

# Monitor Currently Mounted SMB Shares from Server

```
smbstatus --shares
```

SMB Monitoring Script:

```
#!/bin/bash

#SMB Mount Monitoring
SMB=$(smbstatus --shares | grep -oE "\b([0-9]{1,3}\.){3}[0-9]{1,3}\b")

echo "#####" >> /tmp/hacker.info
echo "SMB Mount(s) Mounted!" >> /tmp/hacker.info
echo "#####" >> /tmp/hacker.info
for i in "${SMB[@]}"
do
    echo "#####" >> /tmp/hacker.info
    echo "HACKER DETECTED W/ IP $i" >> /tmp/hacker.info
    echo >> /tmp/hacker.info
    nbtscan "$i" >> /tmp/hacker.info
    nslookup "$i" >> /tmp/hacker.info
    arp -a "$i" >> /tmp/hacker.info
    echo >> /tmp/hacker.info
done

echo "#####" >> /tmp/hacker.info
echo "SMB General Information" >> /tmp/hacker.info
echo >> /tmp/hacker.info
echo "smbstatus" >> /tmp/hacker.info
smbstatus >> /tmp/hacker.info
echo >> /tmp/hacker.info
echo "End SMB Information" >> /tmp/hacker.info
echo "#####" >> /tmp/hacker.info
```