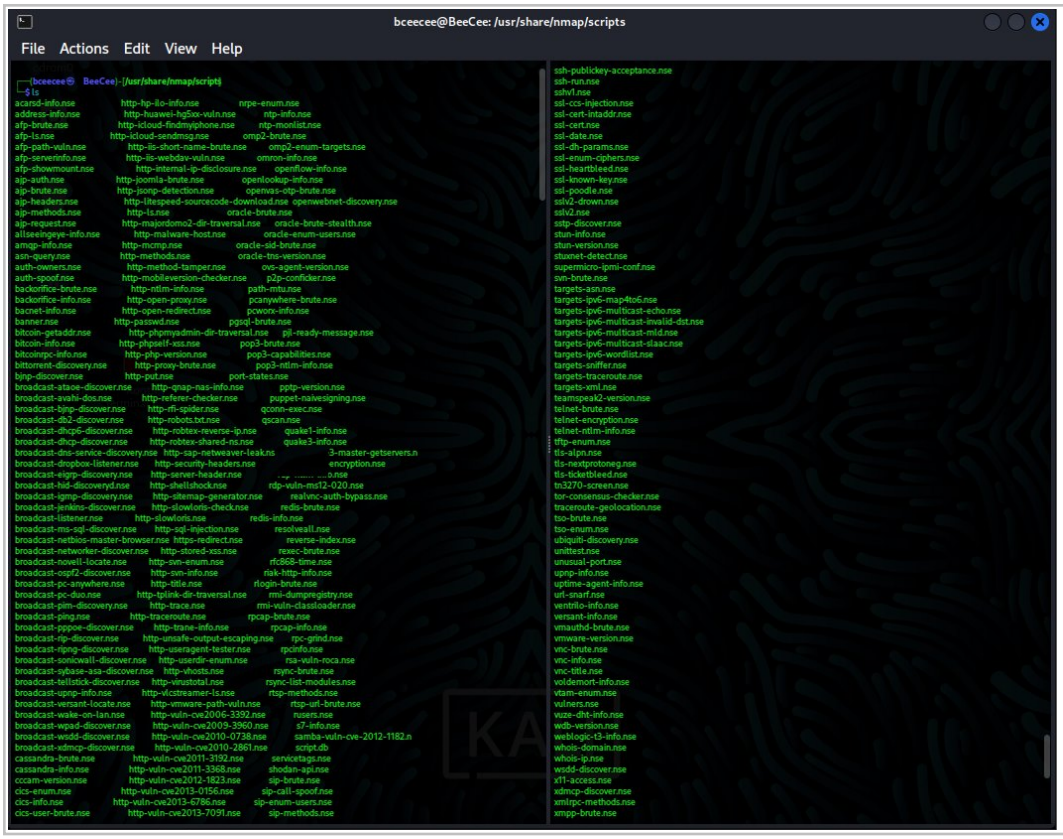
Section 7: Vulnerability Analysis

Name:

