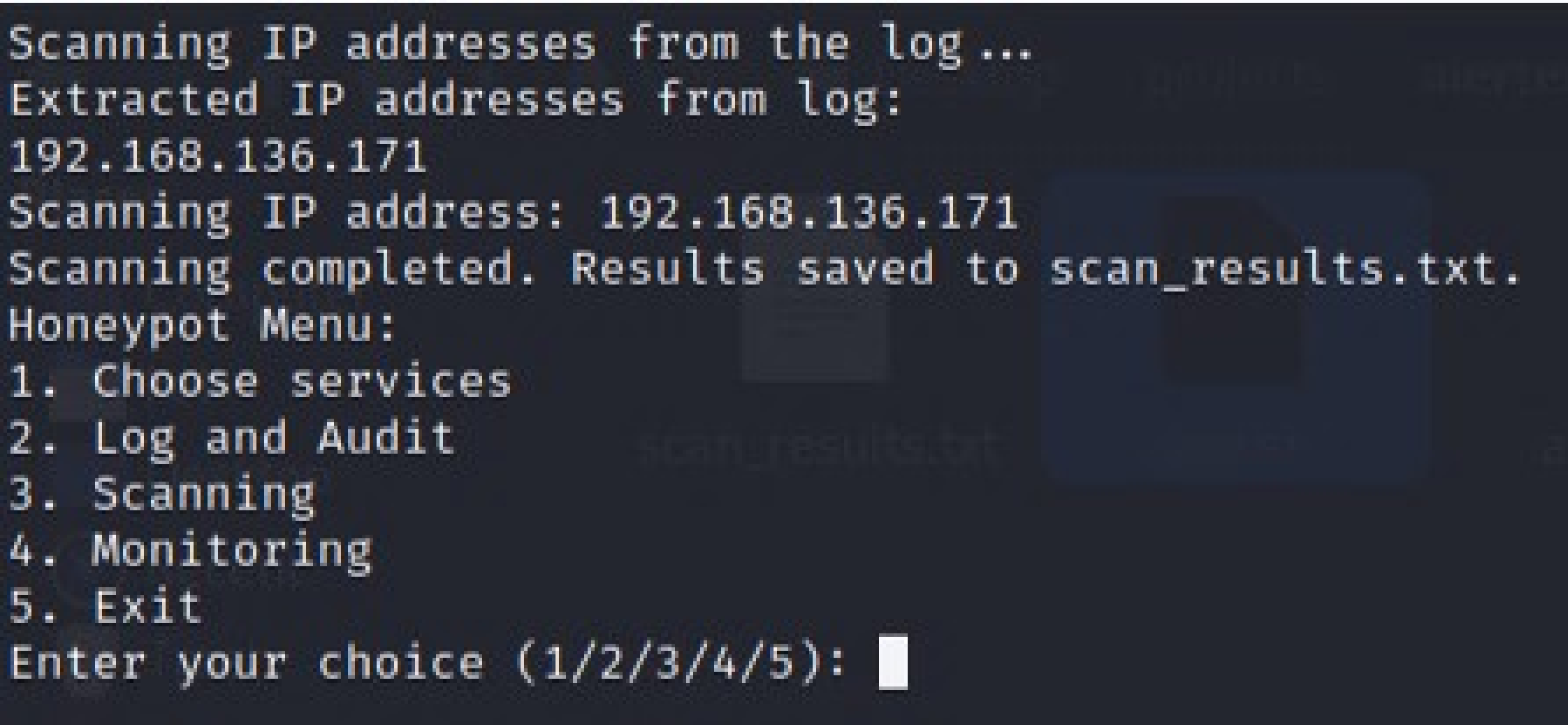
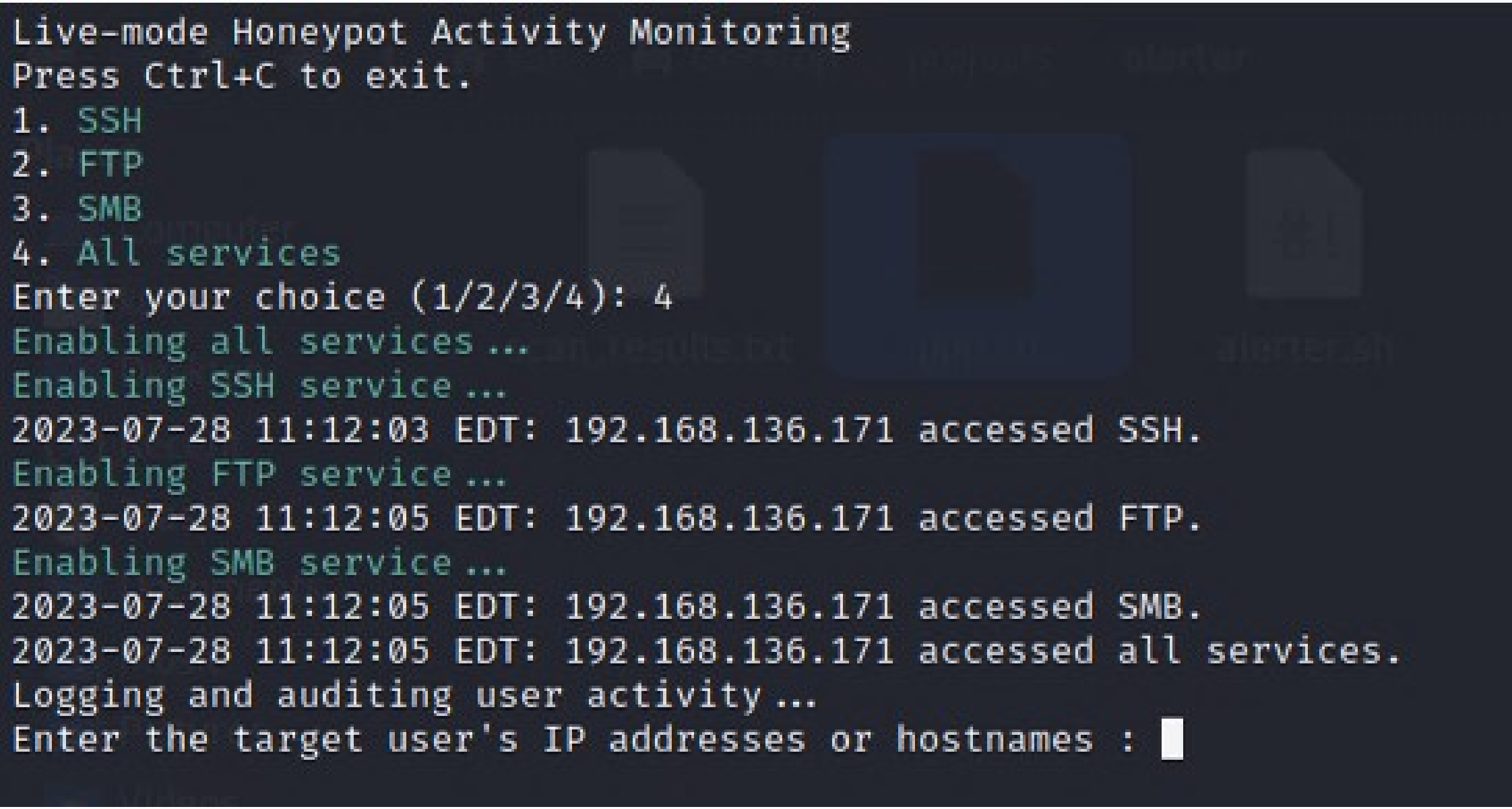

