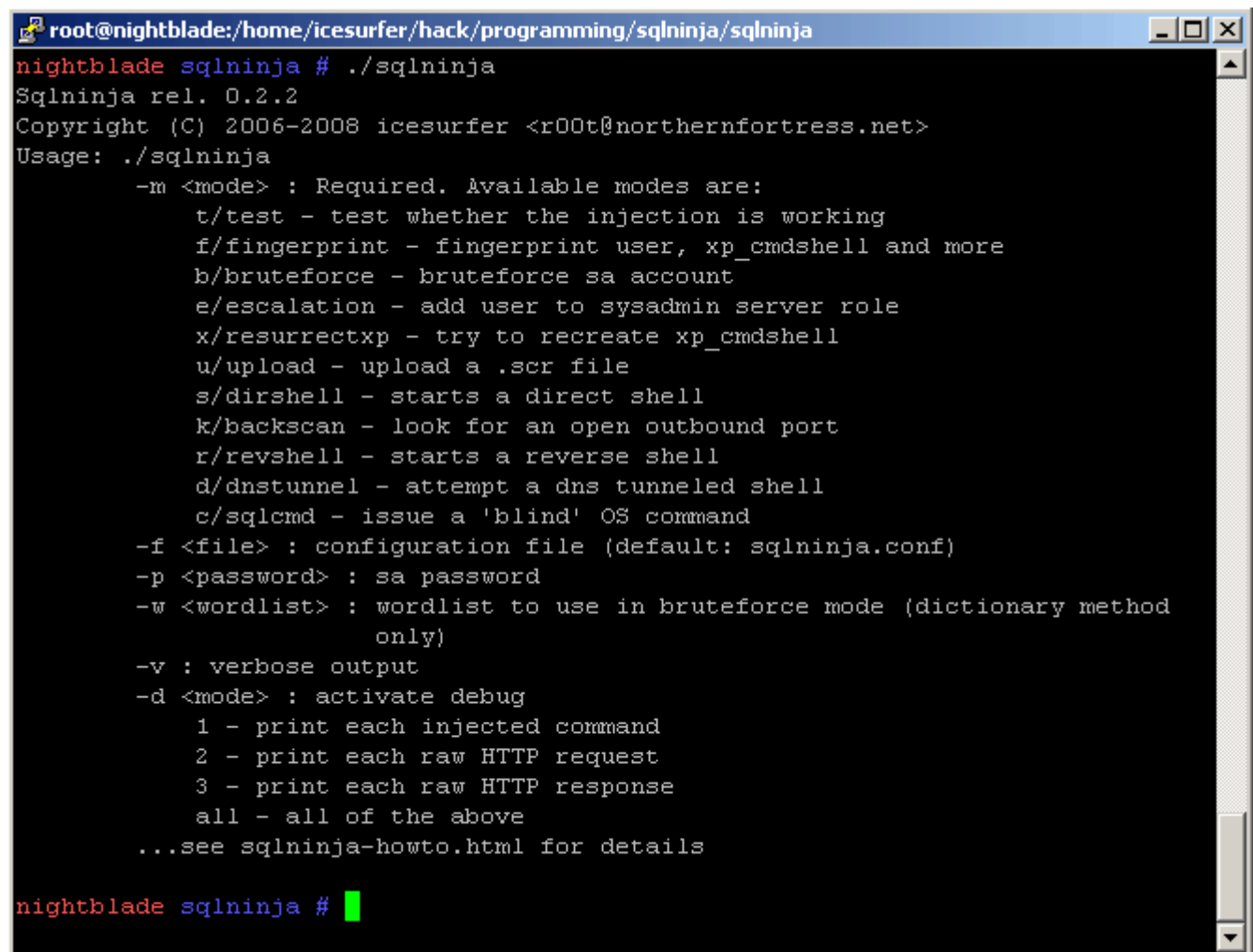


Sqlninja

A terminal window titled 'root@nightblade:/home/icesurfer/hack/programming/sqlninja/sqlninja' showing the execution of the 'sqlninja' script. The script displays its version (0.2.2), copyright (2006-2008 icesurfer), and a detailed usage guide. The usage guide lists various modes and options, including -m for different attack modes, -f for configuration file, -p for password, -w for wordlist, -v for verbose output, and -d for debug options. The prompt 'nightblade sqlninja #' is visible at the bottom.

```
root@nightblade:/home/icesurfer/hack/programming/sqlninja/sqlninja
nightblade sqlninja # ./sqlninja
Sqlninja rel. 0.2.2
Copyright (C) 2006-2008 icesurfer <r00t@northernfortress.net>
Usage: ./sqlninja
    -m <mode> : Required. Available modes are:
        t/test - test whether the injection is working
        f/fingerprint - fingerprint user, xp_cmdshell and more
        b/bruteforce - bruteforce sa account
        e/escalation - add user to sysadmin server role
        x/resurrectxp - try to recreate xp_cmdshell
        u/upload - upload a .scr file
        s/dirshell - starts a direct shell
        k/backscan - look for an open outbound port
        r/revshell - starts a reverse shell
        d/dnstunnel - attempt a dns tunneled shell
        c/sqlcmd - issue a 'blind' OS command
    -f <file> : configuration file (default: sqlninja.conf)
    -p <password> : sa password
    -w <wordlist> : wordlist to use in bruteforce mode (dictionary method
                    only)
    -v : verbose output
    -d <mode> : activate debug
        1 - print each injected command
        2 - print each raw HTTP request
        3 - print each raw HTTP response
        all - all of the above
    ...see sqlninja-howto.html for details

nightblade sqlninja #
```

Fancy going from a SQL Injection on Microsoft SQL Server to a full GUI access on the DB? Take a few new SQL Injection tricks, add a couple of remote shots in the registry to disable Data Execution Prevention, mix with a little Perl that automatically generates a debug script, put all this in a shaker with a Metasploit wrapper, shake well and you have just one of the attack modules of sqlninja!

Sqlninja is a tool targeted to exploit SQL Injection vulnerabilities on a web application that uses Microsoft SQL Server as its back-end.

Its main goal is to provide a remote access on the vulnerable DB server, even in a very hostile environment. It should be used by penetration testers to help and automate the process

of taking over a DB Server when a SQL Injection vulnerability has been discovered.

Download

<http://sqlninja.sourceforge.net/download.html>