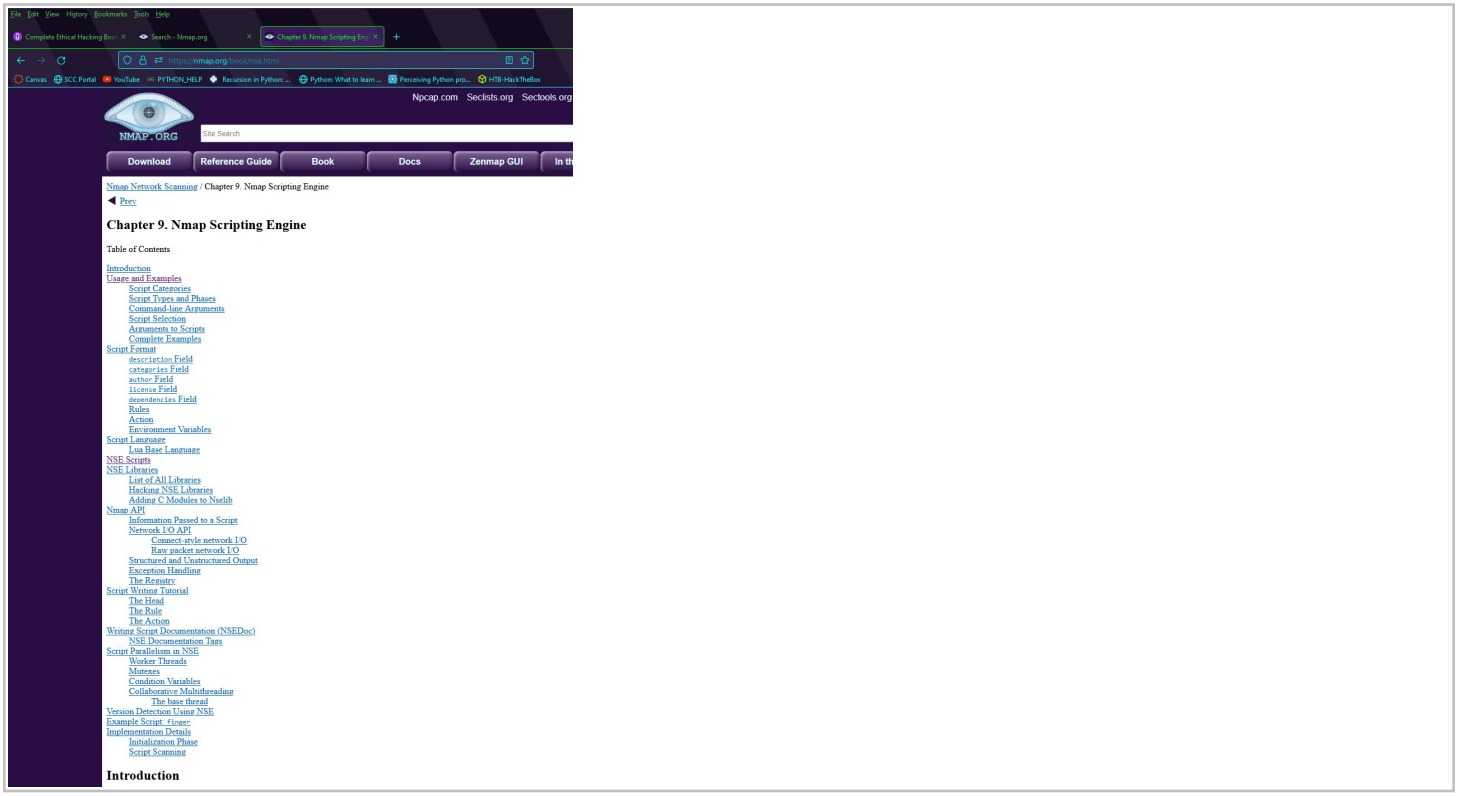
BC

Choose screenshots for each lab that best illustrates your completion of the lab. Submit by clicking the box and locating the screenshot. Use a black-on-white color scheme for all Terminal sessions.