Scanning IP addresses from the log...
Extracted IP addresses from log:
192.168.136.171
Scanning IP address: 192.168.136.171
Scanning completed. Results saved to scan_results.txt.
Honeypot Menu:
1. Choose services
2. Log and Audit
3. Scanning
4. Monitoring
5. Exit
Enter your choice (1/2/3/4/5):

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-28 11:09 EDT
Nmap scan report for 192.168.136.171
Host is up (0.000092s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.3
139/tcp  open  netbios-ssn Samba smbd 4.6.2
445/tcp  open  netbios-ssn Samba smbd 4.6.2
2222/tcp open  ssh         OpenSSH 9.3p1 Debian 1 (protocol 2.0)
| ssh-hostkey:
|   256 b1:c6:8a:fa:54:29:6d:5a:8a:4d:80:64:09:09:93:5d (ECDSA)
|_  256 31:41:07:fa:a4:ab:af:08:34:84:64:c3:0d:9f:43:58 (ED25519)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: -1s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-07-28T15:10:05
|_  start_date: N/A

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.00 seconds
---------------------------------
```

023-07-28 11:09:29 EDT: 192.168.136.171 accessed SSH.
2023-07-28 11:09:30 EDT: 192.168.136.171 accessed FTP.
2023-07-28 11:09:30 EDT: 192.168.136.171 accessed SMB.
2023-07-28 11:09:30 EDT: 192.168.136.171 accessed all services.
2023-07-28 11:12:03 EDT: 192.168.136.171 accessed SSH.
2023-07-28 11:12:05 EDT: 192.168.136.171 accessed FTP.
2023-07-28 11:12:05 EDT: 192.168.136.171 accessed SMB.
2023-07-28 11:12:05 EDT: 192.168.136.171 accessed all services.


Live-mode Honeypot Activity Monitoring
Press Ctrl+C to exit.
1. SSH
2. FTP
3. SMB
4. All services
Enter your choice (1/2/3/4): 4
Enabling all services ...
Enabling SSH service ...
2023-07-28 11:12:03 EDT: 192.168.136.171 accessed SSH.
Enabling FTP service ...
2023-07-28 11:12:05 EDT: 192.168.136.171 accessed FTP.
Enabling SMB service ...
2023-07-28 11:12:05 EDT: 192.168.136.171 accessed SMB.
2023-07-28 11:12:05 EDT: 192.168.136.171 accessed all services.
Logging and auditing user activity ...
Enter the target user's IP addresses or hostnames :

```
Live-mode Honeypot Activity Monitoring
Press Ctrl+C to exit.
1. SSH
2. FTP
3. SMB
4. All services
Enter your choice (1/2/3/4): 4
Enabling all services ...
Enabling SSH service ...
2023-07-28 11:12:03 EDT: 192.168.136.171 accessed SSH.
Enabling FTP service ...
2023-07-28 11:12:05 EDT: 192.168.136.171 accessed FTP.
Enabling SMB service ...
2023-07-28 11:12:05 EDT: 192.168.136.171 accessed SMB.
2023-07-28 11:12:05 EDT: 192.168.136.171 accessed all services.
Logging and auditing user activity ...
Enter the target user's IP addresses or hostnames : 192.168.136.171
set THREADS 10
[*] Starting the Metasploit Framework consOle ... -
```

```
Scanning IP addresses from the log...
Extracted IP addresses from log:
192.168.136.171
Scanning IP address: 192.168.136.171
```