```
#!/bin/bash

TARGET="scanme.nmap.org"
OUTDIR="nmap_results"
DATE=$(date +"%Y-%m-%d_%H-%M-%S")

mkdir -p $OUTDIR

echo "[+] Starting Nmap scan suite on $TARGET"
echo "[+] Results will be saved in $OUTDIR"
echo "--------------------------------------"

# 1. Basic Scan
nmap $TARGET -oN $OUTDIR/basic_$DATE.txt

# 2. Ping Scan
nmap -sn $TARGET -oN $OUTDIR/ping_$DATE.txt

# 3. Top Ports Scan
nmap --top-ports 1000 $TARGET -oN $OUTDIR/top_ports_$DATE.txt

# 4. Full Port Scan (TCP)
nmap -p- -T4 $TARGET -oN $OUTDIR/all_ports_$DATE.txt

# 5. Service Version Detection
nmap -sV $TARGET -oN $OUTDIR/service_version_$DATE.txt

# 6. OS Detection
nmap -O $TARGET -oN $OUTDIR/os_detection_$DATE.txt

# 7. Default Scripts
nmap -sC $TARGET -oN $OUTDIR/default_scripts_$DATE.txt

# 8. Vulnerability Scripts
nmap --script vuln $TARGET -oN $OUTDIR/vuln_$DATE.txt

# 9. HTTP Enumeration
nmap --script=http-* $TARGET -oN $OUTDIR/http_$DATE.txt

# 10. SSL Enumeration (if HTTPS)
nmap --script=ssl-enum-ciphers $TARGET -oN $OUTDIR/ssl_$DATE.txt

# 11. Aggressive Scan
nmap -A $TARGET -oN $OUTDIR/aggressive_$DATE.txt
```

```
# 12. Traceroute
nmap --traceroute $TARGET -oN $OUTDIR/traceroute_$DATE.txt

echo "----------------------------------------"
echo "[+] All scans completed successfully"
```