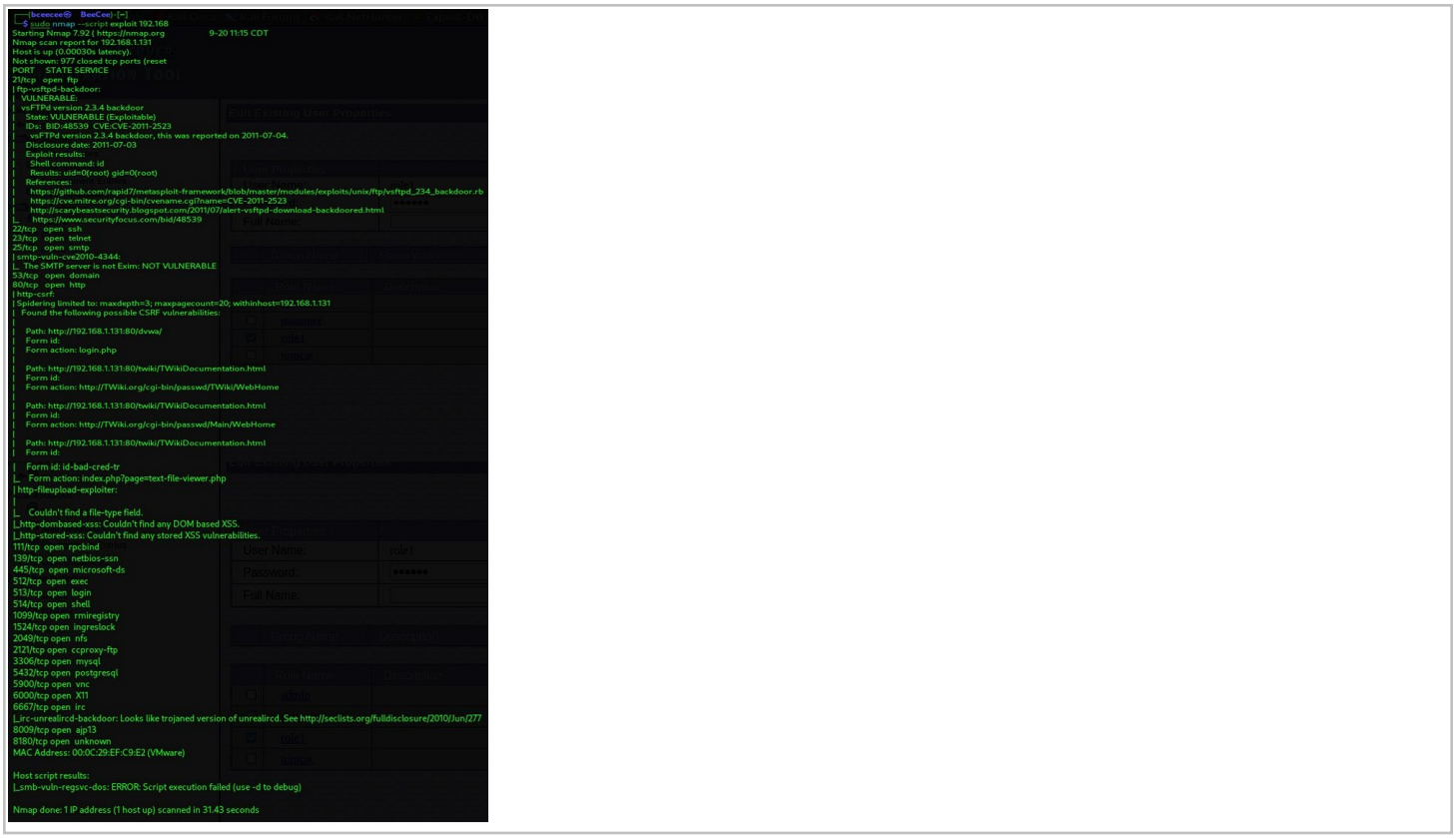
Lab 1: List the available scripts within Kali (53)



