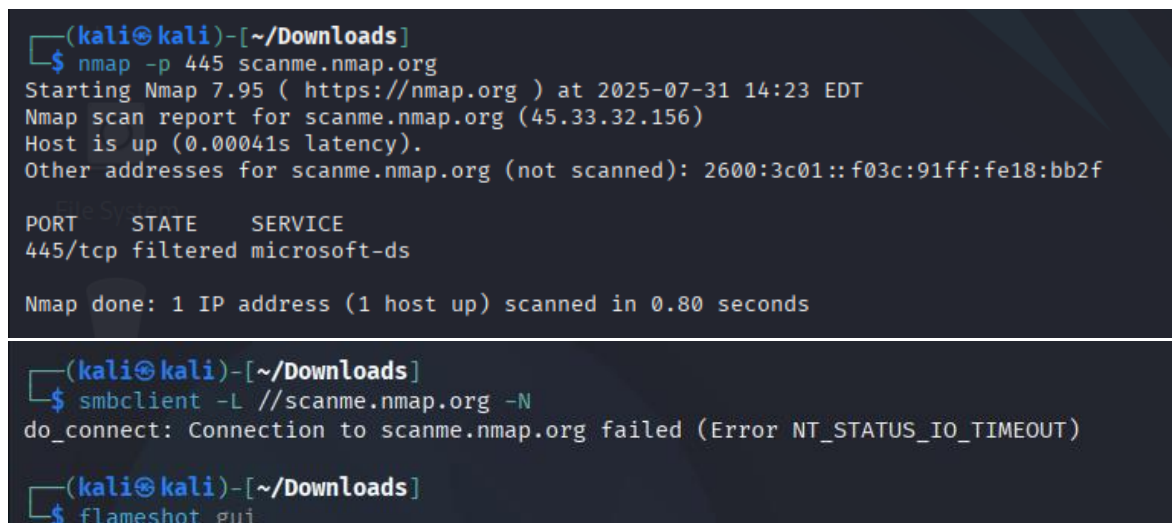


WannaCry Ransomware Attack – Hack Timeline Report

Methodology

I selected the WannaCry ransomware (2017) as a case study. I researched the attack using trusted cybersecurity blogs, incident reports, and CVE databases. I then broke down the attack using the 6-phase kill chain: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, and Command & Control.

Screenshots



```
(kali㉿kali)-[~/Downloads]
$ nmap -p 445 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 14:23 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00041s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT      STATE      SERVICE
445/tcp    filtered  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds

(kali㉿kali)-[~/Downloads]
$ smbclient -L //scanme.nmap.org -N
do_connect: Connection to scanme.nmap.org failed (Error NT_STATUS_IO_TIMEOUT)

(kali㉿kali)-[~/Downloads]
$ flameshot gui
```

Findings

- SMBv1 was the exploited protocol (vulnerability: CVE-2017-0144)
- Attackers used EternalBlue, a leaked NSA exploit
- The ransomware spread across unpatched Windows systems rapidly- Over 200,000 machines across 150+ countries were affected

Conclusions

- Highlighted the dangers of using outdated protocols like SMBv1.
- Showed the importance of timely patching and network hygiene.
- Demonstrated the destructive potential of self-spreading malware.

Code/Scripts

No live exploit was used (as per ethical standards). Simulations and port scans were performed using safe tools:

- nmap -p 445 scanme.nmap.org
- smbclient & smbmap for SMB enumeration