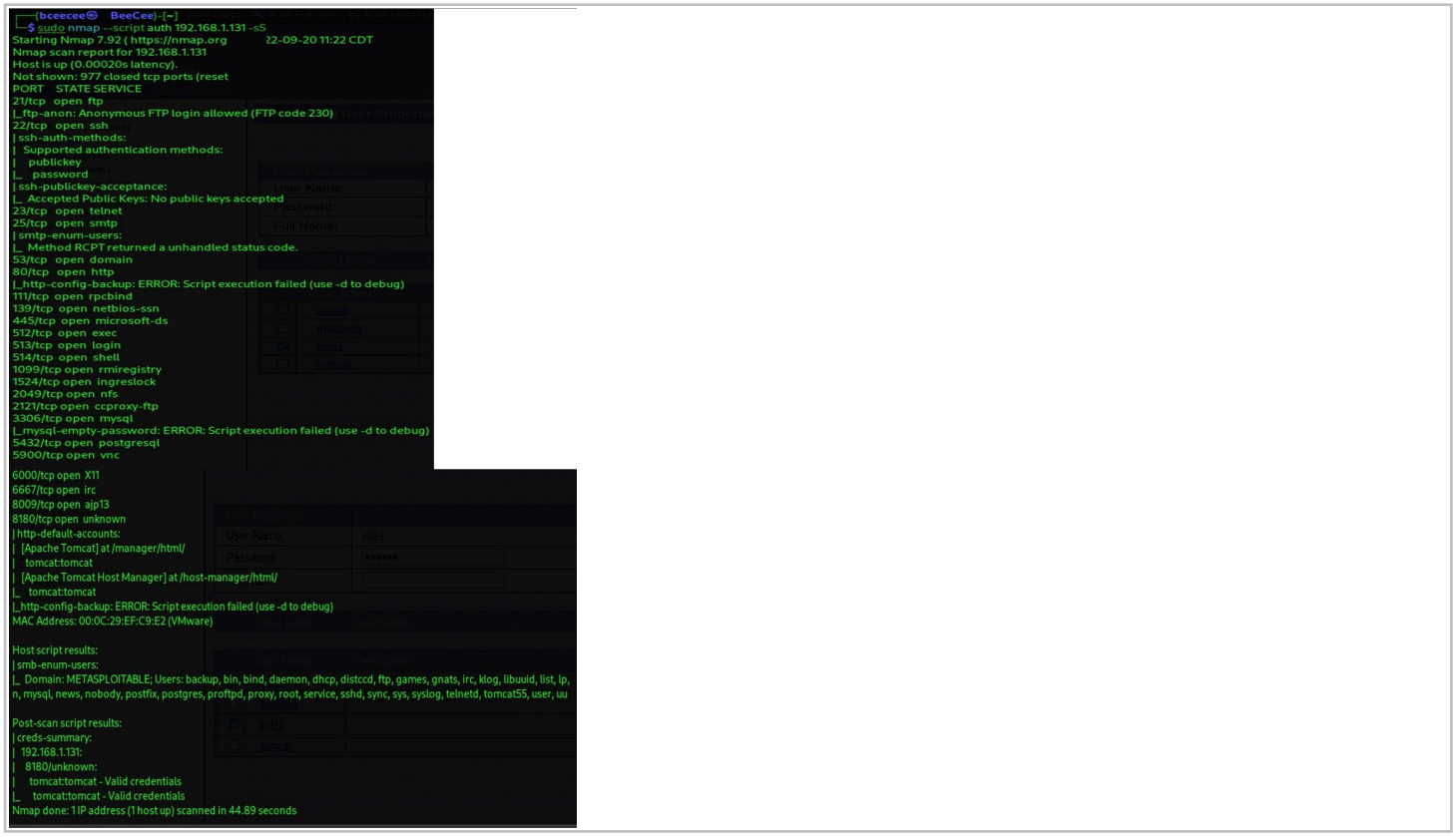
Lab 2: Display the official documentation for nmap scripts (53)



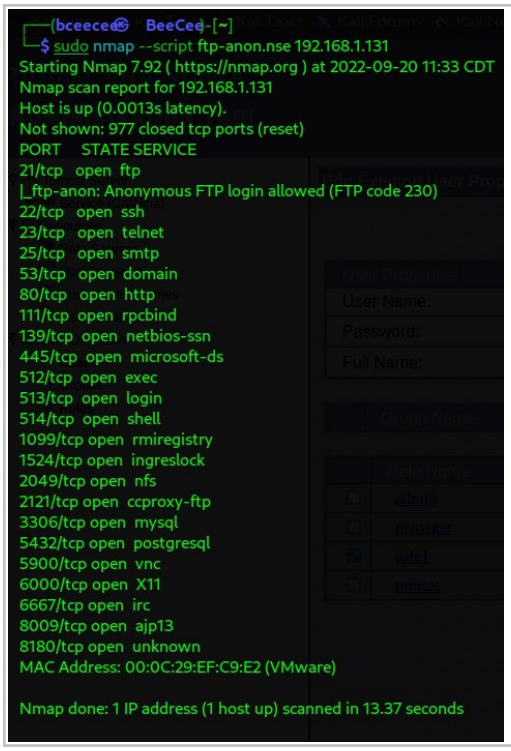
Lab 3: Perform an exploit group scan of Metasploitable2 (53)



Lab 4: Perform an auth group scan of Metasploitable2 (53)

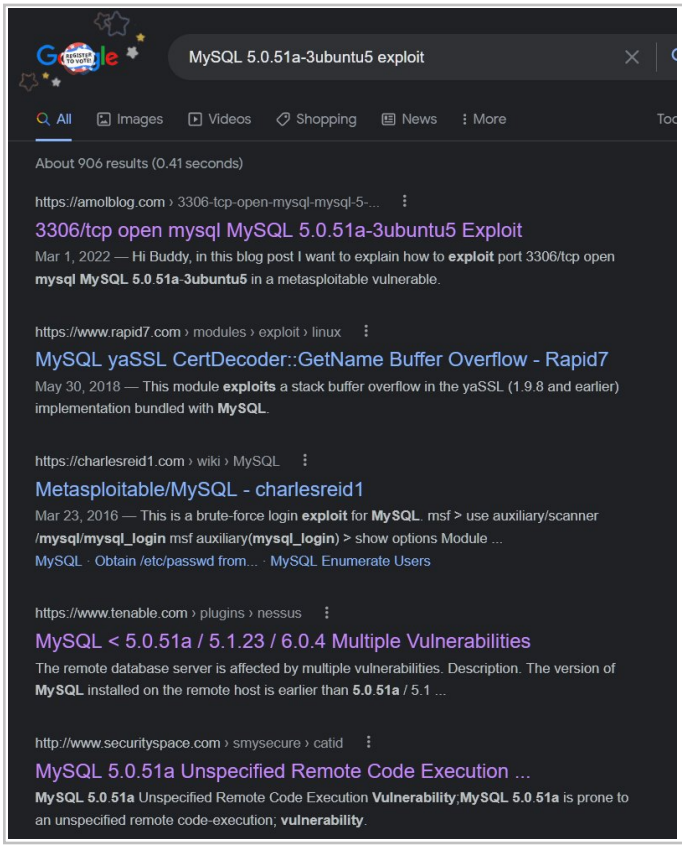


Lab 5: Run the FTP Anonymous script against Metasploitable2 (53)



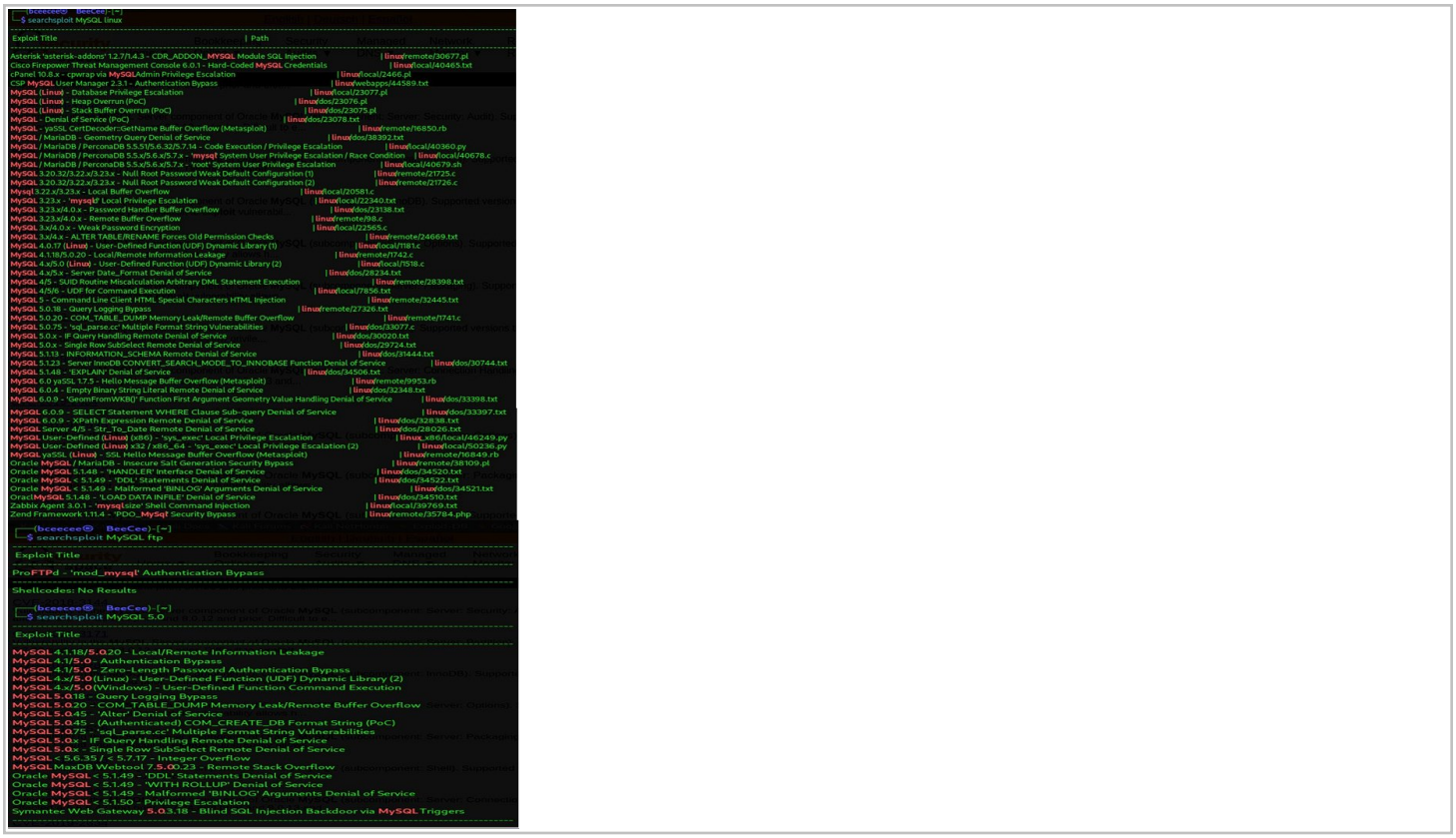
Lab 6: Conduct an Internet search to find an exploit against open port 3306 (53)

What do you enter into an Internet search box to find the exploit? MySQL (5.0.51a-3ubuntu5) exploit

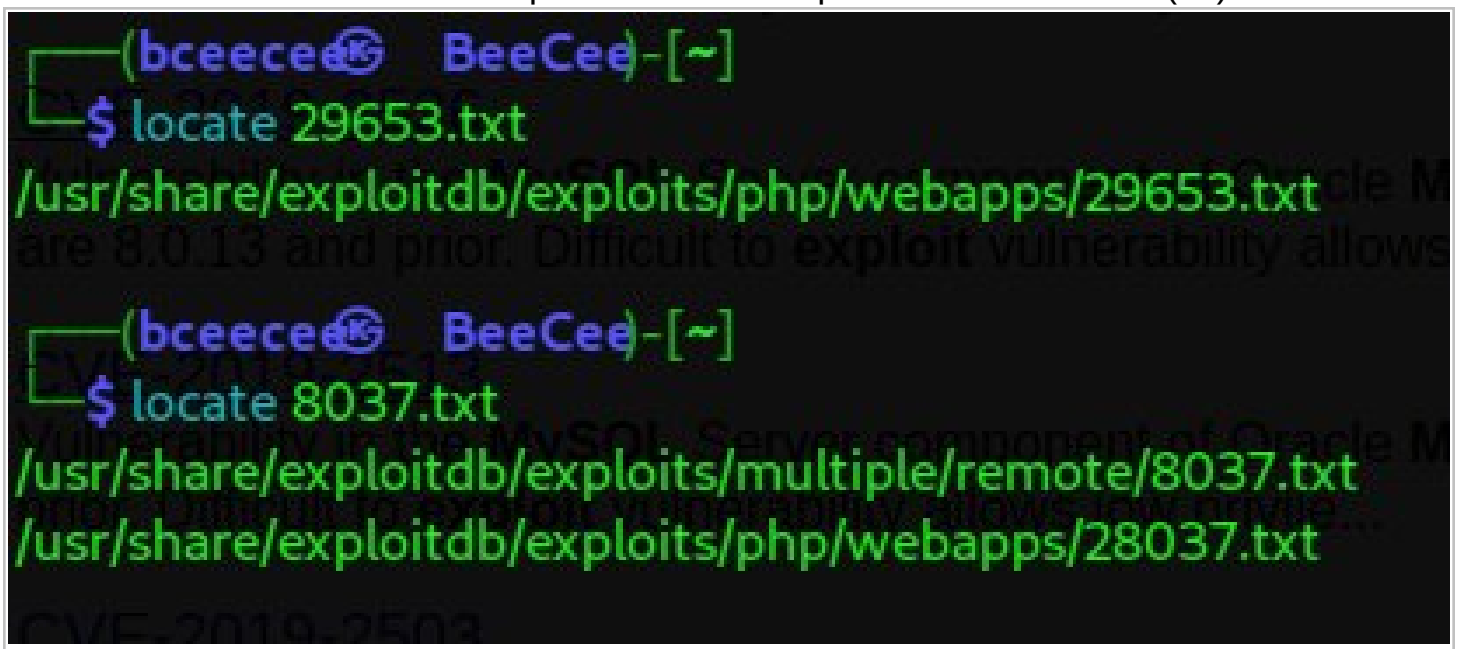


First list exploits for "MySQL Linux", then attempted to search more possibilities.

Lab 7: Run a command to list exploits for the MySQL vulnerability found in Lab 5 (53)



Lab 8: Run a command to find the path for the first exploit from lab 7 above (53)



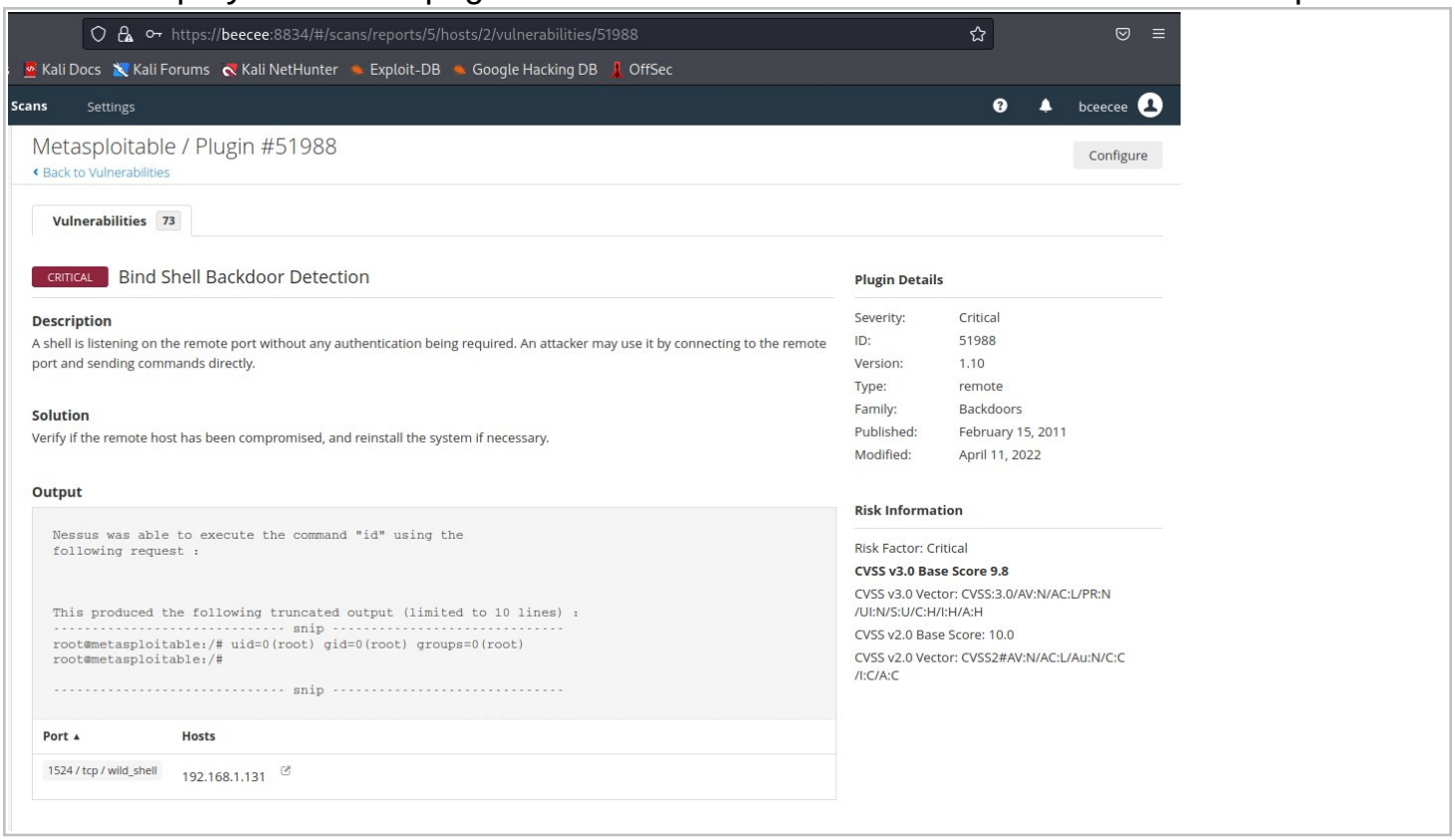
^^ First exploit is from search "MySQL", first exploit. Second is when searching more in depth with "MySQL FTP" in the search.

Lab 9: Display the top 20 lines of code for one of the MySQL exploits (53)

Got Fancy So there is in VI & STDOUT

```
require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
    Rank = GoodRanking

    include Msf::Exploit::Remote::Tcp

    def initialize(info = {})
        super(update_info(info,
            'Name'           => 'MySQL yaSSL SSL Hello Message Buffer Overflow',
            'Description'    => %q{
                    This module exploits a stack buffer overflow in the yaSSL (1.7.5 and ear
lier)
                implementation bundled with MySQL <= 6.0. By sending a specially crafted
                Hello packet, an attacker may be able to execute arbitrary code.
            },
            'Author'         => [ 'MC' ],
            'License'        => MSF_LICENSE,
            'Version'        => '$Revision: 9262 $',
            'References'     =>
                [
                    [ 'CVE', '2008-0226' ],
                    [ 'OSVDB', '41195' ],
                    [ 'BID', '27140' ],

                ],
            'Privileged'     => false,
            'Payload'        =>
                {
                    'Space'    => 100,
                    'BadChars' => "\x00\x20\x0a\x0d\x2f\x2b\x0b\x5c",
                },
            'Platform'       => 'linux',
            'Targets'        =>
                                                39,1-8      20%

┌──(bceece㉿  BeeCee)-[/usr/.../exploitdb/exploits/linux/remote
└─$ vi 16849.rb

┌──(bceece㉿  BeeCee)-[/usr/.../exploitdb/exploits/linux/remote
└─$ awk 'FNR>=12 && FNR<=32' 16849.rb
require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
    Rank = GoodRanking

    include Msf::Exploit::Remote::Tcp

    def initialize(info = {})
        super(update_info(info,
            'Name'           => 'MySQL yaSSL SSL Hello Message Buffer Overflow',
            'Description'    => %q{
                    This module exploits a stack buffer overflow in the yaSSL (1.7.5 and ear
lier)
                implementation bundled with MySQL <= 6.0. By sending a specially crafted
                Hello packet, an attacker may be able to execute arbitrary code.
            },
            'Author'         => [ 'MC' ],
            'License'        => MSF_LICENSE,
            'Version'        => '$Revision: 9262 $',
            'References'     =>
                [
                    [ 'CVE', '2008-0226' ],
```

Lab 10: Display the details page about a critical issue from a Nessus scan on Metasploitable2 (55)



https://beecee:8834/#/scans/reports/5/hosts/2/vulnerabilities/51988

Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

Scans | Settings | bceecee

Metasploitable / Plugin #51988

Configure

‹ Back to Vulnerabilities

Vulnerabilities 73

CRITICAL Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```
Nessus was able to execute the command "id" using the
following request :


This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

------------------------------ snip ------------------------------
```

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.1.131

Plugin Details

Severity:	Critical
ID:	51988
Version:	1.10
Type:	remote
Family:	Backdoors
Published:	February 15, 2011
Modified:	April 11, 2022

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Lab 11: Display details about a critical issue with Windows 7 based on Nessus (56)